The Case of the Russian Electronic Identity Card: from the Promise of E-government to the Problem of Data Sovereignty

by

Iryna Matiyenko

B.A., V. N. Karazin Kharkiv National University, 2003
M.A., V. N. Karazin Kharkiv National University, 2004

A Dissertation Submitted in Partial Fulfillment
of the Requirements for the Degree of

Doctor of Philosophy

in the Department of Political Science

Supervisory Committee

The Case of the Russian Electronic Identity Card:
from the Promise of E-Government to the Problem of Data Sovereignty

by

Iryna Matiyenko

B.A., V.N. Karazin Kharkiv National University, 2003
M.A., V.N. Karazin Kharkiv National University, 2004

Supervisory Committee

Professor Colin J. Bennett, Department of Political Science, University of Victoria
Supervisor

Professor Oliver Schmidtke, Department of Political Science, University of Victoria
Departmental Member

Professor Serhy Yekelchyk, Department of History, University of Victoria
Outside Member

Abstract

Electronic identity cards have been the focus of different disciplines in the last two decades. They are viewed as technological tools that enable e-government in public administration studies; as systems of surveillance and social sorting in more critical social studies literature; and analyzed as a result of political pressure from powerful groups and private sector interests in political science. This work examines the rise and fall of the electronic identity card in the Russian Federation using concepts and theories developed in Western scholarship.

This is a qualitative case study of the Russian "Universal Electronic Card" project focusing on the processes of policy definition and implementation, while contextualizing them culturally, politically and historically within a state with the legacies of oppressive passport regimes. I document ideas expressed by the policy interpretive communities and analyze their views on innovation as a symbol of technological progress, which are expressed through multiple conflicting interpretations regarding the practicality, legitimacy, and morality of this progress. Based on interpretive policy analysis, I identify two antagonistic policy models that target the reform of the state identification system, based on the technological innovation of the electronic identity card. The first model, the *Oligopoly on the Means of Identification*, relies on market solutions to government problems through public-private partnerships with the banking and IT sectors. The second model, *State Monopoly on the Means of Identification*, is concerned with the enforcement of the electronic identity card technology, from design to production and implementation.

I argue that a political struggle between the two models leads to the proliferation of problems with information ownership, control, and security, forcing the state to address these problems through national security, cybersecurity reviews, and data sovereignty regulations. As demonstrated here, the inability of the state to enforce data sovereignty in a complex, interconnected, and globalized technological system of information exchange became a significant constraint to the implementation of a national electronic identity card system in Russia.

Keywords: case study, e-government, digital services, electronic identity cards, resistance to identity cards, state identification systems, data ownership, privacy, data sovereignty, public administration reforms, Russian politics, smart cards, social sorting, surveillance.

Table of Contents

List of Figures

List of Abbreviations

International:

eID: electronic Identification

eIDAS: electronic Identification, Authentication and trust Services

EU: European Union

IdM: Identity Management

ICT: Information and Communication Technology

IM/IT: Information Management/Information Technology

NPM: New Public Management

OECD: Organization for Economic Co-operation and Development

The Russian Federation[1]:

ESIA (ЕСИА): Edinaia Sistema Identifikatsii i Autentifikatsii [Single System of Identification and Authentication]

FRGU (ФРГУ): Federalnyi Reestr Gosudarstvennyh i Munitsypalnyh Uslug [Federal Registry of Government and Municipal Services]

SNILS (СНИЛС): Strahovoi Nomer Individualnogo Litsevogo Scheta [Individual Social Insurance Account Number]

SMEV(СМЭВ): Sistema Mezhvedomstvennogo Elektronnogo Vzaimodeistviia [System of Cross-departmental Electronic Communication]

MSC: Sotsyalnaia Karta Moskvicha [Moscow Social Card]

UEC (УЭК): Universalnaia Elektronnaia Karta [Universal Electronic Card]

[1] Russian words in this dissertation are transliterated based on the US Library of Congress system of romanization

Acknowledgments

I would like to express my deepest gratitude and respect to **Dr. Colin Bennett**, my academic supervisor, a career mentor and a privacy advocate, who impacted my life, my academic journey and my professional career in so many ways. Dr. Bennett not only provided guidance and believed in me during my long research journey but also offered many opportunities for professional networking through invitations to the numerous privacy and data security conferences, workshops and seminars. Dr. Bennett introduced me to the founders and prominent members of the Surveillance Studies Network. Because of him and research experience within the surveillance studies, I am professionally involved with privacy protection and compliance operations in the public sector and enjoy my specialization very much. Dr. Bennett's funding, supervision and teaching style was instrumental for transferring academic skills and knowledge into my professional development.

I am profoundly grateful to **Dr. Oliver Schmidtke** for his guidance and advice during my graduate fellowship at University of Victoria's Centre for Global Studies (CFGS). CFGS's staff and research fellows provided much needed support during the writing phase of my research, enabling collaboration with other PhD candidates, exchange of feedback and ideas during writing sessions, as well as providing a wonderful office space on university campus.

I am thankful to **Dr. Serhy Yakelchyk, Dr. Marlea Clarke**, **Dr. Feng Xu**, and **Dr. Andrew Wender** for insightful conversations that helped me to shape my thesis. I appreciated their personal interest and support of my academic and professional journey as a mother and an international student. They always made me feel included and respected while providing honest feedback on my academic progress and teaching experience. I enjoyed very much many TAs and guest lecture opportunities under their supervision, which allowed me to develop my teaching style and share my research findings with the students and broader community.

I am grateful to the staff at the **University Child Care Services**, who provided an outstanding level of care for both of my children, while supporting their social, intellectual and physical growth. I value this contribution to the academic and professional development of students with dependent children very much. Their hard work and dedication allowed me to focus on the work in the library, engage in teaching and research and to connect with other parents on a similar journey towards the Ph.D. degree.

Last but not least, I would like to express my appreciation to the administrative staff in the Political Science Department: **Rosemary Barlow**, **Joanne Denton** and **Rachel Richmond**. Thank you, for the welcoming attitude, kind smiles, informative advice and assistance with the all the procedural steps required for successful graduation.

Dedication

To my loving family, for their unconditional love, support, patience, and encouragement during this journey.

Chapter 1: Introduction

1.1: Context and Research Questions

In 2013, Russian TV broadcast a commercial depicting a group of secondary school students on a trip to the fictional "Ancient Museum." The museum guide takes visitors through a hall filled with glass screens containing different forms of official documents and government records while explaining their outdated inefficiency: "*Today*, *nobody remembers that in the past, to receive a service from the government, citizens were required to provide many kinds of paper documents. Documents were damaged, lost, expired. People were wasting time, money, energy*" (Figure 1).

Figure 1 The problem of a paper-based bureaucracy, a screenshot from the commercial.

Note. The image is a screenshot of the UEC commercial posted in the UEC official marketing channel "PressaUecard, 2013" (https://www.youtube.com/watch?v=WqUB3YUntrM).

The guide approaches a digital transparent screen with a map of the world and flashing images of the plastic card with a microchip and Russian national emblem and declares: "*But*

now, when everybody has a Universal Electronic Card, we cannot imagine how it was, to wait endlessly in a queue". The digital screen is continuously changing images of a banking payment card number and microchip accompanied by lines of digits and flows of computer system processing data (Figure 2). The commercial ends with a joke, as one of the students asks the question: What is a queue? (PressaUecard, 2013).

Figure 2 Universal Electronic Card as a paperless solution for government, a screenshot from the commercial.

Note. The image is a screenshot of the UEC commercial posted in the UEC official marketing channel "PressaUecard, 2013" (https://www.youtube.com/watch?v=WqUB3YUntrM).

The persuasive language of this commercial creates a contrast between "old-fashioned paper-based bureaucracy" (Figure 1) and the efficiency of the modern "smart identity card" (Figure 2), a plastic identity card with an embedded microchip. This innovation, adopted from credit cards, promises to improve the verification of citizens' identity just as machine-readable credit cards have improved the verification of banking clients' identity, thus enabling cashless and remote transactions. The goal of the commercial was to show how the verifiable banking

payment card could change the bureaucratic processes of the Russian state identification system. This system was historically an overly bureaucratized process of documenting identities based on peoples' residential registration. In-person identity verification was required, supported by original documents signed with wet ink and stamped with wet stamps on the official template by authorized employees, in order to receive some types of government or public service. These processes produced the shared understanding of the problem with "*many damaged and lost documents*" as well as a need "*to stand endlessly in a queue*" to verify identity in person again and again, in order to apply for yet another official document supporting your eligibility for the service. The technological promise of the plastic card with a microchip to confirm identity and streamline access to government services to verified eligible individuals promotes the vision that children would never know the reality of the paper-based relations with the state, nor would they need to stand in a queue as their parents once did.

This appeal to novelty is a fallacy based on the assumption that new is always better than old, and that technological progress will inevitably bring about improvements in our lives. There are no limits to how technology can improve pathologic bureaucracies burdened by red tape, duplication, and waste. The electronic identity card is very powerful conceptually, in terms of the promise of making government services more accessible, more citizen-centered, more user-friendly, and more secure. Such innovation is also tangible, visible, and universal in application. Unlike technological investments into the government's internal IM/IT infrastructure and systems, the electronic identity card can be perceived as a marketable political idea that political leadership can deliver to many voters and taxpayers, as they promise to make life easier for everybody. I became interested in this subject because the policy language in many jurisdictions

promotes the same appeal to novelty fallacy, giving greater significance to the concept of a technological fix for persistent bureaucratic problems (Johnston, 2018).

The process of government modernization utilizing smart card technology is a global trend, and according to the industry, 3.6 billion citizens in 136 countries will carry a national electronic identity card by 2021 (Acuity Market Intelligence, 2017). The presumed inevitability of technological progress embodied in the smart card is discussed reciprocally with the concepts of electronic government, securing digital access to public services, more effective and efficient public administration, and more inclusiveness and accountability in government programs (Melin, 2016; Ott et al, 2018; Goede, 2019;). However, in 2021 the trend is still not consistent with the predictions from 2017 as "120 countries are in the process of deploying electronic passports and over 70 countries are implementing electronic ID" (Thales report, 2021). It is important to consider that deployment and implementation may not necessarily result in national electronic identity card institutionalization.

This Ph.D. thesis aims to understand the driving forces, circumstances, and outcomes of the government's electronic card implementation through a case-study analysis of the Russian national electronic ID project – the Universal Electronic Card (UEC). The driving motivation for this dissertation is to establish why and how the electronic identity card became government policy, and to determine what problems of public service and administration it was designed to address.

My initial hypothesis was formulated under the influence of the surveillance studies literature. I expected that the Russian government understood the potential of microchip technology to create a record each time the electronic identity card is used, and was interested in building a more efficient state surveillance system for the collection of information about their

citizens, and implementing government policies which correlate to discovered patterns of behaviour. Such an observation would confirm several theoretical claims developed within Western scholarship, supporting the view that electronic identity cards are more likely to be implemented by strong unitary states, with hierarchically organized public administrations and centralized state functions, and institutionalized paper-based national identification systems (Bennett & Lyon, 2008; About et al, 2013; Lee, 2018). My Ukrainian background compelled me to connect my family's "passport stories" about movement control and discrimination in the former Soviet Union with a possible reinvention of the oppressive Soviet passport system, greatly improved by the new electronic identity card. When Vladimir Putin again became president in 2012, and Soviet nostalgia bred a new political anti-Western ideology, the idea of using electronic identity cards to improve the administrative tracking of the citizens, while keeping everybody under control of the state surveillance machine, seemed to be an evident policy goal.

However, the longer I examined the case, other, more interesting contextual practices revealed themselves, demonstrating surprising drivers but also institutional constraints to the innovation of the Russian electronic identity card. This thesis tracks the development of the Universal Electronic Card (UEC) initiative shortly after its inception in 2010, through 2017, when the project was officially discontinued. I document the rise of the UEC as a marketable political idea, filled with the enthusiasm and promise of government modernization and liberalization of the Russian state, and a strong G8 partner under Medvedev's presidency. I then analyse its failure to become an acceptable national identification instrument due to the growing national security and global cybersecurity concerns after Edward Snowden's leak of National Security Agency (NSA) documents in 2013, and after the institutionalization of the new Russian

sovereignty doctrine following the Russian military invasion in Ukraine and illegal occupation of Crimea in 2014. In 2022, the decision by the Russian government to invade Ukraine resulted in a full-scale war and further alienation from the global technological markets and standards through an official policy of technological sovereignty (Medvedev, 2022). The growing political, economical and technological isolation of the Russian Federation as well as mass exodus of the tech companies and specialists in reaction to the war against Ukraine, would further undermine the ability of the Russian government to implement new information and communication technologies in public administration.

I also reflect on the role of institutionalized legacies in the Russian state identification system, explaining their functions in the past and demonstrating the ways in which they reveal themselves in the case of the UEC. This thesis not only focuses on the eID as a government innovation, but also attempts to understand the commitments to a paper-based Russian bureaucracy. Why are Russians required to provide so many original documents to prove their identity and obtain government services, as the commercial (Figure 1) seems to suggest? How has this bureaucratic tradition become institutionalized and why? I argue that the historically illiberal nature of political power in Russia has shaped state identification practices, which are concerned with population control through strict administrative documentation of individual identities and movements, and this is an important element of Russian national security and state sovereignty. In Russia, freedom of movement is always a privilege, and the state identification system governs the application of this privilege through complex rules and exemptions regarding resident registration, notifications of movement, and military conscription. The institutionalization of administrative practices of the state identification system in Russia provides the means for the sovereign state to exercise coercive control over its population.

This research is concerned with the politics of technological innovation within the Russian state identification system. It is a qualitative case study of the Russian UEC, which was proposed to modernize the Russian national identification system, hierarchically organized within federal law-enforcement institutions, and manifested in the obsolescent surveillance practices of passport procedures. The UEC is an example of external innovation to modernize traditional ways of doing things within a bureaucratic "iron cage," using an internationally recognized set of tools for secure identification. My thesis therefore ponders why this modernization has failed. The project was officially cancelled by the Russian government in December, 2016 and relevant legislative changes were documented in a federal law (RF, 471-FZ). Why didn't the UEC project ever move from the pilot implementation across the Russian regions to the federal level as an official identity document? After almost a decade of federal coordination of this initiative, proposed by the President and supported by several ministries, why was it cancelled? Moreover, *what* exactly was cancelled?

Some may answer this question by pointing to political corruption, inefficient Russian bureaucracy, a lack of acceptable technological solutions, and fragmented policy structures in a vertically integrated bureaucratic system (Zherebtsov, 2016; Gritsenko & Zherebtsov, 2021). I argue that the import of an e-government solution, the Universal Electronic Card, was problematic due to the historical legacies of the Russian state identification system. Those legacies reveal themselves as important cultural and political justifications, shaping interpretations of the proposed innovations and associated concerns by key stakeholders. Some of them suggested the UEC will support traditional and modern functionalities of the Russian passport, while others questioned the appropriateness, legitimacy, and security of the proposed technological solution.

The institutionalized practices of Russian state surveillance could seemingly justify the electronic identity card system without political or public resistance, because the process of documenting citizens became an internalized social practice over centuries. As a result, the undocumented status of individuals may be perceived as a marker for social suspicion, triggering a lack of trust and reasons for exclusion or differential treatment. New technology could facilitate citizen surveillance on a scale never experienced before, where everyone would be uniquely identified, authenticated, and authorized to pass or denied entry by the click of a remote button, without even realizing that a complex set of rules and algorithms were applied to the process. While the historical legacies of the passport system could justify the implementation of more sophisticated surveillance techniques, they also determine and limit what exactly in this innovation is appropriate and what is not, shaping and legitimizing a final solution within a particular political, institutional, and legislative framework.

National identification systems are the result of a complex interaction of administrative, technological, political, and policy choices, contextualized within cultural, social, and historical circumstances (Bennett & Lyon, 2008). One of the essential findings in historical studies on identification documents is that the meaning of the documents is socially constructed through social and bureaucratic practices of documenting the legitimate citizens within the nation-state (Torpey, 2000). This cultural understanding of the process of identifying citizens within a bureaucratic apparatus requires exploration of the contextual differences and similarities of the institutionalized identification practices in different countries and in different historical periods (Caplan & Torpey, 2001; About et al., 2013).

The contemporary global development of electronic identity cards is associated with the similar processes of population management and the modernization of the state bureaucracy.

However, in terms of policymaking, the electronic identity card is very often framed in the positive language of technological progress that promises productive and efficient public administration within the framework of e-government and, moreover, claims higher citizen satisfaction from governmental services (Gore, 1993; Moe, 1994; Reddick, 2010; Amoretti & Musella, 2011; Henderson, 2017).

Many countries reforming their state bureaucracies into paperless and more efficient agencies have introduced new technological tools for identity management using web-based e-authentication, e-government services, and electronic identity cards (van Dijck & Jacobs, 2019; Manby, 2021). The most complex and all-embracing project in this respect is the multifunctional or multipurpose electronic identity card. The multifunctional card is able to support various services, both public and private, so cardholders do not need any other documents or methods to facilitate verified transactions, such as financial transactions, electronic signatures, voting, or eligibility for public service or discounts (Morgan & Parsovs, 2017).

In the case of the Russian UEC, multifunctionality was brought to a new level. Cardholders would use the UEC to apply for and receive public services or financial assistance, link the card to their banking account and use it as a banking debit card, pay for public transportation, government fees and fines, and municipal services, obtain social assistance, and visit a doctor remotely through the internet, thus avoiding time-consuming bureaucratic procedures and arguably improving accountability of public spending (PressaUecard, 2013).

Multipurpose or multifunctional cards are studied as instruments of e-government, a source for technological modernization, and whether they have a positive or negative impact on society. This thesis will examine how the *universality* of UEC modernization preserves the traditional functionality of the Russian passport. I argue that the Russian case is not about

modernizing or reforming an existing state identification system, but rather that it is about building a profit-generating business solution in collaboration with the banking sector. This public-private partnership produced a multifunctional identity instrument that would support a variety of government needs in documenting citizens, verifying their identity, and ensuring transparency and accountability of services provided to its citizens. Thus, the *universality* in the Russian case is not only targeting convenience for citizens, but also creating a promise to different governmental agencies to improve their mandates, from fiscal performance to control of citizens' movements.

This work explores the story of how the Universal Electronic Card became a policy project with a particular focus on the social construction of technology, including processes of policy justification, definition, alterations, and redefinition in response to constraining or enabling flows of ideas, events, historical legacies, and power conflicts. The UEC aimed to modernize the way citizens are documented, and use their identities in the new digital economy, but at the same time the functionality of the state identification system was not subject to modernization. What can the analysis of the social construction of technology tell us about the mechanisms of policy choices, and the prospects of technological solutions becoming a policy reality?

1.2: Research Objectives and Knowledge Contribution

There is a particular assumption in this study that the Russian case will contribute to existing research on electronic identity cards in terms of local specificity, cultural meaning, and the legacies of identification practices. In a way, the goal is to reconstruct the policy story of the UEC project based on explanatory models and theories developed in different contexts. The

electronic identity management industry promotes electronic identity cards as tools that increase the security of ICT in public administration, improve government-citizens relations, and facilitate the development of trust in government. Moreover, they promise to fix corrupt and inefficient bureaucracies in developing countries (Khan & Roy, 2019) and are often presented as tools supporting democratization (Piccolino, 201; Metcalf, 2019). But these approaches tend to ignore the shaping factors of the political regime, political culture, and attitudes towards this technology in a particular society. There is also critical Western scholarship about electronic identity cards as tools of surveillance, and this work seeks to locate the critical Russian resistance to the UEC within this tradition (Yakovleva, 2013; Tsareva, 2015).

The results of this research will contribute to the existing academic knowledge developed through relevant studies of electronic identity cards within different disciplines: public administration, political studies, and interdisciplinary social sciences. Public administration research approaches electronic identity cards as tools to reform electronic identity management in public administration and facilitate transition to a more efficient and effective government under the concept of e-government. This approach is instrumentalist and perceives identity cards as policy instruments implemented to achieve a particular social goal established by government (Bennett &Lyon, 2008, p.13; Tammpuu & Masso, 2019). For example, how does one develop a remote verification of citizens' identity using electronic identity cards, that are secure, reliable, and meeting the highest level of identity assurance requirements, while protecting privacy and confidentiality? (Belanger & Hiller, 2006; Park & Lee, 2018, Van Dijck &Jacobs, 2020;). How can e-authentication and e-government improve public services and make them cost-effective and efficient? (Ahn & Bretscheider, 2011; Domingo & Enríquez, 2018). How does this contribute to better government and the mitigation of corruption in developing countries?

(Ndou, 2004; Ojha, Palvia, Gupta, 2008, Khan & Roy, 2019; Manby, 2021). A popular theme within this approach is the exploration of e-government in the context of its democratization potential towards a more democratic, open, and transparent government, significantly decreasing levels of corruption and bribery in the delivery of services (Mistry & Jalal, 2012; Singla, 2011; Schmidt & Cohen, 2014).

Distancing itself from the instrumentalist approach, political studies aim to explain the political and institutional motivations driving the implementation of electronic identity cards in different political regimes. Bennett and Lyon (2008) observe that electronic identity cards are likely to be developed in the non-democratic countries or transitional democracies, that the reasons behind the policy implementation are ambiguous even within a particular jurisdiction, and that the structural configuration of the state and policy legacies determine the electronic identity card policy. These authors suggest a framework that covers four factors explaining why some jurisdictions have electronic national ID and others do not: (1) *political culture* is shaping popular and political opinions and justifications in respect to the adoption or opposition to eID; (2) *policy legacies* of the state identification systems explain why some Western democracies have eID and some are not even considering them; (3) technological drivers reveal the role of international high-tech companies in promoting eID for governmental needs; and (4) the structural configuration of the state suggests that *strong centralized states* have a specific interest in eID as a tool for a greater centralization and control. This literature asks “why” questions. Why do certain countries implement electronic national identity cards and others do not? Why do we need electronic and smart technologies in order to serve citizens better? What are the political drivers for this new policy solution and why do they exist? A first glimpse at the Russian policy documents (Federal Program Electronic Russia 2002-2011; Federal Program Information Society

2011-2020) reveals similar Western discourse about improving bureaucracies by utilizing e-government standards and tools. The Russian story will help to understand how such ambitious technological innovations are shaped, challenged, and eventually terminated due to the competing interests, institutional legacies, and the cultural context.

Finally, there is a more critical approach to electronic identity cards as technological tools of surveillance, which are developed to support the current distribution of power and structures of control within society (Clarke, 1988; Gandy, 2002; Lyon, 2003, 2009, 2019; Webster, 2010; Barnard-Wills, 2016; Leman-Langlois, 2012, 2018). These authors approach electronic identity cards as a manifestation of the broader theoretical issues, such as state identification, social sorting, and surveillance. Normative fundamental questions guide this tradition: What are the social consequences of these developments? When looking at the outcome, who will be a winner and who will be a loser? Will identity card systems contribute to social equality and justice, or will they be an instrument of greater social control and social exclusion? One of the common arguments in contemporary surveillance literature is about liquidity (Lyon & Bauman, 2012) and the dispersion of power and control. The state is perceived not as a leading source of surveillance, or as a Big Brother, but rather as one of the agents sharing power with corporations and other agents. However, this approach may not be constructive in attempting to understand what is happening in the Russian Federation, where the processes of nationalization and centralization interlink with the growing power of the state over the Russian corporate world. Therefore, the Russian experience can provide new interpretations of modern surveillance theories due to the post-Soviet legacies in the state identification system, the possible cultural "normalization" of surveillance practices (Wood & Webster, 2009), and the lack of privacy advocacy within a weaker civil society.

All three directions of inquiry are necessary for understanding how electronic identity cards work in public administration, why they are developed, and what are the possible social consequences of their use for the broader population, including social resistance.

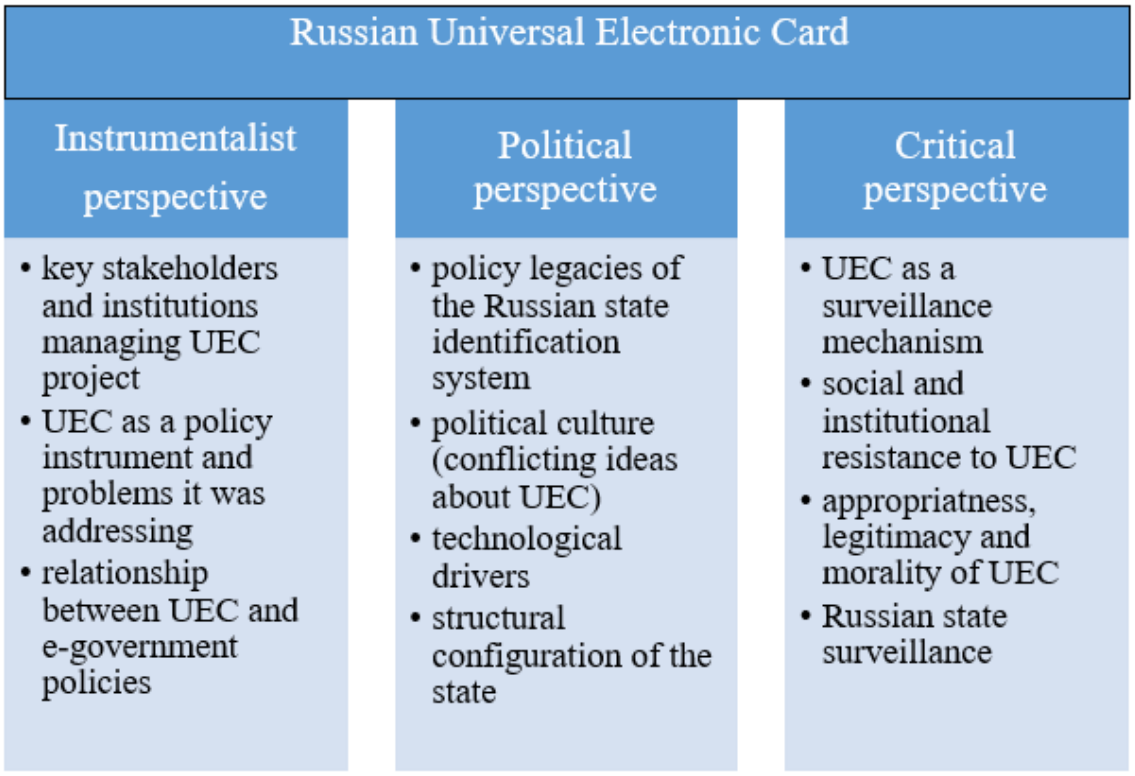


Figure 3 Qualitative Case Study Analytical Framework

Therefore, the goal of this research is to examine thoroughly and comprehensively the characteristics of the Universal Electronic Card development in the Russian Federation, to reconstruct the story of this policy instrument, and to explore the reasons behind the multi-functional technological design, the legislative and organizational framework, and the competing political interests as well as the failure of UEC to become a national identity card. The instrumentalist, political, and critical perspectives shape my analytical framework (Figure 3) and guide the exploration of the Universal Electronic Card phenomenon through these lenses, in order to reveal multiple facets of this case study and to contextualize the empirical observations.

The findings of this case study will serve as "evidence for use" (Crasnow, 2011) to further understand general processes involved in modernization of the state identification systems and, therefore, to contribute to the broader tradition of research on identity cards and state identification practices. The research methodology builds upon the broader tradition of interpretive approach in social science (Geertz, 1972; Roe, 1994; Bevir, 1999; Yanow, 2000; Bevir & Rhodes, 2012). The Russian Universal Card is not only a technological token that is driven by the logic of rationality, but it must also have specific meanings that reflect cultural, social, and political assumptions about the need and a specific role for this eID in Russian society.

The analytical framework allows me to understand how the UEC became a policy objective, including an exploration of the drivers, infrastructure, and consequences. The interpretive analysis emphasizes the importance of the contextual meaning behind the language of persuasion that is employed by policy actors. In other words, it is as important to explore how the UEC was described and talked about as a policy idea as understanding how different ideas about the UEC were expressed in policy drivers and outcomes, including regulations, organizational framework, and technological design, but also through institutional resistance. In terms of sources of information and analysis, this methodology focuses on published materials devoted to the UEC, including official government records and documents, white papers, conference materials, media propaganda, academic and professional articles, and the content of social media websites, and blogs dedicated to the subject. The methodological section in Chapter 3 will explain how several methods of interpretive analysis apply to the policy-relevant text concerning the reasons, infrastructure, and consequences of the UEC.

1.3: Outline of the Dissertation

This dissertation consists of eight chapters. Following the introductory Chapter 1, Chapter 2 **"*Three Approaches to the Study of Electronic Identity Cards: Instrumentalist, Political, and Critical"*** reviews and summarizes the existing body of literature on electronic identity cards. It discusses perspectives on electronic identity cards found in three different disciplines: public administration, political science, and interdisciplinary surveillance studies. These approaches are contrasted based on their epistemological and ontological assumptions. In the public administration literature, electronic identity cards are instruments of technological modernization within government, where implemented electronic identity card (eID) systems are supposed to improve effectiveness and efficiency of public services, enhance security of government systems, and protect personal information while facilitating the development of e-government. Political studies view electronic identity cards as tools of governance, as policy instruments implemented as a result of political negotiation and under the constraints of traditional bureaucratic practices and historical legacies. Finally, surveillance studies are engaged in a more critical approach exploring the social consequences of electronic identification systems for the population. The chapter identifies existing gaps in the literature and suggests possibilities for further research.

Informed by the findings of this chapter, the following Chapter 3: **"*Case Selection and Research Methodology"*** justifies the selection of the case, the Russian Universal Electronic Identity Card, and explains the significance of this policy analysis for the literature. It draws on the literature review and incorporates all three approaches into an interdisciplinary theoretical framework that builds on the existing knowledge and connects it with the interpretive policy

analysis perspective. Crucially, the chapter explains the case study research design, and the methods of data collection, selection, and analysis.

Chapter 4, the **"*Institutionalized Legacies of the Russian Passport System*"** reviews the historical legacies of the state identification reforms and their outcomes for Russian society. It uncovers the enduring character of the excessive bureaucratic regulation of population movement within the state that withstood changes in political regimes. The chapter concludes that the traditional function of identity documents to excessively regulate population movement within the Russian state reinvents itself as an important function supporting Russian sovereignty over its population and territory.

Chapter 5, **"*The Universal Electronic Card Implementation: Bringing the Moscow Social Card Experience to the Regions*"** describes the policy implementation process with a focus on policy justifications, the regulatory framework, technical design, and implemented smart card applications. First, the Moscow Social Card experience informs the UEC legal framework and technical infrastructure and supports the idea that Russian capital success in digitizing government and municipal services for city residents can be duplicated across regional capitals in Russia and eventually lead to the interoperability of the newly developed regional electronic identification systems. Second, leaders in the Russian financial and telecommunications industry, as well as the Ministries of Economic Development and Telecommunication, opted for the UEC public-private partnership securing significant financial contributions from the private sector, and regional budgets, while anticipating a monopoly on the newly developing market for the digital identification systems and infrastructure. The chapter concludes that the policy structure and strategy of the UEC implementation reflected the Medvedev government's attempt to advance the role and influence of economic liberals and

technocrats within the Russian state, providing multiple opportunities for new types of private-public partnerships as part of this technological modernization. In other words, the vision of the card itself and state-provided opportunities within this policy was a major driver for multiple actors to be involved in the new political and economic activities, which contributed to the development of the "Card Cartel" (Lyon, 2009) as a state-supported project to facilitate the growth of the Russian digital economy.

Chapter 6, ***"Playing the Meaning of the Russian Universal Electronic Card: Interpretive Communities and Competing Ideas"*** explores the politics of the UEC project through the analysis of conflicting views on the legitimacy of the appropriate solutions supporting modernization of the Russian state identification system and the role of the state in it. The chapter identifies four interpretive communities, acting as political factions: economic liberals, technocrats, siloviki, and traditionalists, and analyzes their views on, and interpretation of, the UEC technology, and its role in the modernization of the state identification system. The chapter argues that the UEC experiment led to the formulation of the two models of state identification system reforms. The first, *Oligopoly of the Means of Identification,* proposed market-driven solutions developed by the banking and IT industries, promising to fix multiple problems of inefficient government with the progressive technology of the electronic identity card. The second model, *State Monopoly on the Means of Identification,* while recognizing the usability of the smart card technology for state purposes, questioned the legitimacy of the proposed technological and business solutions and insisted that government should have full control, ownership, and oversight over the newly developed electronic state identification system.

Chapter 7, ***"The Fall of the Universal Electronic Identity Card and the Problem of Data Sovereignty"*** examines the tensions between those two models and suggests that the return of the state is inevitable to address the problems of data ownership, control, and access to resolve the ambiguity of the political legitimacy of the electronic identity cards developed under the influence and control of private corporations. The solution was found through attempts to establish data sovereignty, or the ability of the state to keep information about its citizens within its own legal jurisdiction and under its full control. This illustrates how government IM/IT requirements, as well as relevant data privacy and security regulations, are contextualized within the concept of state sovereignty, as an ability of the State to maintain complete and exclusive control over its territory, population, and recorded and extracted data about the population in the global information society. This political purpose to reinstate state sovereignty is a critical reason why the Russian Federation is concerned with the protection of personal information of its citizens, enforces data residency laws, and ensures that the development of the electronic passport is fully controlled, from production to the service, by government institutions. It also explains why the UEC ultimately failed.

The last Chapter 8 ***"Lessons of the Russian Universal Electronic Card Case Study"*** summarizes the findings of the research through the lens of the instrumentalist, political, and critical perspectives. The chapter outlines the main findings of the Russian case study, and explains how this knowledge contributes to existing theories and studies, while suggesting directions for further research.

Chapter 2: Three Approaches to the Study of Electronic Identity Cards: Instrumentalist, Political and Critical

2.1: Introduction

The subject of identification documents is extensive and has been studied from many perspectives and social disciplines. The scope of this dissertation is limited to the use of identity cards in public administration and public services, rather than in the private sector. The problem of identity cards in security, border control, and population cross-border movement control were also excluded from the research because this sphere is mainly regulated by international agreements and standards on traveller identification (International Civil Aviation Organization, 2006; 2013). The Russian government, based on the Soviet practice and many other post-communist governments, have maintained two identity documents: one for identification purposes within the country, and one as an international travel document. The international passport is limited only to travel purposes and cannot be used for identification within the country, due to the lack of certain identifiers recorded in the internal passport. The regulation on Passports of Citizens of the Russian Federation (Government Degree no. 828, 1997) lists additional personal information included in the internal passport: residence registration record, marital status, conscription service status, information about children under 14, and information about other identity documents. This information is regularly verified and updated when passport holders move to a different address, obtain an international passport, apply for a job, apply to a post-secondary institution, or conduct transactions requiring identity verification. Passports containing multiple and unique elements of personal identity, which are regularly verified by authorities, are central in

the Russian state identification system. The modernization of this system, a change from a paper-based document to an electronic identity card, is the focus of this research.

The objective of this chapter is to review and discuss conceptual and theoretical approaches to analyzing the electronic identity card. In order to inform a case study of the Russian Universal Electronic Card, I explore similar case studies in different jurisdictions, as well as comparative research and research within different disciplines, particularly focusing on policy definition and justification, and policy implementation, including organizational and infrastructural developments and critical assessments of the political implications. Because this work follows an interpretive tradition in policy analysis (Yanow, 2000; Hendriks, 2007; Wagenaar, 2011), the crucial objective of the literature review is to identify different assumptions about the research object – an electronic identity card – and to explore the implications of these assumptions for research outcomes. Existing knowledge on relevant concepts and their operationalization has guided my selection of primary sources and the analysis of these documents. I have organized the literature into three categories: instrumentalist, political, and critical.

2.2: The Electronic Identity Card as an Instrument of E-government

There is an abundance of specialized policy studies, conference research papers, industry publications, and public administration literature focusing on the electronic identity card as a technological instrument. According to this literature, electronic identity cards can solve the problems of ineffective governments and streamline government services for people (Gore, 1993; Moe, 1994; Reddick, 2010; Amoretti & Musella, 2011; Henderson, 2017), while also facilitating information and communication technology (ICT) reforms (Cambell, 2012;

Hollands, 2008; Lytras & Visvizi, 2019). These authors share certain uncontested assumptions reflecting a technocratic worldview, linked to the inevitability of technological progress and to the objectivity of technology in relation to society, as an independent phenomenon insulated from social, cultural, and political circumstances. Electronic identity cards are not viewed as categories that are socially or politically problematic. The electronic identity card is regarded as an apolitical instrument, and when applied according to the outlined technical and procedural principles and standards, should lead to a social change, solving problems of ineffective governments, while minimizing security risks, protecting privacy, and improving public service delivery (Dunleavy et al., 2006; Ashbourn, 2011; Birch, 2016). These assumptions are generated at the level of the digital identity industries and supporting technological sector (Windley, 2005; Mayes, 2017), and popularized by the telecommunication and financial sectors (Rankl & Effing, 2010; Sullivan, 2008, 2018), offering solutions for secure on-line identity management systems. Finally, these uncontested assumptions about electronic ID are universalized within E-government policy-oriented research, dedicated to the conceptualization of the "one-size-fits-all" ready-to-implement technological "best practices" for public administration around the world, and in any political regime (Gelb & Clark 2013; Gelb & Metz, 2018).

The subject of eID can be found in a significant body of public administration literature devoted to electronic government. It is discussed within a narrow group of studies associated with electronic service provision (Lips et al., 2009; Axelsson & Melin, 2013; Lentner & Parycek, 2016), identity management (Bertino & Takahashi, 2010; Birch & McEvoy, 2016), e-authentication (Garson, 2006; Modi, 2011; Allen & Pickup, 2016), and data interoperability (Backhouse, 2006; Leitold, 2010; Novakouski & Lewis, 2012). Contrary to political theories

of state identification practices, the public administration literature typically does not analyze identity cards as a system of control over the population, but rather as a tool that will enable the more efficient functioning of public administration. However, this approach is also concerned with the problems of privacy, data security, and the trust of citizens in e-government systems.

This section will focus on several areas of knowledge contribution associated with the application of electronic identity cards in public administration. This will be done in two steps: first, through an analysis of how digital identity management is informing the adoption of electronic identity cards in government to enable a secure verification of citizens online, while supporting interoperability of solutions across different government systems without compromising individual privacy; and second, through an analysis of how the development of e-government has enabled the implementation of electronic identity cards in the public sector through the influence of e-commerce innovations, and the promotion of smart cards for the provision of a variety of municipal services.

2.2.1: The Evolution of the E-government Concept

Studies on e-government emphasize the evolution of the practical institutionalization of internet-based technologies in public administration. It seems that the great promise of the internet in the late 1990s to democratize the state-citizen relationship and to change the face of bureaucracy (Milward & Snyder, 1996; Lawson, 1998; Wimmer & Traunmuller, 2000) was transformed at the level of policy implementation in the 2000s, and focused instead on technological problems, solutions and practical applications (Gronlund & Horan, 2005; Chen, 2007; Reddick, 2010). The normative democratic vision has shifted to practical implications – to

provide public services to citizens through the internet; in other words, “to reassume the role of citizens as clients and users of the improvement in the quality and efficiency of the administrative machines” (Maria & Micelli, 2005). Starting mid-2010, the term “e-government” began to be mentioned in the literature, as well as within government programs, along with a similar term: “digital government” (Bannister and Connolly, 2012; Janowski, 2015). Digital government amplifies the need for government not only to rely more on technology to improve citizens services, but also to ensure that technologically designed services are user-centered, iterated frequently as technology progresses, and employ software solutions that are open-sourced, cloud-ready, and subject to safeguards protecting personal data, human rights, and public trust (Digital Nations Charter, 2014).

E-government is seen as a tool to re-invent the state, to facilitate the transition from traditional vertical hierarchical structures of the classical Weberian bureaucracy to the integration of all management links and designing a “single point of entry,” or as Tambouris and Wimmer (2005) define it, “a single window for citizens applying to government services through a single point of access using the communication channel of their choice: citizen center, call center, web site or mobile application” (p. 116). Furthermore, information and communication technology (ICT) enables government officials to provide more lean services while using fewer resources, or “do more with less” (Janssen & Estevez, 2013), while drastically reducing the distance between them and citizens, and optimizing government spending. The goal to make government more cost-efficient and effective by using ICT tools is associated with the movement toward the New Public Management (NPM), concerned with the creation of the “Slim State” through “Slim Management” (Cordelia, 2007) and breaking down administrative silos with a “joined-up government” (Hood, 2005). Over time, the concept of e-government extended

to include social and political outcomes, cost-efficiencies, new values of public trust, fairness and legitimacy of government institutions (Cordella & Bonina, 2012), development, improvement of public service and participation, digital skills, and innovations (Pang et al., 2014).

Initially, the role of ICT in public administration was seen as a tool to reinvent the government and fix an old and inefficient bureaucracy. This would be done by integrating electronic technologies of information exchange, developed in e-commerce in order to improve the quality of these services, and consequently to manage government as efficiently as a business (Schedler & Scharf, 2001; Schuppan, 2009). To achieve this, as identified by Dunleavy et al. (2006), New Public Management (NPM) reforms aimed to restructure traditional bureaucratic hierarchy through *disaggregation* of public service provisions outside of vertical hierarchy, by decentralizing and increasing the autonomy of its individual connections. Certain government functions would be contracted out to private sector and non-profit organizations, thus strengthening its focus on citizens as consumers (p. 470). This would facilitate *competition* in service delivery, while at the same time rewarding public servant performance and offering *incentivization* for contracting out and disaggregating further program delivery (p. 473).

For example, in the 2000s, one of the reforms in post-Communist administrations within European member-states was the transfer of the national identification system and driver licensing from national police to the service centers operated by either municipal bodies, or by the private sector. Service centers would operate as a one-stop shop for government services (Kubicek & Hagen, 2000), while being located closest to the citizens, in their municipalities. The services would include issuance of national IDs, driver licencing and license plates, municipal and social services, and applications for social assistance or a business permit.

I witnessed the practical realization of this modernization policy during my work as an interpreter for a non-profit organization in Poland. Between 2005-2008, I visited many municipal authorities with groups of public officials from Ukraine to see the one-stop shops supporting citizens cervices. The process was digitized as much as possible, leaving the collection of witnessed signatures and the verification of identity to the front-line staff. The performance of the centers was measured based on customer wait-times, number of processed requests, and number of issued documents, and then ranked against other centres. Highly performing clerks and managers were encouraged to learn all lines of service and were rewarded accordingly. Although the performance depended on the location of the service and population volume, the overall outcome was a more efficient management of identity documents (Study Tours to Poland, 2008).

One of the unintended consequences of NPM reforms was the complexity of governing, controlling, and overseeing multiple private organizations delivering public services. Reporting structure, legitimacy, and the issue of the public nature of services became problematic (Cordella & Bonina, 2012). In response to the identified problems and increased number of informational and departmental silos within government, the role of the ICT innovations in supporting integration and collaboration between different departments became prominent – i.e. "joined-up" government. Hood (2005) refers to "joined-up" government, implemented by Tony Blairs' New Labour Government in the 1990s, as an old principle of coordinated public administration where "many parts of executive government should interconnect, complement one another, and pool related information" (p. 19). As Dunleavy et al. (2006) explain, digital innovations under the policy goal of "joined-up" government will address the problems associated with NPM's competition and outsourcing with *reintegration* of processes and collaboration for the purpose of

service delivery. Instead of competition, the focus would be on the needs of users (*needs-based holism*), and departments will work collaboratively with users of their services to develop one-stop shops (Dunleavy & Margetts, 2013).

The timely and accurate information availability and secure systems, permitting an instant exchange of information, become an important factor supporting such coordination. But the challenge is controlling information-sharing between departments governed by different mandates, authorities, and regulatory requirements, and competing for funding from the government budget. The critical role of ICT tools is to enable the reintegration of complex informational systems based on the secure collection, sharing, and retention of current and authentic information on citizens.

A key role in the integration process is performed by information technology, which allows government officials to provide more services with less effort, while drastically reducing the distance between them and citizens. Within this new concept, the electronic identification of citizens is supposed to reduce data duplication within the government, continuously provide original data supporting evidence-based policymaking, facilitate cooperation across levels of government, focus on the convenience of electronic identity cards for public service clients, and support the development of automated processes based on the new types of electronic data available.

There is also a different trend that theoretically locates “e-government” within the “good governance” movement, due to its potential to mitigate corruption in public administration by removing the human factor from procedural decision-making, impartially supported with online service delivery (Ndou, 2004; Ojha, Palvia, Gupta, 2008; Bannister & Connolly, 2014; Manby, 2021). E-government is supposed to increase the effectiveness and efficiency of public

institutions by providing services faster and with fewer resources, thus facilitating the growth of citizen confidence and public trust in government (West, 2004; Andersson & Twizeyimana, 2019; Benay, 2018; Roy, 2020). Subsequently, a more responsive and accessible digital government builds public trust in government decision-making (Welch & Moon 2005; Tolbert & Mossberger, 2006; Cordella & Bonina, 2012). It is supposed to create "public value," in addition to saving resources.

A significant influence on this academic literature are the criteria and metrics established by international organizations. For example, a national questionnaire was distributed among United Nations member states and affiliated experts to measure the E-Government Development Index based on scope and quality of online services, telecommunication infrastructure, and human capital (UN E-Government Survey, 2003-2020). The Organization for Economic Co-Operation and Development (OECD) has funded a significant amount of research on e-government initiatives in a global context in the 2000s, but recently has shifted to the term of digital government (OECD, 2019). The trend emphasizes the role of technological innovation in adopting a "digital by design" approach (p. 6), impacting not only online service delivery but calling for the re-engineering of public processes and creating data-driven and evidence-based public policies, while at the same time calling for user-driven input to public services (OECD, 2020).

The reports and studies funded by international organizations on e-government and digital government have been focused on the practical policy recommendations – i.e. achieving certain standards of digitizing government services and processes of self-assessment in relation to those standards. As a result, the nation state can be ranked higher or lower among global digital leaders or early developers. Some non-democratic states, including the Russian

Federation and Saudi Arabia, have utilized proposed instruments of digital innovations as a more politically and culturally acceptable way of reforming government institutions, and have participated in international competition with established democracies to demonstrate modernity and legitimacy to the international community (Maerz, 2016).

2.2.2: The Expansion of Smart Cards from E-commerce

Second, the electronic identity card concept does not represent a recent development of state identification practices, but rather illustrates the adoption of smart card technology used in e-commerce, as a process of government reengineering (Gore, 1993). Just as ATMs, plastic credit cards, and national networks made banks more convenient, e-government is supposed to make interacting with the state easier and faster (Moe, 1994). Practically, the goal is to reduce transaction costs as much as possible. A smart card is a plastic card with embedded technology that allows for automated electronic transactions, and can store data securely and run several algorithms and functions (Mayes, 2007).

Research on smart card development emphasizes the role of plastic cards in the banking industry, where Visa and MasterCard were pioneers in advancing technological possibilities of electronic transactions by means of smart identity cards with embedded micro-chips (Rankl & Effing, 2010). According to Rankl and Effing (p. 15), smart card inventions in the banking and telecommunicating industries in the United States, France, and Germany have produced a product desirable in many areas of society due to the high level of security available to everyone, since it could safely store secret keys and execute cryptographic algorithms.

The influence of e-commerce innovations on e-government has also shaped the language of public service delivery reforms. Otenyo and Lind (2011) identify a trend in e-government

studies that borrows terminology from the banking industry: citizens become clients, and their relationship with e-government is simplified to the levels of electronic transaction and client satisfaction. This “e-commerce” language reinforces the influence of private sector ideas in public administration and, moreover, emphasises the building of an “E-service society” with emphasis on the economic values of transactions between consumers and organizations (Lamersdorf et al., 2004).

There is also a significant trend of the banking industry *participating* in the development and implementation of national electronic identity schemes that promote e-banking applications. In 2014, the European Union implemented a regulation on electronic identification and digital services for electronic transactions in internal markets (European Commission, 2018). This provided for cooperation between the member states in recognizing digital identity systems and ensuring digital interoperability of the electronic identity cards across the EU. Under this framework, member states are encouraged to leverage banking instruments (electronic identity verification systems) for implementing national identity cards. The list of countries that have implemented eID cards with e-banking applications and a micro-chip supporting digital signatures include Austria, Belgium, Estonia, Finland, Germany, Italy, Liechtenstein, Lithuania, Portugal, and Spain (European Commission, 2021).

While in the European Union the e-banking application allows the use of the ID card for authentication purposes online, Russian policy-makers were eager to create a national payment system based on the national universal electronic card that would eliminate credit card competitors from the market (UEC press release, 2014; The Moscow Times, 2016). In practice, language and technology from e-commerce have influenced the use of smart cards in e-

government. There is also a trend in local and welfare politics to facilitate smart eID implementation.

Third, smart electronic identity cards are rarely implemented centrally and hierarchically as a national and comprehensive electronic identification document. The exception would be Estonia, a European Union member state that effectively rebranded its own name to E-stonia to reflect the extensive digital modernization undertaken there since 1997. This relatively small EU state, with a population of 1.3 million and a centralized government, has invested in the expansion of internet networks and has established paperless principles in public administration, effectively transforming a Communist system into a digital democracy (Runnel et al., 2009). The Estonian eID system relies on a unique personal identification code (PIC), and supports functionality of the digital signature allowing cardholders to access government services online (Henderson, 2016). The Estonian model supports interoperability of data contained in over 350 government systems and databases via "X-Road" decentralized linkages, a technological integration providing secure information sharing between different agencies and departments to support the provision of government services to citizens (Goede, 2019).

Elsewhere, the trend of electronic identification card distribution is found more often in municipalities. Many cities implement smart cards to improve social service delivery to city residents. This locally driven process is often embraced by the "smart city" concept and explains how ICT technologies are changing municipal governance and residents' lives (Cambell, 2012; Hollands, 2008; Lytras & Visvizi, 2019). For example, multifunctional local smart cards in the UK allow residents to conduct recreation and public transport transactions (Deakin, 2013). In Russia, the Moscow Resident Card was designed to support local residents, who qualified for social assistance, before it became a prototype for the national electronic universal card. Many

national electronic identity cards in the European Union were implemented first at the municipal level as pilot projects (Leitold & Zwattendorfer, 2011; Rebeiro et al., 2018), allowing cardholders to pay with a national e-ID for their parking, a bus ride, or access free Wi-Fi across the city.

Given the symbolic importance of information technology in modern culture as the embodiment of technical and, consequently, social progress, the popularity of the concept of "electronic government" is not surprising. The introduction of information technology not only generates confidence in the possibility of more rational decision-making, but also creates the basis for additional rational legitimization of the public administration system, as advanced, modern, and corresponding to the needs of society, free from political constraints and agendas. The banking and smart card industries offered electronic identity cards as a solution to electronic government, expanding their markets. With a technological token that provides a high assurance of the cardholder's identity, the transactional nature of banking made its way to government. This new practice required new types of studies to address the secure and effective management of new types of electronic identities and information.

2.2.3: The Electronic Identity Card (eID) as an Instrument of Digital Identity Management

The eID as a mechanism for secure e-authentication in e-government systems appears in a vast range of public administration and policy analysis literature. There is a need to clarify some definitions, such as e-government, e-authentication, and identity management, before outlining the central claims found in this literature. The process of accessing services through the internet requires mechanisms that can determine that the user is the right person for a particular service. This mechanism is referred to as the process of *e-authentication* (Garson, 2006). The

system does not need to know who the person is; rather, it only needs to know whether the person knows a unique identifier (set of numbers, login) and a password, and is therefore authorized to complete a transaction or access the system. A multifactor e-authentication involves other factors. For example, something the person has (electronic identity card) or something the person is, a unique biological characteristic of the person or biometrics (electronic identity card with a facial recognition technology or fingerprints). E-authentication is not equivalent to the process of *identification*, where a particular person is required to provide proof of his or her identity. However, e-authentication is a part of the broader concept of *electronic identity management* that is a "process of identifying individuals and controlling access to resources based on their associated privileges" (Modi, 2011, p. 1). Ashbourn (2011, p. 39) defines identity management as a process of "knowing objectives and considering mechanisms by which we aim to create, store, and subsequently verify an identity."

Identity management is based on the assumption that citizens' identity in their files is regulated by the government, meaning the government will decide what personal information should be gathered and maintained by the bureaucratic agencies. However, the public administration literature typically does not view the existence of governmental databases on citizens as problematic. The major concern is the quality of the information in the databases, its availability, and confidentiality. Therefore, electronic identity management is presented as a tool to protect data security and to avoid duplications in data entries (Dunleavy et al., 2006; Ashbourn, 2011; Birch, 2016). The principal assumption is that data collection, use, and disclosure by government is not being subjected to different interpretations or discretionary decision-making, but is rather limited by legal framework, policies, and standards. The focus is on the security controls supporting availability, integrity, and confidentiality of data in the

control and custody of the government. In this context, personal information is just another type of confidential information.

Electronic or digital identity management analysis is viewed in the public administration literature through the narrow perspective of electronic design and implementation and tends not to be concerned with the legacies of identification systems (Lips, 2010). Discussions surrounding identity management tend to concentrate on comparing the identity of a particular person with the digital information about that person that exists in the system, with the goal of electronic authentication and the decision to provide/deny services or treatment. Identity management can be based on the use of logins and passwords, a public key infrastructure (that involves cryptography and security certificates), smart cards, electronic identity cards, and/or biometrics. The problem that electronic identity management is trying to address is assurance that individuals are indeed who they claim to be. Historically, the verification of identity claims was always a problem for bureaucratic systems. The claim of identity on the internet, where the risk of identity fraud is rather high, requires multi-factor authentication methods. There is a strong opinion in the literature and among industry experts that the process of e-authentication would be more secure, faster, and easier if it were conducted through smart identity cards, as an instrument supporting multifactor e-authentication and providing a higher level of identity assurance (Fioravanti & Nardelli in eds. Chen, 2008; Birch, 2017).

Electronic identity management also includes control over the personal information that is gathered and maintained by governmental agencies. Before the digital revolution, bureaucratic institutions in most countries controlled and managed their own system of files and databases. To confront the problem of government “silos,” or a fragmentation of informational resources along institutional divisions, electronic identity management also led to the development of policy

ideas like personal data interoperability (Backhouse, 2006), “joined-up” government (Raab, 2005; Dunleavy & Margetts, 2013), and automated public decision-making (Cobbe, 2019). Although data interoperability is presented as a positive development that improves the effectiveness of government processes through information-sharing and limiting the duplication of data, contrary views state that data sharing may violate privacy laws and create risks to individuals or marginalized social groups. This could be the case when personal information, collected for the purpose of providing one government service, is shared with a different government agency for a new purpose and without the knowledge or consent of the individual (Novakouski & Lewis, 2012; Best & Pane, 2018). Some authors suggest that the logic of bureaucratic interest in reducing welfare fraud tends to override privacy safeguards in practice and, moreover, is reinforced with the new policies of sharing data horizontally across the government, for the purpose of identifying people who are not providing full information or lying on their applications (Anderson et al., 2009). Additionally, electronic processing of the personal and sensitive data through the interconnected databases requires network connections, which may be subject to the internet hacker’s attacks. Cybersecurity experts (Annual Vancouver International Privacy & Security Summit, 2022) warn that the risk of hackers’ attacks on the government information systems is increasing with digital modernization, and without proper security controls, malicious actors may cause significant financial or reputational harms for organizations and impacted individuals.

Another reason to reduce bureaucratic barriers to the flow of information between departments is to reduce the duplication of identity verification processes each time the individual applies for a public service. Electronic identity cards can be a source of citizen information that can be transmitted and processed automatically without human intervention,

thus saving on administrative verification procedures. However, there is a privacy concern with the secondary use of information that was collected indirectly from a different department without the knowledge of the client. Privacy protection regulations in developed democracies guarantee to individuals that their personal information is collected, used, and disclosed only for a legitimate purpose and with their full knowledge or consent, when necessary (Solove, 2008)

The dual goal of electronic identity management, to gather and maintain relevant identity information as well as to control the process of lawful access to public services through authentication mechanisms, can be attained with the use of the electronic identity card. The smart identity card is not only an instrument of online authentication, but also an informing or "detecting" tool about the online activities of the card holder (Hood & Margett, 2007).

There is also another side to the story: electronic identity card development is associated with the *new methods of information manipulation*. It is not just personal information anymore; it is also raw aggregated data about the population in an electronic format — easy to access, to share, and to analyze statistically. New trends in identity management emphasize the growing need for data interoperability between different government agencies, and the need to address the challenges of this development (Otjacques, Hitzelberger, Feltz, 2007; Scholl, Klischewski, 2007).

More critically oriented public administration researchers identify smart identity cards as a manifestation of the digitization process in bureaucracy, enabling algorithmic surveillance of the population (Graham & Wood, 2007). Overall, however, the electronic identity literature and data interoperability literature view electronic identity cards as a technological opportunity to improve public service delivery, provide secure online access to government services, and

maintain the quality and history of changes in personal information of citizens in government databases.

The subject of e-government corresponds to a broad and diverse area of study. I have tried to identify studies and conceptual influences that serve as the rationalization for electronic identity card implementation within e-government. First, the digital revolution in public services calls for technologies that intensify online relations, but also improve data protection with appropriate security controls. Second, the successful history of smart cards in the banking industry offers a glimpse into what the relationship between citizens and government can look like, in terms of service delivery. Third, the growing popularity of smart cities shows the positive effect that electronic identity cards have on municipal service delivery. All these developments show that smart card technology is a tool for the new, technologically advanced state.

The problem is that the introduction of the smart identity card will require significant changes in terms of government reforms, including changes in legislation, investments in infrastructure, and more spending on security. More importantly, when so many changes have to be implemented, it would be irrational to use the smart card solely for the purpose of e-authentication. Therefore, smart cards, when they are implemented, tend to grow in both function and application to address the different needs of citizens and governments, and they can then become the basis for a new bureaucratic architecture.

2.3: The Politics of Electronic Identity Cards

There are a number of studies dedicated to the development of the electronic identity cards as policy solutions in different jurisdictions. These studies explore the drivers of electronic identity cards and reveal variations in the political justification for their implementation within

different societies. This perspective brings our attention to the importance of the political regime, political culture, and historical practices of the national identification systems. The variation of interpretations of meaning of the ID card as an enabling, detecting or controlling policy instrument reflects circumstances and values that support the system of national identification. An electronic identity card is a tool of governance developed within bounded rationality, depending on the existing practices and the political regime. It can be more or less invasive, industry-based, or government-led. Contrary to the neutral and apolitical examination of the smart identity card as a material technological object within the e-government literature, political studies focus on the governmental and social practices associated with the implementation of identity cards. The politics around identity cards is a highly problematic area due to power struggles. Political researchers ask "why" questions: Why do certain countries implement electronic national identity cards and others do not? What are the political drivers and motivations for this new policy solution and why do they exist? Why is there political opposition and social resistance to identity cards in some jurisdictions, while in others this new technology is being developed and implemented with an overwhelming level of popular support?

This literature tends to approach the identity card is as a policy tool —which is used to reach certain policy goals but also to respond to social problems (Hood & Margetts, 2007). Authors espousing this view argue that the electronic identity card can be used for different purposes, depending on the political system and the institutionalized practices of governing. In this case, the choice of the eID would not be a rational policy decision, but rather a reflection of historical, cultural, and institutional conditions in the particular country, or of the structural configuration of the state (Bennett & Lyon, 2009).

This section of the literature review will cover three approaches to identity cards, formulated as a result of the examination of case studies across the globe. On the one hand, electronic identity cards in Mexico, India, Brazil, Saudi Arabia, and Turkey were implemented under modernization slogans with high levels of popular support. These cases are critically viewed by researchers as a modernizing project, where electronic identity cards and technology are used to reinforce the central hierarchical power of the modern nation state. In the EU, on the other hand, the adoption of eID by Germany, Austria, Belgium, Italy, Portugal, Finland, and other member states can be explained partially due to their political legacies but also due to the political economy of technological development, the growing influence of technological industries, and the reinforcement of networking governance under neo-liberal reforms. Finally, I will discuss the literature on identity cards in Canada, the United States, Australia, and the United Kingdom, where identity cards have been strongly resisted.

2.3.1: eID as a Modernization Project in the Global South

Case studies of electronic identity card deployment in a number of countries in the Global South reveal intriguing similarities across cases, including use of eID with biometrics to prevent crime and fraud (Wilson, 2006; Gelb & Clark, 2013), developmental and modernization rhetoric associated with eID solutions, and the centralization of government and increased state control over certain populations (Wilson, 2013).

For example, in a comparative analysis of the transition to e-government in Jordan, Ethiopia, and Fiji, the authors confidently discussed the high anti-corruption potential of e-government (Pathak et al., 2010), even though the required infrastructure was not available in these countries, and the state information resources were of poor quality. Many citizens had low

computer literacy skills, did not have access to affordable internet, or were poorly informed about the possibility of interacting with authorities in electronic form (p. 12). The political situation was characterized by a high level of instability, preventing effective planning. Although there were practically no conditions for a "revolution in management" through the introduction of information technology in the analyzed countries, this did not prevent the authors from being optimistic and recommending the widespread use of marketing technologies as the main recipe for success, in order to "promote" the benefits of e-government to citizens.

International experts and organizations (World Bank Group, ID4D) have also targeted poorer countries with expensive but seemingly depoliticized electronic identity card schemes with extensive biometric features as a solution to poverty, without questioning the legitimacy of such solutions within the context of existing state identification practices. The mandate of these international organizations is to provide financial aid to people in these fragile or failed states, where governments no longer function properly and are unable to provide public services. To ensure that financial aid can reach those who need it most, international development organizations propose new identification schemes. Developmental researchers see electronic identity cards as progressive and something that can improve the access of poor people to social services, therefore reducing poverty (Gelb & Clark, 2013; Gelb & Metz, 2018). These authors suggest that identification should be considered an element of development policy (p. 52), claiming that state surveillance is not an issue in developing countries, and pointing to Western democracies where governments are more focused on security issues and terrorism prevention.

Critical political studies identify the rhetoric of modernization that reinforces the centralization of state control, and the need for stronger systems of citizen identification. For example, electronic national identity cards are presented by the Turkish government as part of

modern life and a demonstration of the Europeanization processes supported by the government (Bozbeyoglu, 2011). The author also identifies factors that increase state control over citizens through central databases containing the religious affiliations and ethnicity of citizens. Another example of the Mexican "more modern" biometric identity card is researched by Velez (2012). His findings emphasize that policy development was based on assumptions that biometrics are effective in the war on crime, but he is cautious about the increase of state control over individuals, where everybody is under suspicion. In Brazil, the government justifies the new eID as modernization and national coordination in the name of fraud prevention, and the promotion of citizenship paired with the growing number of centralized and interlinked digital databases (Kanashiro & Doneda, 2012). In India, the national identity card (Aadhaar card) scheme has increased access to social services for a significant amount of the population due to the legitimization of an individuals' existence through new identification policies (Yadav, 2013). However, extensive biometric projects will likely lead to more violations of citizens' freedoms and liberties (Ramakumar, 2010; Oduro-Marfo, 2021).

These technological developments in countries with high social inequality and few civil liberties may lead to a situation where governments will predominantly use smart national identity cards for the purpose of more centralized state control. Moreover, this process, in some cases, is encouraged by the United States and the United Kingdom within the Gulf Cooperation Project, the North American Free Trade Agreement, and other instruments of international agreements about border security and the prevention of terrorism (Bozbeyoglu, 2011). The international support for electronic identification of the poor and of residents of "terrorists' territories" is troubling, especially while many developed democracies consider national identity card solutions "as unacceptable extensions of state surveillance" (Lyon & Bennett, 2008, p. 14).

Additionally, the international popularity of electronic identity cards and digital modernization of government has generated a new wave of global development, a movement of experts, expert literature, and expert organizations devoted to the problem of adapting the state to a technological society. This includes influential international organizations (UN, World Bank), global experts in the field of management and information technology (consulting companies such as Accenture, Gartner, Capgemini), as well as multinational IT corporations offering specific (and often very expensive) solutions designed to revolutionize the system of government management, and methods of secure online authentication of client-citizens (such as IBM, Microsoft, HP, Cisco).

The fact that the United Nations Department of Economic and Social Development has begun monitoring the readiness of countries around the world for its development since 2001 has also shown that the e-government concept has acquired international status. Every two years, an international e-government rating is published, based on an analysis of national state portals (and taking into account a number of statistical indicators, such as the level of internet penetration and the number of citizens who have received secondary and higher education). National governments are encouraged to use this rating if they want to comply with UN requirements and apply for funds (Whitemore, 2012).

2.3.2: eID and Digital Economy in Europe

While case studies on electronic identification in the Global South share similar explanatory factors of modernization and developmental theories, the research on eID schemes in European member states is focused on the categories of the politics of Europeanization, markets and population mobility, and the expansion of information and telecommunication

technologies. There are 15 EU member states out of 27 that already have national electronic identity card solutions (European Commission, 2021). However, the eID national schemes that have been developed so far are different on many levels and in many respects (Leitold & Posch, 2012). This problem of national variation is addressed by the European Commission through the project “Digital Agenda for Europe” with the goal “to reboot Europe's economy and help Europe's citizens and businesses to get the most out of digital technologies” (DAE, 2014).

One of the goals of the Digital Agenda for Europe is European interoperability of e-government services and mutual recognition of the e-ID by member states. The e-Government as a project refers to digitally available public services provided by member states to all European citizens. It is not a description of the supranational institutional arrangements but rather the collection of open and flexible public services accessible electronically according to unified principles and technological standards (Amoretti & Musella, 2011). It is a new direction in the politics of Europeanization, that is defined as an “institutionalisation of formal and informal rules, procedures, policy paradigms, styles, ‘ways of doing things’ which are first defined and consolidated in the making of EU decisions and then incorporated in the logic of domestic discourse, identities, political structures and public policies” (Radaelli, 2003, p. 30). Through the politics of Europeanization, the European Commission outlines the advantages of Pan-European electronic identification management (eIDM) in facilitating cross-border interoperability of personal data, and promotes national electronic identity card developments in member states.

Pan European eIDM will coordinate the coexistence of different national systems of electronic identities and allow identity cardholders to access public services anywhere in the European Union. The main objective of borderless identity management is to establish “the readability and exchangeability of user data, both locally (i.e. directly from a token) and at a

distance (i.e. by relying on national authentic sources if they are not stored on a token), within the scope of existing data protection regulations" (Pan-European eIDM Framework, 2006). This data interoperability will allow citizens and businesses to benefit from the growing single digital market, improve citizens' mobility, and contribute to the development of e-government without borders. A more recent development is targeting interoperability of the national identity schemes across the European Union through a new European Interoperability Network (European Commission, 2017). Since 2019, due to the eIDAS regulation, citizens of Germany, Italy, Estonia, Spain, Croatia and Luxembourg can use their national electronic identity cards to cross borders and to access European online services (European Commission, 2019).

However, there is also significant influence from the private sector. For example, electronic and technological industries advocate for the popularization of new technological products for public administration. The cost of identity management based on an identity card system is high, and there is not only the cost of implementation, but also the cost of maintenance and data security. Therefore, the more complex the identity card's design, the more elaborate and expensive is the infrastructure required. This is clearly a new market development; Lyon refers to this new type of relationship between government and high-tech companies as a "Card Cartel" (Lyon & Bennett, 2007; Lyon & Topak, 2013).

The growing role of high-tech industries in European public administration encourages new types of policy advisers who have expertise in technological solutions. Experts from various industries advise politicians and public officials on the advantages of the particular technological solution, but in reality, they facilitate the promotion of particular products. Also, their unique knowledge and skills allow them to become an exclusive epistemic policy community (Yanow, 2015), providing advice that goes beyond their expertise; for example, advising on new public

policy directions (Horrocks, 2009). As a result of these developments, high-tech companies prosper in the growing market of electronic identification. What is more, they are the first to identify growing probabilities of personal data breaches and therefore advocate for higher and more expensive levels of data security and privacy protection, for which governments cover the costs (Porcedda, 2018). In terms of the political economy, the European Commission's Digital Agenda for Europe is the best strategy to nurture those public-private relations that do not solve any particular social or economic problem, but instead focus on the creation of markets for expensive technologies.

The main differences in electronic identity card development in the EU compared to countries in the Global South include: a focus on supranational standards in electronic identity management; an emphasis on market development in terms of growing citizen mobility; and economic growth linked to digital technologies and professions rather than developmental politics and state modernization. There are also studies on the implications of European electronic identity cards for privacy, data security, and citizens' trust (De Hert, 2008; Neumann, 2012; Seltsikas & O'Keefe, 2010). Overall, the idea of electronic identification is not criticized as a wrong policy tool in Europe; instead, researchers focus on identifying problems and issues with the technology itself that require public attention and debate.

2.3.3: eID Resistance Movements

Finally, there is an area of literature concerned with the development of popular resistance and democratic opposition to electronic identity card schemes around the world. Democratic opposition to electronic identity cards has been well organized in some Western democracies (and particularly in the common law countries such as the United States, Australia,

Great Britain, and Canada). This resistance has a long history in America and Great Britain and has focussed on the economic costs and the larger risks to privacy (Wills, 2008).

Governmental attempts to introduce national identity cards have been viewed as an enormous intrusion into the private lives of citizens, and labelled as a dangerous bureaucratic initiative to gather and maintain information on every citizen from "cradle to grave" or "womb-to-tomb" (Packard, 1964; Warner & Stone, 1970; Campbell & Connor, 1986). Froomkin (2009) suggests that the development of popular resistance to identity cards is associated with the common-law countries (United Kingdom, United States, Canada, Australia) due to the romantic idea of free movement as opposed to a culture of travel documents in civil law countries (Europe, Russia). Most common-law countries have, at some point, had policy discussions about national identity cards, but those projects have failed under pressure from political opposition and civil society resistance.

The Australian "Access Card" was a short-lived electronic identity card project, terminated in 2007, which was widely criticized as an invasion into privacy, containing unlimited technological ability to be utilized for a wide range of purposes, including discrimination and social sorting (Wilson, 2008). The United Kingdom identity card scheme from 2006 was subject to similar public and political criticism, focusing on the lack of pragmatism in expensive technological solutions to unspecified problems, as well as dangers of new forms of social control, potentially eroding public trust and confidence in government (Wills, 2008). In 2010, The Identity Document Act was passed, reversing the introduction of identity cards in the UK and requiring destruction of the information from the National Identity Register (Beynon-Davies, 2011).

In Canada, policy discussions about national ID schemes never resulted in an official federal project due to the complexities associated with legislating technology of electronic identity cards and requirements of the multi-jurisdictional negotiations (Clement et al., 2008). As a result, only some Canadian provinces slowly implemented electronic identity card schemes. For example, the BC Services Card (BCSC) combines information about driver licensing managed by the Insurance Corporation of BC (ICBC) and a citizen's Medical Service Plan number, managed by the Ministry of Health (Parsons & Molnar, 2013). The BCSC model relies on individual consent to combine a driver's license and MSP number in one card, and to share information included in the card with other government departments when applying for government services online (gov.bc.ca/bcservicescard). However, at the federal level, Canada maintains a more pragmatic approach, supporting online authentication of citizens by any of the trusted identity providers or credential brokers, for example online banking credentials (Sign-In Partners by Verified.Me) or provincial digital identities (MyAlberta Digital ID or BC Services Card). The federal Canadian approach is focused on multi-stakeholder coordination, open standards rather than specific technologies, and a commitment to interoperability and compatibility of existing digital identity solutions (Abraham, 2020).

Resistance to identity cards also stems from more surprising sources and groups, reflecting their values, beliefs and, sometimes, myths. For example, there is religious opposition that views national identity cards as metaphorically representing the "mark of the beast" (Monahan, 2008). The Orthodox Church in Greece and Russia has organized conferences and public campaigns, outlining the religious concerns with electronic identity cards and government issued unique identifiers (Molokotos-Liederman, 2003, 2007). Other examples of a myth-based resistance are more fluid and harder to locate, such as conspiracy theories about the politics of

identity cards in relation to the power of global technological corporations, such as the ID2020 project involving Microsoft and Bill Gates (Thomas & Zhang, 2020). Some of these beliefs about a hidden agenda behind electronic identity card innovations exist in the form of generalizations and stereotypical thinking about the world ruled by a few people and Western corporations, controlling global population by means of electronic microchips, either embedded within an electronic identity card or implanted in human bodies during mass-vaccination (Sturm & Albercht, 2020).

Political analysis of electronic identity cards tries to understand the reasons and motivations for smart identity cards as policy solutions to problems of bureaucratic inefficiencies in public administration. There are different political and cultural attitudes to eID in Western jurisdictions, countries of the Global South, and the European Union, and these lead to different policy solutions and levels of acceptance or resistance. The complexity of reasons behind the eID applications around the world gives rise to new questions about the social and political implications of such developments. Surveillance studies focus on the examination of the consequences of technologically enhanced identification practices in modern societies and warn us about possible unintended outcomes, and societal and individual risks.

2.4: The Critical Studies of e-ID as a Surveillance Mechanism

Finally, there is an abundance of critical research into government surveillance. It is a multi-disciplinary enquiry, with the focus on normative, ethical, and political assessments of the growing role of technology in an information society. These studies focus on the ways in which surveillance technologies impact our lives and alter the ways we manage personal information. The well-established claim here is that this growing attention to, and collection of, personal

information by many organizations and types of technology creates new challenges to privacy protection, information security, and individual freedoms. Surveillance studies see electronic identity cards as an instrument of social sorting, and believe that these instruments can lead to discrimination, as a result of their unprecedent ability to collect and process personal data, determining trends in behaviour and classifying people accordingly (Ericson & Haggerty, 2006; Lyon, 2009; Bennett & Lyon, 2008; Lyon, 2013; Zuboff 2019).

The surveillance studies literature raises critical and normative questions about electronic identity cards. What are the social consequences of these e-ID developments? When looking at the outcomes, who will be a winner and who will be a loser? Will identity card systems contribute to social equality and justice, or will they be an instrument of greater social control and social exclusion? This school of thought views electronic identity cards as a manifestation of broader theoretical issues, such as state identification, social sorting, and surveillance based on assumptions about the universality of social control, discipline, and class inequality across jurisdictions and cultures. Therefore, the electronic identity card is viewed as being the result of existing structures of social control and social inequality, and as a tool for reinforcing their influence. Surveillance studies are an extensive area of research that includes sociologists, neo-Marxist theorists, criminologists, and privacy researchers. In this section, I will address the concept of surveillance and explore its significance for the subject of electronic identity cards. I will also analyze the literature that addresses the implications of electronic identity cards through the concepts of social sorting, dataveillance, and function creep.

2.4.1: The Identity Card as a Social Sorting Instrument

Surveillance studies view identity cards as a system that allows governments to monitor and control citizens. This idea rests in the logic of the modern state that, according to James C. Scott (2003), has always sought sophisticated ways to count, tax, allocate, monitor, and order the activities of citizens. The goal of the modern state is to classify, measure, and allocate human subjects, creating "legible people," in a way that will reinforce national state power (Scott, 1998). Theories of modern nationalism and citizenship emphasize the significance of national identification systems in the process of state-making and constructing national identities (Marshall, 1950; Joppke, 2010; Greenfeld, 1992). At first, identification documents were used to locate populations within borders, control travel, and differentiate between citizens and non-citizens; but lately they have become a legitimizing instrument for welfare inclusion and the control of social services (Torpey, 2000).

Historically, government attempts to design a surveillance system based on identity documents had serious practical limitations, even in the case where the regime had all the controls of a repressive apparatus. For example, the Russian passport system, while repressive and violent for certain sects of the population, was also contradictory, costly, and ineffective for society and for public administration in general (Buckley, 1995; Semukhina & Reynolds, 2013). Surveillance heavily relied on the culture of denunciation and bureaucratic discretionary power, and not on the practice of technical impersonal observations and decision-making (Garcelon, 2001). Passports became a practice of social "masking" (Fitzpatrick, 1999): the bureaucracy and the police were engaged in complex and time-consuming identification practices that attempted to establish and confirm the social origin of individuals and their current place of residence and work; and people were engaged in masking their identity and working on ways to obtain that

desired passport status that would allow them to benefit from the new communist system of distribution (p. 132).

Today, electronic identity cards are promising to deliver efficiency and effectiveness in state identification practices. The promise is to make citizens accurately identifiable and arguably serve them better and more cost-effectively. The idea is to make sure that "the right person receives the right treatment," but does this also mean that the new types of records about the service and the person will be automatically created, stored, and shared across different government departments? This requires the creation of electronic categories of the population and interlinked registry databases in governmental agencies. David Lyon (2009) identifies e-ID as a sorting system "to put citizens into categories, to be better seen and thus differently treated by the State" (p. 40). Lyon is one of the leading theorists to write on the use of the electronic identity card as a social sorting and social classification tool (Lyon, 2002; Bennett & Lyon, 2008).

For example, smart card technology is used for social sorting in welfare, healthcare, and municipal services in many jurisdictions. The smart "welfare cash cards" that were implemented in Australia in 2012, Moscow in 2009, and debated in the United States and United Kingdom, are based on the social classification of different types of welfare groups, and include the prediction and prevention of risks associated with welfare fraud. The cards allow for the close monitoring of welfare spending history and provide data for establishing statistical correlations and data-matching between socio-demographic characteristics and consumer behaviour, including tendencies toward fraudulent activities (Bray, 2013). Graham and Wood (2007) describe the use of smart cards as a tool of digital surveillance in the city used to differentiate consumers within transport communication and service provision. Another example is smart

cards that regulate access to community services: for instance, transport, libraries, and social services in the UK have a system of loyalty points. Cardholders can accumulate points through healthy choices; therefore, behaviour is not only monitored through the smart card but also reinforced (Lips, Taylor & Organ, 2009). As a result of the new digitizing surveillance embedded in the smart identity card, some clients receive priority service and treatments while others are identified as a potential risk.

These cases illustrate how electronic identity cards can go beyond the purpose of authentication and work as a digitization tool – providing electronic data about the activities of the cardholder. These data are then used by governmental agencies to generate new types of databases where information can be easily manipulated mathematically and statistically, and where a new type of knowledge can be created and used in public policymaking and implementation (Tavani, 1999; Marx, 2001; Raab, 2009).

2.4.2: Electronic ID and Dataveillance

Although electronic governmental databases seem to be a new development, they are nested in the idea of bureaucratic rationalization, part of which includes record-keeping activities (Weber, 2009). The critical literature on governmental databases as a system of state surveillance and a threat to privacy and civil liberties has existed since the 1960s in the United States and the United Kingdom (Packard, 1964; Ruggles et al., 1968). Moreover, the research has become more intensive following the computerization of state bureaucracy, thus exposing the new dangers of large electronic databases for civil liberties and privacy. Computers and large data systems decrease the cost of data sharing and increase the ease with which data can be shared with any

organization. This technological capacity for data surveillance must be controlled and subjected to the rule of law and procedural due diligence (Westin & Baker, 1972; Westin, 2013).

The existence of interlinked registry databases theoretically allows for a higher level of data interoperability between agencies. Data interoperability implies the creation of networked and searchable databases and the free flow of personal information between government agencies for better service, law enforcement, and fraud prevention. Although in some societies it is emphasized that personal data is well protected under privacy laws, the interoperability of different systems facilitates population surveillance. Clarke describes this process as "dataveillance": "monitoring of the actions of many people via data matching and record linking" (1988). Gandy refers to this process of statistical surveillance in governmental agencies as statistical analysis of data "to place individuals within a dynamic multidimensional matrix of identities" (Gandy, in eds. Ball, Haggerty & Lyon, 2012).

Surveillance as a sorting mechanism implies a difference between two types of identification created by the state: "who you are," which is presented in the particular e-ID card, and "what you are," which emerges after statistical manipulation with the searchable and interlinked population registries. Electronic identity management systems employing statistical surveillance will concentrate more on the "what you are," and what services you have used, and therefore produce conclusions for policymaking that may facilitate discrimination and social exclusion. On the surface, people will be using electronic identity cards to securely authenticate themselves online. However, the fact that a uniquely identified individual was accessing a government program will be captured and stored and may be linked with the corresponding record from a different system or program, for example to understand transition of individuals with certain social-demographic characteristics through the government systems. Such data-

linking increases the surveillance potential of electronic identity cards, and increases the ability of the state to manage populations through new policies or eligibility requirements.

2.4.3: Function Creep, E-identification and Surveillance

One other critical aspect of electronic identity cards includes the concept of "function creep" as a threat to privacy. Function creep describes a continually growing use of surveillance technology applications that goes beyond their initially intended purposes (Clarke, 2013; Lyon, 2008).

Woodward suggests that "identification systems would gradually spread to additional purposes, not announced or not even intended when the identification systems originally were implemented" (Woodward, 1997). As an example, the author provides the history of the Social Security Number (SSN) used in the United States. Before the 1960s, the SSN was not intended for identification, but eventually the number became a mandatory identification tool. Today, privacy advocates, human rights activists, and watchdog organizations have cited many cases where new technology is introduced to do one thing and is later used for an entirely different purpose. An example is the use of surveillance cameras or license plate scanners for establishing the monitoring of protesters and activists (Wipond, 2013; Balko, 2013).

In this respect, the promotion of smart cards with endless possibilities of functions and applications looks troubling in terms of preventing cases where the new usage of eID may violate privacy and civil liberties. Greenleaf, in his analysis of Hong Kong's smart ID, explains how intended but undefined expansions of the identity card functions can increase bureaucratic discretion in dealing with personal information (Bennett & Lyon, 2008, p. 80). His analysis defines the core problem with the new identity card and associated administration "Registration

of Persons Office" (ROP) and their database, particularly its technological design, supporting unlimited new functionalities and uses depending on available government or private sector services that require verification of individual identity. The author is concerned with the unlimited opportunities for function creep, where ID card policies and regulations are worded rather generally to include "any lawful purpose" for the collection and processing of data created every time the card is used (p.82).

This more critical literature focuses on electronic identity cards as tools of surveillance that are nested in old and well-institutionalized practices associated with a modern nation-state. The development of record-keeping systems has depended on the accuracy of the identification policies and vice versa. The duality of records-keeping and identification practices has facilitated the growth of surveillance power of the bureaucracy. Finally, the use of smart technology has not only intensified this process but has also enlarged it, including private sector organizations and private-public initiatives. As a result, electronic identity card systems reinforce governmental and private practices of social sorting and citizens' classification within a new system; they facilitate the creation of a new type of knowledge extracted from databanks through data matching and linking, supporting data analytics and dataveillance. Finally, they lead to new and unregulated identification practices and personal information processing due to function creep in the technological design of smart cards or intentional universality of the smart card functionality design. All three developments encourage research on the consequences for social justice, privacy protection, and civil liberties.

2.5: Conclusion

Although the electronic identity card has become an issue only within the last several decades, it has generated considerable interest among researchers from a broad array of disciplines and traditions of inquiry, including public administration, political science, and critical social science. All three disciplinary approaches are equally crucial for understanding how electronic identity cards work in public administration, why they are developed, and what are the possible social consequences of their use in the public service.

The Instrumentalist approach to electronic identity cards calls for analysis of the e-government policies and programs developed in the Russian Federation to establish the relationship between the goals of ICT modernization of Russian government systems, and the role of the UEC as an instrument in this process. How does this instrument fit an overarching framework of government digitization? Does it have a specific role in a bigger project and how are they connected? What does this instrument support in Russian e-government? This analysis leads to the identification of key stakeholders and institutions responsible for the implementation of the UEC, and determines similarities and differences of the expressed justifications for using this instrument across institutional and organizational divides. The literature on digital identity management will help to document and assess the design of the UEC and identify potential implications for security and privacy, as well as document proposed technical and policy controls.

The political science approach deepens and contextualises this case study by bringing into focus institutionalized legacies of the Russian state identification system, and the administrative practice of documenting Russian citizens and controlling innovations in this area. How do key stakeholders formulate the meaning of UEC innovation in relation to existing political culture and their political interests, and how do they innovate to fit existing

identification practices? How does the process of innovation fit within the structural configuration of the state, the relationship between the public and private sectors, federal and regional authorities, law enforcement and economic development, and with what outcomes? Finally, how do technological drivers documented in other case studies compare with Russian technological drivers? Are there more similarities or differences indicating policy convergence or divergence of electronic identity card developments across jurisdictions and political regimes? And how do those similarities and differences impact regulatory and technological design of the UEC?

A critical approach views the UEC as a potential mechanism of state surveillance. Can the UEC be used to support existing non-democratic processes of controlling civil society and monitoring political dissent in Russian society? Does it support Russian state surveillance? Does it allow government to target social assistance and track the use of government programs? What social groups are targeted and with what outcomes, and how are those processes expressed in the justification of policies? Is there a popular criticism directed at this innovation from the perspective of surveillance studies, privacy, and civil liberties? Is the UEC being criticized for a similar reasons as electronic identity cards in other case studies? Who is criticizing UEC implementation, what are their demands in terms of UEC design or use, and how successful are they with impacting the outcome of the innovation?

The next chapter will provide details on application of these three perspectives to the qualitative case study of the Russian UEC. They constitute three pillars of the theoretical framework, providing a foundation for the comprehensive and detailed inquiry from the multiple points of view. I explain the collection of primary resources (various forms of documents and

recordings capturing UEC development by the witnesses of events) and provide details on documentary analysis shaped by the interpretive policy method.

Chapter 3: Case Selection and Research Methodology

3.1: Why the Russian Universal Electronic Card?

This chapter provides academic and personal reasons for the selection of the Russian Universal Electronic Card as the subject of my research. It clarifies my research objectives and provides an overview of the qualitative case study methodology. It describes the theoretical framework, outlines procedures for collection and evaluation of primary resources for qualitative document analysis and explains the application of the interpretive policy framework.

Although electronic identification systems are a contemporary global trend, and many cases have been studied, there is no substantial research in English about the Russian case. The largest country in the world, with significant power in the international arena, tried to implement a new electronic identification system with significant social and political implications. This study focuses on the contemporary development of the Universal Electronic Card (*Universalnaia Elektronnaia Karta*), while contextualizing it within the institutionalized legacies of the state identification practices, existing political and technological drivers for eID, socio-economic factors, and relevant policy communities in the Russian Federation.

Russia is a country of many social, political, and economic contrasts that make it a unique political system for a qualitative case study analysis. It is an illiberal democracy (Engelstein 2011, Shevtsova 2007, Zakaria 2007) with authoritative executive leadership and a weak civil society. At the same time, it is an acknowledged global player with a strong inclination in international relations to rebuild colonial influence over post-communist territories. Russia is a multi-ethnic federal state, but it is ruled from the center by the hierarchical, predominantly Russian, bureaucracy. The processes of privatization are accompanied by the processes of nationalization in the interest of the oligarchic groups nested in the circles of Putin's

influence (Gessen, 2012). The processes of modernization and development, driven by oil money, are confronted by corruption and bureaucratic inefficiency (Konstantinov, 2006).

It is interesting to examine whether the same kind of motivations, drivers, and resistance to electronic identity card development exist in this unique political system as in the Western context. Another reason to study the development of the eID in the Russian Federation is due to the observed institutionalized legacies in state surveillance and oppressive state identification systems. The "passport" in Russia is not just an identification document; it is crucial in terms of determining an individual's position within the social class structure, which has implications for mobility, human rights, and cultural status. This thesis explores the extent to which the universal electronic identity card is driven by these institutionalized practices, the legacies from the past, and to what extent the new system embraces and reinforces those practices.

Conversely, what can American, Canadian, and European studies of electronic identification learn from the Russian case? The Russian case may be a mirror for Western discourse around technological bureaucratic modernization and the problems the electronic identity card is supposed to solve. The initial development of the UEC was quickly progressing with growing technological expertise within the government, insulated from the processes of accountability, procedural due diligence, and institutional and public consultations, and was overseen directly by the President, Dimitry Medvedev. Over time, the UEC project has slowed down, accompanied by limited resources for implementation across all the Russian regions, growing criticism by the Orthodox Church community, and national security concerns with Western technology. What explains this shift from optimistic modernization, supported by the President, to policy failure? The failure, which instead of being publicly acknowledged as such,

was reframed as a more appropriate project – the Russian Electronic Passport postponed for better times.

Finally, to what extent is this policy solution a particular and unique Russian idea, shaped by the historical practices of the comprehensive passport regulations, and to what extent is it influenced by the broader global processes of policy transfer, political economy, and the interests of high-tech corporations? What can we learn from local knowledge about the evolution of state identification practices? What kind of deeper meaning, expressed through cultural assumptions and policy justifications, is associated with the UEC? What does it promise to the Russian population, Russian government, and businesses, and how do those promises reflect cultural and political beliefs about what is right and wrong?

3.2: The Theoretical Framework

The objective of this work is to combine the instrumentalist, political, and critical perspectives in the literature to reveal the story of electronic identity card development in the Russian Federation. My guiding assumption is that any technological innovation would be subject to a meaning-making process of defining the appropriateness and goals of the innovation within a specific institutional, political, and socio-economic policy context. How was the meaning formulated and presented as a policy solution and what key stakeholders were involved in it? How was it translated into a legislative framework and regulations? Was there any policy deliberation around the meaning and definition of the electronic identity card innovation? Who was involved and what did they emphasise and communicate about what this innovation would mean for Russian society? Finally, how has the UEC worked out practically, and what contextual (cultural, societal, and political) factors have shaped these policy outcomes?

The meaning in policymaking is crucial, as it is constitutive of political action and public policy (Wagenaar, 2014). This is a dual process, as Wagenaar explains: "people perceive and experience social phenomenon under the influence and constraints of social factors (politics, culture, institutions, values, believes), and in turn, the meaning that people attach to social phenomenon influences the institutions, social practices, and public policies, or even determine their very existence" (p. 4). I will focus on the Russian UEC project employing an interpretive policy approach. This requires a contextual understanding of "local knowledge and practice" (Yanow, 2000). What do key stakeholders, involved in the delivery of the UEC innovation, say, promote, and do and within the institutional and organizational settings in which they act?

This interpretive policy approach to the case of the Russian UEC is framed by the empirical findings developed within instrumentalist, political, and critical perspectives discussed in the literature review. They help to identify directions of the inquiry, formulate questions, and look at the research subject and its characteristics from different angles, providing an in-depth appreciation of the case. Their academic contribution is based on different assumptions about the subject of research, an electronic identity card, and these assumptions require comparison. Instrumentalist and critical perspectives share foundationalism in their assumptions and justifications about the objective nature of the eID cards. This foundationalism rests on two beliefs about the definition and function of the eID cards.

First is a belief in the supremacy of technology of the eID card, and that the technology will effectively perform the tasks it was designed to perform. This technological imperative exists independent from our knowledge of it, our perception of it, and our experience with it. The technology will shape our experience with it, not the other way around. The difference between instrumentalist and critical perspectives is that the first views eID as an apolitical and objective

tool which can be controlled with an operational manual, and with standardized procedures to ensure compliance with the regulatory framework and legislation. The critical perspective, on the other hand, focuses on the eID as a surveillance tool, serving the interests of those in power, recording electronic trails created by the card within searchable and networked databases, and facilitating social sorting (Lyon, 2009). Gandy (1993; 2021) refers to the growing ability of the governments to use technology for identification, classification, and assessment of population as a panoptic sort, supporting disciplinary surveillance and embracing cost optimization of public spending. The eID system not only supports secure authentication of citizens online – it also records behavioural trends in usage depending on identity, allowing the government to track the transition of classes/groups of individuals through multiple government programs (Gandy, 2021). This makes administrative decision-making about classes of individuals in new programs more efficient and more targeted.

Second is the belief in the universality principle of eID card technology. If eID cards are instruments that are objective in relation to human agency, that means they will generally function in practice as they are designed, as long as they're used according to the established standards. For example, an electronic ID that was designed to improve citizen access to online services in Estonia, if implemented under specific conditions, would do the same thing when implemented in Ukraine or Brazil. The standards and procedures are crucial for the technology to perform effectively in any context. Following this logic, the modernization potential of eID is evident. Similarly, the surveillance literature embraces the universality of ID cards for their ability to result in social sorting and to discriminate despite the political regime.

On the other hand, the political approach to eID brings political interests and power imbalances into question. This approach emphasizes that the reasons and practices of eID

implementation, while influenced by the technological promise of smart cards, is significantly influenced not only by human agency, but also by political culture, history, institutions, and administrative practices. Therefore, the outcomes of an eID project in any given country are determined by the interplay of many local factors and variables. Lyon and Bennett (2008), through analysis of national eID case studies, illustrate how the process of eID implementation is influenced by culture, institutions, and history whose influence can be contradictory and lead to unpredictable results (p. 18). Those unpredictable results of the seemingly rational plan to implement the Russian Universal Electronic Card stimulated my interest in this subject. How exactly do the global technology standards in eID, the e-government concept, and secure identity system management standards interact with the historical legacies, institutional settings, the structural configuration of the state, and cultural perceptions? Who is interpreting these global solutions within the local setting, how, why, and to what end?

I attempt to explain the process of the electronic identity card mutation during policy implementation, as a result of a conflict between foundationalist beliefs about the universality and technological supremacy of the eID in policy justifications, and practical and political challenges of implementation. My focus is on the political practice of negotiating power structures and incentives within a proposed eID system, included and excluded policy communications and their interpretations of the technological innovation. The electronic ID card is a technological innovation that will mutate because errors in its implementation are inevitable. There will be a period of cultural appropriation, and a continuing cycle of policy definition, justification, failure, and redefinition. My analysis tries to identify and analyze those contradictory forces in policy implementation that will lead to confusion, mistakes, uncertainties, crisis, and failures, which will result in policy mutations.

My assumption about the eID card technology is that it will transform in response to the contextualizing power of societal and political factors, including resistance to innovation. The complexity of society and tensions between agency and institutions will challenge the underlying foundationalist assumptions about the supremacy of technology, its independence from the human agency, its apolitical nature, as well as a tendency to assume that technology enables rational, evidence-based decision-making. No matter how complex the technology, the algorithm, or the identification mechanisms are, the eID will fail to capture and regulate the complexity of the social world and human interactions and will have limited applications through a series of trial and error.

This thesis includes the instrumentalist perspective by asking questions about electronic identity card as a material technological object, which is an element of e-government supporting rationally planned policy goals. What are the characteristics of it and how is it designed to operate? How is it regulated? The analysis focuses on understanding the role of the universal electronic identity card in the electronic identity management and governmental information management in the Russian bureaucracy. In other words, what kind of information about the individual is included in the card, who can access it, and for what purposes? How and under what conditions can the cardholder use the card for online authentication? What happens to the electronic trail logs each time the card is used in a reading device? The answers to these questions will provoke questions from the critical perspective to test the assumptions from surveillance studies, that this information may be accumulated and maintained in the form of large and interconnected data sets, which can be utilized for new purposes within the broad government information system leading to increased population control.

The Russian government developed the UEC project based on the success of the urban model, the Moscow Social Card. I apply a critical perspective by exploring the ways this card was operating in Moscow as an instrument of surveillance and social sorting (Lyon, 2009). In Chapter 5, I collect and organize evidence of how the Moscow Social Card was implemented to provide social benefits to specific demographic categories of the population, and to control the effectiveness of public spending. The critical perspective helps to establish what electronic registries of population exist, how they are regulated, and what categories of the population are defined as the target audience for government-funded programs. This research will explore how the electronic data sets from identity card usage are accumulated, how the data was shared with other agencies (data interoperability), if applicable, and even more importantly how this new information management is regulated. In terms of the Universal Electronic Card project, which failed to produce a national identity document, the critical perspective is useful in understanding different concerns regarding the surveillance power of the UEC expressed by the key stakeholders and policy communities opposing the initiative. The evidence I gathered through this research supports the view that the UEC is perceived by some policy stakeholders as an instrument of global surveillance, which challenges Russian sovereignty through the collection and use of personal information on Russian citizens by foreign companies.

From the political perspective, this thesis views the identity card as a politicized object and unveils sometimes hidden or not-so-obvious reasons for its development and outcomes. There are four factors within this perspective that are utilized in explaining electronic ID development in Russia: technological drivers, policy legacies, political culture, and the structural configuration of the state (Bennett & Lyon, 2008). This theoretical framework originated from the comparative analysis of global identity card development, which considers identity cards as

policy instruments that target specific *policy problems,* as opposed to the notion of the identity card as a technological tool. The implementation of such a policy instrument is associated with new governmental and social practices, new politics, and power redistribution. It is important to ask the question, what problem was it solving? Who was framing the problem, and how was it being framed? And why were certain solutions advocated over others? To what extent are technological industries and companies involved in this process? What lessons were drawn from other jurisdictions?

The first variable from the political perspective is the *technological drivers* of the Universal Electronic Card. To what extent can this case be explained through the perspective of the Card Cartel theory (Bennett & Lyon, 2008)? The Card Cartel theory suggests that the growing trend of electronic identification systems globally is the result of expanding public-private initiatives targeted at the technological transformation of public administration. Strong industries have been advocating for more and more complex and costly technological solutions to government operations. Electronic industries not only build new markets for their products, but also gain an important voice in shaping public policy. But this process is neither democratic nor inclusive (Horrocks, 2009). It is important to identify these industries and companies in the Russian case, and to explore their relationship with international corporations.

The second variable is the role of *policy legacies* around identification and surveillance practices. Chapter 4 examines the history of the Russian government's attempts to modernize passport administration during three historical periods. I try to identify the drivers of state control in terms of bureaucratic identification practices, which have been concentrated in urban centers. Based on this historical analysis, I identify Moscow to be the experimental ground for identity document reforms which, once institutionalized, were to be transferred to other urban centers

before becoming universal state policies. Second, I illustrate how local practice and knowledge of the Moscow Social Card was internalized within the Universal Electronic Card (UEC) project through analysis of the UEC legislation, the organizational and institutional framework, and the technological infrastructure. I analyze policy steps that were documented by the government to ensure that the project was successful in urban centers across different regions before it could be integrated as part of the national state identification system. Finally, I focus on the role of the "interpretive communities" engaged in this policy innovation, whether in supportive or opposing roles. I will analyze who is involved, what institutions they represent, and how they interpret the UEC project as a policy innovation.

The third variable is *political culture*. What do citizens think about the universal electronic identity card? It is important to explore the general level of support for electronic ID as well as existing negative perceptions and resistance. Some might think that the UEC would align with existing levels of surveillance normalization due to the historical passport identification legacies and modern practices of the omnipresent surveillance by the Putin regime's law enforcement and security services (former KGB[2] in the Soviet Union). Therefore, there would not be much civil resistance to the new electronic ID as state surveillance is a deeply embedded cultural practice. This may explain the lack of the political opposition to the innovation, the lack of privacy and civil liberties concerns voiced by independent journalists, lawyers, or civil activists, and the lack of independent social movements opposing the new policy. In other words, people who would normally criticize Putin's illiberal regime did not target this innovation as an instrument for greater surveillance by the regime.

[2] *Komitet Gosudarstvennoi Bezopasnosti* a Committee for State Security, foreign intelligence, and domestic security. The KGB's main successors are the FSB (Federal Security Service) and CVR (Foreign Intelligence Service).

However, I discovered a different type of resistance to eID voiced by the Russian Orthodox Church and the key stakeholders responsible for the state identification system within the Ministry of Internal Affairs. Their political pressure and criticism resulted in the UEC going from obligatory to voluntarily in 2013 and being discontinued in 2017. Additionally, the Ministry of Internal Affairs announced a whole new electronic passport project in 2021 which was limited to their Ministry, to substitute the UEC with a national electronic passport. The most recent proposal of the national electronic passport is out of scope for this research, but the war against Ukraine has deprioritized this idea. It is also not clear whether, under sanctions impacting the technology sector, the Russian government will be able to initiate another technological innovation. Through the exploration of the political culture, I will demonstrate how and why resistance was mobilized against the UEC policy innovation.

Fourth, *structural configuration of the state* is concerned with the extent of bureaucratic centralization, processes of state privatization, and the general structure of decision-making. I explore how the idea of the electronic identity card travelled through the Russian bureaucracy from the Moscow Social Card to the federal level as an all-inclusive and universal card with similar functionalities. The structural configuration of the state also draws attention to the possible policy failures, due to the differences between federal and local government responsibilities, associated tensions over public funding, and different mandates for the UEC project expressed by multiple stakeholders. I identify and describe institutional and organizational bodies working towards hierarchical integration of the public administration by means of the UEC project, and those dedicated to the deeper centralization of state identification. Additionally, I explore the role of the public-private partnership “JSC UEC” and one of the biggest Russian banks, SberBank, in shaping technological functionality and delivery of the UEC

across Russia. I draw the conclusion that the complex relationships between all these structural elements, and the inability of the state to oversee and navigate those relationships, partially explains the failure of the UEC in the Russian Federation.

The conceptual framework supports a comprehensive and multidimensional case study of the Universal Electronic Card, through exploration of the rich variety of factors and questions reflecting instrumentalist, political, and critical perspectives developed in studies of electronic identity cards. It is appropriate to embrace as many characteristics of the studied phenomenon as possible. It is expected that certain explanatory factors will reveal themselves as more meaningful during the analysis, while other factors will serve an important descriptive function.

3.4: Justifications for a Qualitative Case Study, Sources and Analysis

My experience of research enquiry is that it is a process of interpretation and making sense of the phenomenon under investigation. The qualitative case study is my choice of methodology for investigating this technological innovation from its announcement (2010), through partial implementation (2013-2016), and then, ultimately, failure (2017). It is a story that has a beginning, conflict, conflict resolution, and an end. The use of the case study method is intended to capture the complexity of the object of study from a different perspective, to understand how the phenomenon of the electronic identity card is socially constructed in the policy community, how its implied rationality is limited by conflicting interpretations, the ideas and myths about its appropriateness, and legitimacy depending on the cultural or political context.

According to Merriam (1998), the case study "focuses on holistic description and explanation" (p. 29) of a social phenomenon. Stake (1995) describes qualitative case study research as a combination of a variety of methods, involving naturalistic, ethnographic, historical and biographic research methods aimed at catching the complexity of a single case. As a trained sociologist and political scientist, I am naturally drawn to the exploration of the "real-life, contemporary bounded system (a case) over time, through detailed, in-depth data collection involving multiple sources of information and reporting case description and case themes" (Creswell, 2013, p. 97).

Case studies constitute an important method of enquiry in comparative politics because of their ability to support establishment of general propositions leading to theory-building in political science (Lijphart, 1971). Following different typologies of the case-study methods and their contribution to the theory-building exercise, this dissertation examines the rise and fall of the UEC project through a perspective of the three theoretical approaches and intends to test their propositions and established generalizations. According to Lijpart (1971), the application of the established variables and propositions to the new unique cases can either result in theory-confirming or theory-infirming case studies (p. 692). The first one may be useful for strengthening universality of the findings and their applicability to different cases, while the theory-infirming cases could provide crucial falsifiability test and identify gaps in existing propositions.

In this sense, the study of the Russian UEC case is important because it will allow to test the relationship between authoritarian, centralized and hierarchically organized state, and its potential to implement new technology, able to provide more efficient state control over the population, supported with the surveillance capacity of the electronic identity documents. This

thesis is organized as a narrative that helps to interpret the policy language of the Universal Electronic Card's development, as presented in published texts, including media reports and articles, conference presentations, academic studies, legislation, policy drafts, and programs. An important characteristic of this policy development was the lack of a deliberative policy process or policy analysis within the public administration. Rather, there was a central political announcement followed by rapid legislative changes, and simultaneous policy activity in different spheres. The story emanated from Moscow to the regions, from the idea of the Moscow Social Card as a tool to modernize public administration, to the federal government idea of the "all-in-one" technological solution. The policy language is shaped by different policy actors that represent different institutions, industries, and levels of government. This language is characterized by the tone of the technological inevitability of the Russian Universal Electronic Card due to its practicality, convenience, and prospects for modernization. The policy story starts with the interpretation of the meaning that multiple policy stakeholders formulate and attach to policy justifications, and the consequences for society.

The findings of this research serve as "evidence for use" (Crasnow, 2011) for further understanding of the general processes involved in identity management policy solutions and, therefore, contribute to the broader identity card research. The Russian Universal Card is not only a technological token that is driven by the logic of rationality, but it must also reflect cultural, social, and political assumptions about the need for this eID in Russian society at this time. Interpretive policy analysis helps to extract socially constructed meaning behind policy solutions, based on the ontological assumption that the existence of things is determined by our language (Rochefort & Cobb, 1994). Exploring how this is articulated and communicated within

different contexts, and how policymakers enact a set of myths to justify, rationalize, and legitimize their actions (Hier & Walby, 2014, p. 154) is one of the goals of this research.

An interpretive policy analysis requires the gathering of documents, artifacts, presentations, and other materials created with the purpose to explain, describe, justify, or criticize the Russian UEC. For the purpose of this research, I mostly relied on open-source materials, searchable and available on the internet. My knowledge of Russian and my understanding of the structure of the Russian government, the mass-media, and Russian search engines and social media channels helped me compile the relevant documents, videos, and other materials from a diverse array of sources, audiences, and messages.

To support the goals of this case study, any document, video, article, or presentation in the Russian language, created by any individual or organization describing, discussing, promoting, or criticizing the UEC project is included as a primary source. The full list of primary sources is included in Appendix A. First, I collected the official documents created within government agencies, ministries, and financial and telecommunication industries dedicated to the Universal Electronic Card. I analyzed programs, reports, and projects prepared by the experts and employees of participating industries. While reading the documents and watching the videos and interviews, I took notes in English, translating the most important themes, repetitive ideas, claims, justifications, conflicting ideas, and connections. My goal was to explore what solutions were presented as innovative policy options for the government, and how they were presented.

I also tracked internet sources, using Google Alerts and Russian search engines (Yandex.com; Rambler.ru) to constantly monitor any news that mentioned the Russian Universal Electronic Card. In terms of primary documents, many original and relevant policy documents were gathered and presented at the web resource for Russian government employees:

http://www.gosbook.ru. Between 2010 and 2019, Gosbook was a social network of experts and public servants involved in public administration reforms in Russia. The network community "UEC implementation" consisted of 272 members and their electronic library provided access to 358 different sources with tags 'electronic government' and 'UeID'. Available sources varied from news articles to government reports, programs, and the notes of Committee meetings, discussions and conference papers and reports. Between 2014 and 2015, I downloaded over 100 relevant documents from this portal. In 2019, the Gosbook portal was discontinued due to the growing national security concerns over this publicly available information hub for government officials and government policy experts.

Primary sources used in this work also include statutes, laws and regulations, and corporate and organizational records available through online government depositories. Official copies of annual reports containing signatures and stamps, screen shots, and corporate Power Point presentations were archived from the Universal Electronic Card UEC Agency website (www.uecard.ru[3]). Promotional materials, advertisements, and recordings of conferences and round tables are available at the PressaUecard YouTube channel (www.youtube.com/user/PressaUecard) and SberBank website (www.sberbank.com). Some of these internet sources are not accessible anymore from Canada or anywhere else as websites were taken down, or certain IP addresses are blocked, which is the case for the Moscow Government and the Ministry of Internal Affairs websites. Media sources, such as published interviews with policy leaders, press-releases, commercials, and news reports are also included in the analysis as they contain insights regarding the interpretation of the technology for different audiences,

[3] The website is not hosted anymore but some of the content is archived by the Russian IT magazine Cnews: https://uec.cnews.ru/archive/articles/uec

revealing perceived attractiveness and persuasive marketing language. Before including a primary source in the analysis, I evaluated its currency, authority, credentials, accuracy, and reliability. This assessment process occurred several times during this longitudinal study (in 2014, 2016, 2017, and 2018), in order to address the need for repeated observations during the significant changes in policy direction within the study period. The full list of primary sources is included in Appendix A.

Originally, when I was planning my fieldwork in 2014, I was hoping to travel to Moscow and attend one of the information technology industry conferences and establish opportunities for interviews with key informants. Tragically, the Russian government forcefully occupied Crimea and organized direct military interventions of Donetsk and Luhansk Oblasts in Ukraine. International relations between Russia and the West have worsened, so I decided against travelling to Russia for personal and safety reasons. I have also confirmed with my colleagues from past Polish-Russian democratization exchange projects (Stefan Batory Foundation, 2007) that any interview involving a Russian public official or researcher at the public university with a foreigner is subject to review by law enforcement and security agencies, who reserve the right to be present at the interview or request a report. In this situation, I could not protect the confidentiality of the interviewees and could possibly put them at risk with my dissertation topic. I had no plans of applying for clearance from Russian law-enforcement and doubted that under such conditions any interviewee would provide me with information that is not otherwise publicly available. Instead, I utilized my knowledge of the Russian language and focused on open-source intelligence. My professional experience as a privacy analyst with the government of British Columbia helped me to develop an informed perspective on technological innovation in public administration, including awareness about tensions between legal requirements, privacy compliance, security standards,

business needs for technological innovations and digital reforms. My experience guided me with interpretation of the materials gathered in the beginning of the research. Thankfully, the open government reforms implemented by Medvedev (2011) were a fruitful time for government websites, which became filled with copies of government policies, statements, reports, and programs (Gossbook.ru, Government.ru/docs, Gosuslugi.ru). I just needed to locate, download, and organize them. The list of primary sources in the Russian language is included in Appendix A, transliterated, and translated.

The review of the primary sources, as well as collecting additional sources, was conducted from 2016 to 2018. The practical value of this prolonged process was an ability to observe in real-time the changes in language and interpretation of the UEC. This was supported by substantial evidence from multiple sources. This study has documented the wide online public distribution of UEC-related documents and white papers, which was later followed by organized attempts to clear the internet of information and restrict access to certain documents after policy directions shifted. This work collected and secured unique primary information, available only in the form of screenshots of PDF documents, once distributed openly to support open government initiatives. Since 2017, some documents began to disappear from open access following the Russian government's decision to withdraw from the implementation of the Universal Electronic Card.

The process of document collection and inclusion in the research was completed in three steps. First, I searched online for the term "universalnaia elektronnaia karta" [Universal Electronic Card] and skimmed through sources, identifying the most relevant sources, and organizing them into groups based on the agenda, content, target audience, and ownership. Appendix A reflects this classification. Second, within these collected documents, I searched for concepts derived from the Instrumentalist perspective: e-government, authentication, online access to government services,

efficiency, reasons for implementation, technological design and functionality, security, additional legislation, and regulations. I have identified the role of the Moscow Social Card, the evolution of the payment function idea, the reasons for the involvement of the SberBank, and the connections with public transportation. Third, I identified key individuals who were giving interviews, participating in conferences, and publicly speaking about the UEC, either endorsing or criticizing. I identified their roles and associations with the relevant institutions and created a list of all stakeholders. Based on the analysis of their messages and engagements on the subject, I classified them into four policy communities: economic liberals, technocrats, *siloviki*[4] and conservatives/traditionalists. My analysis was focused on uncovering the interests of each of these communities in the UEC project, the ways in which they were interpreting the UEC, and the ways they were shaping the outcomes of this innovation.

In the interpretive analysis, the goal of text analysis is not to separate facts from opinions. The attention is on the opinions and ideas about electronic identity cards that different texts communicate in a persuasive or biased manner reflecting certain political agendas. Different texts include minutes of State Duma[5] speeches, minutes of Committee meetings, policy papers, industry reports and relevant conference presentations, blog entries, and YouTube videos. My method of establishing local knowledge focused on uncovering linkages between policy texts and communities that they were shared with, including the target audiences of these messages. Most of the selected primary sources from this category contain language that appeals to emotions while promoting a particular political, religious, and ideological agenda representing a specific point of view, including values and even myths and prejudices. I discuss these arguments in more detail in

[4] A Russian term to describe employees of the government's law-enforcement agencies and departments.

[5] A lower house of the Federal Assembly of Russia (Russian parliament), while the upper house is the Federation Council (Russian senate).

chapter 6 “Playing the meaning of the Russian Universal Card: interpretive communities and Competing Ideas.”

The agenda of each group is the very target of this research inquiry. My research attempts to map the agendas out, classify them, and understand how different policy communities use them to create different meanings, to shape policy justifications and to influence policy outcomes. My knowledge of Russian allows for in-depth text analysis as well as a contextual understanding of the regulatory framework. My proficiency in Russian also allows for interpretive policy analysis of the documents and other primary text resources in the original language gathered during the research. Furthermore, my post-Soviet socialization experience and post-secondary education in Ukrainian and Canadian universities has prepared me for reflexive thinking about the political and social phenomena as they are presented in propaganda materials or by the recognized experts. These linguistic and cultural advantages contribute to the quality of the narrative policy analysis over and above the mere description of the factual information about policy development.

Noticeably, white policy papers and government action plans advocating for the Russian Universal Electronic Card refer to the concept of e-government and discuss related issues of national security, practicality, and the universality of application. I will critically analyze the meaning of e-government in the Russian context and the associated terms employed by officials to justify their preferred policy. The universality and popularity of the e-government concept, which are reinforced by the inevitability of technological progress for security and convenience reasons, limits the opportunities for a meaningful critique. The rhetoric about e-government and the digitalization of public services contains embedded power structures controlling and directing the ways the subject matter is discussed or communicated, and this power is hard to challenge (Hajer&Versteeg, 2006; Ficher, 2003). The discourse seems to insulate the subject of technological

policy innovation from those who are not experts in technology or who are critical about the democratic nature of the Russian government. In this respect, the descriptive perspective of this research will employ interpretive analysis and the researcher will be tracing patterns within the texts and language that reflect values, beliefs, and political agendas.

In summary, this research is an example of a qualitative one-country case study. It employs mixed methods of data gathering and analysis, including primary and secondary data, historical sources, document, and textual analysis. The research fits within the scope of interpretive policy analysis. The assumptions are that language, and the ways policy solutions are discussed matter a great deal in policy implementation. I reconstruct a story of how the UEC became a policy goal, and how and why it failed to achieve that goal. There is a story that is built on persuasive metaphors and justifications, which are part of the Russian culture and language. The goal of this inquiry is to bring this story to light, identify influential storytellers and their motives, and compare the findings with the knowledge that has been developed in different cultural contexts.

The next chapter will provide an important background for understanding the institutionalized legacies, practices, and political culture of the Russian state identification system. It establishes the foundation for understanding the contextual forces as important elements that support the political and critical perspectives of this case study. More specifically, this chapter addresses two questions which have not been pursued elsewhere. First, how should we connect the historical evidence of the repressive practices of the Russian internal passport regime with the modern innovation of the Russian Universal Electronic Card in Putin's illiberal regime? Second, to what extent does the history of policy failures and tensions in the Russian state's identification system explain the failure of the UEC?

Chapter 4: Institutionalized Legacies of the Russian Passport System.

"A decent Russian person consists of three parts: soul, body and a passport"

A Russian Proverb

4.1: Introduction

This chapter explores the historical legacies of the Russian state identification system, emphasizing the differences and similarities between Tsarist Russia, the Soviet Union, and the early post-Soviet Russian Federation, between 1719 and the 2000s. The goal of this comparison is to identify recurring identification practices, both formal and informal, as well as to explore the complex relationship between the evolution of the internal passport regime and the formation of the Russian state.

In this context, what kind of iterations should one expect from the Universal Electronic Identity Card when it hits the messy and complex realities of the social world? On a more general level, this question addresses the technological promise of electronic identity cards to solve old institutional problems. Therefore, this chapter will address the historical relationship between the *ideas* behind identity documents and their innovations, and the administrative *practices* that were developed during the Tsarist, Soviet and post-Soviet periods. This chapter will also explore the recurring nature of *ideas* and *practices*, identifying those that were successfully institutionalized within Russian society despite changing political regimes and administrative reforms.

This chapter uncovers the excessive bureaucratic regulation of population movement within the state, and illustrates how this vision reinvents itself in different periods despite the regime change in Russia, accompanied by intensified urbanization, state managed labour migration, and a bureaucratized system of social stratification. The political goals of the passport

policies contrast with the realities of the administrative and societal practices. Despite the political intentions of total control, the internal passport system mutated within the extensive Russian geography and inadequate public administration, resulting in numerous contradictions and the growing role of police in enforcing and managing the passport policies within urban centers.

4.2: The Russian State Identification System in Historical Research

The history of Russian passport innovation is often discussed in Western scholarship as a representation of autocratic or authoritative practices. There is also an observable preoccupation with certain historical periods and their respective passport reforms. For example, the analysis of the Stalinist Soviet Passport policy reforms (Fitzpatrick, 1993; Kotkin, 1997; Kessler, 2001) and the internal migration during serfdom and post-serfdom historical periods in Tsarist Russia (Burds, 1998; Stanziani, 2010) explicitly focused on the experiences of Russian peasants with the restrictive passport regulations (Moon, 2002; Garcelon, 2001). There is also an increasing amount of literature in English, including by Russian researchers, where the politics of the identity documents in Russia become a central question of the inquiry (Steinwedel, 2001; Popov, 1996). Despite this fruitful scholarship, no one has applied these historical legacies to interpret current developments concerning identity management in the Russian Federation in general, and, in particular, with respect to the innovation of an electronic identity card.

The question of historical legacies is noticeably present in transitional studies on Russia and its puzzling road to democracy and the free market (Hedlund, 2008; 2011). However, these studies focus on the limitations of the electoral and administrative reforms, on the issues of Russian

federalism and regional representation, and on violations of human rights and political freedoms within a fragile civil society as a consequence of the Soviet totalitarian regime, known for its comprehensive and intrusive surveillance passport system, that was able to govern the everyday lives of the Russian population. It is surprising that post-Soviet reforms of the Russian state identification system are not explored as crucial elements of decommunization in the democratization literature. Therefore, there is a disconnect between theories emphasizing the correlation between the coercive Russian regimes and their dependence on past internal passport systems, and the theories of the contemporary illiberal (Laruelle, 2016) or authoritarian Russian regime (Ambrosio, 2016).

There are, however, some examples in recent literature that conceptualize the historical continuity of passport policies in Russia, connecting the Communist and Tsarist periods. Lonergan (2013) explores how the Soviet passport regime and residence registrations within urban centers were reintroduced by Stalin in 1932, not invented, and that this was the bureaucratic realization of a society where "all subjects quite literally knew their places" for the first time since Imperial Russia (p. 41). Baiburin (2009, 2021) emphasizes the historical role of the passport in facilitating state surveillance of citizens in both periods. Unfortunately, the exploration of these continuities does not reach contemporary passport practices, even though many of them were carefully preserved within similar institutional arrangements and avoided liberalization reforms. Such as residence registration ("*propiska*") with police, police-centered passport bureaucracies, and informal practices where one had to be ready to present a passport to anyone who seemingly might have power in a particular situation.

For the purpose of this dissertation, examining history will help us understand why certain policies recur, and will help to establish foundational, cultural, and politically specific assumptions

about the role of the passport initiatives for the state and society. These assumptions, which underpin local knowledge, unavoidably shape and influence policy discussions, and reveal themselves in multiple ways during the development of the Russian UEC.

4.3: Legacies of the Russian Empire

Western historical studies of Russia's public administration often point out its continuing and enduring characteristics, such as absolutism, patrimonialism, arbitrariness, and political patronage (Ryavec, 2003; Lynch, 2005), which are shaped, to a certain extent, by Russia's immense geography and imperial history. The Russian state is extended across highly diverse regions and ethnolinguistic and cultural communities, where "one state is intending to govern many different societies" (Rowney & Huskey, 2009, p. 7). The Tsarist administration was, in essence, a colonial administration concerned with the expansion of Russia's frontiers and internal modernization. Public officials were appointed from the deserved nobility in the political center, sometimes European by origin, in the hopes of introducing a civilized European-style administration across the Empire and regulating the population's obligations to the state (p. 27). However, this centralized structure of public administration was not supported by the communication channels, or by operations, or by standardized and uniform procedures (Ryavec, 2005). To support this observation, Kotsonis (2014) suggests that the Russian administration was inherently trapped in two everlasting contradictions, one being "very large ambitions of the central government and limited policy capacity" of local public offices (p. 19), and the other being denial of political and social agency to its population but demanding that "rightless" subjects conform to their state obligations. The author states that the only solution that was developed to solve these contradictions was greater coercion, the police state, reliance on bodily

constraint, and public denunciation (p. 24). These observations explain why the Russian bureaucracy was dedicated to the ambitious vision of the total passport society, yet continuously failed to implement this vision efficiently and effectively.

4.3.1: Governing Imperial Frontiers

The uniqueness of the Russian passport regime is determined by Russia's geographical size and multiple tensions between the central political power, the local bureaucratic administrations, and the police. The center/periphery dichotomy seems to be a structuring principle for the implementation of government policies that has been institutionalized throughout history in many spheres (Etkind, 2011). Moreover, passports rationalized this dichotomy and served as an organizing element of social geography, regulating movement between center and periphery and establishing stricter surveillance mechanisms within the center as well as at the borders of the Empire (Bradley, 1985; Bassin, 1999). The extensive size of the bureaucratically unregulated territories and communities posed a significant challenge for comprehensive passport policies. Another challenge was the unique form of Russian officialdom, which was developed to serve and maintain an absolutist regime instead of establishing independent rational-legal authority (Rowney & Huskey, 2009).

Passport policies were necessary for the central establishment as an indication of a strong state; however, there was a lack of policy capacity and operational independence that prevented smooth implementation. Finally, instead of acknowledging geographical, communicational, and organizational obstacles to the internal passport system, the absolutist state utilized policing mechanisms and unjustified violence to address the failures of the passport regulations. Geographical challenges, operationally-weak bureaucracies, and police preoccupation with

passport regulation enforcement — all of these account for the enduring characteristics of the Russian passport system: fragmented applications, arbitrariness, corruption, and coercion.

Historically, the Russian state was preoccupied with its geography as a contestation between the civilized European political center, the traditional rural territories, and wild Siberian land. The dichotomy of the civilized (Western) vs. barbarian (Asian) parts of the Russian Empire was reflected in many administrative policies (Bassin, 1999, p. 6), including the organization of penal systems (Schrader, 2002), restricting movement of the "backward" peasantry (Bradley, 1985; Kotsonis, 1999) and establishing colonial administrations to modernize the "internal Orient" and its territories (Etkind, 2011). Significantly, the passport system played an important role through the codification of different types of identities that should be contained and regulated within specific territories of belonging. In the administrative sense, passport regulations contributed to the containment of the desired, non-desired, and temporally tolerable categories of the population within appropriate geographic areas. This process became central to passport administration for many years to come and was closely related to the attempts of the central political power to civilize and control its colonial subjects across regions. The passport system was also fragmented, as it worked differently within and outside of cities, and passport regulations were applied differently to different social groups.

The Russian state, geographically located in both Europe and Asia, continuously attempted to modernize itself according to certain idealistic European views. Brower, while analyzing the politics of Tsarist urbanization, suggests that St. Petersburg was designed as the ideal model of a Western city, and this model should be implemented throughout the Russian Empire (Brower, 1990). Western architecture and the official policy of "public orderliness" (p. 10) became symbols of urban Enlightenment, and city registration and police control of passport

regulations were instruments of its enforcement. The idea is quite straightforward: “a civilized European city should consist of civilized people – nobility, state bureaucrats, civil servants, merchants, artisans, and, possibly, *meshchane* (defined as a lower urban class) (p. 25). At the same time the city outsiders, peasants, and labour migrants should be kept away, as they may bring revolts and uprisings, crime, disease, and poverty (p. 26).

This idea of social sorting served as the justification for city passport regulations and accounted for permanent and temporary residency status of the city’s residents. However, the complex reality of urbanization and the growing need for cheap labour from the peasantry were constantly challenging the enforcement of this vision. The police were overburdened with the exclusively administrative tasks of determining the residential status of city newcomers, and isolating and removing potential criminals (Bradley, 1985). At the time, Moscow was described as a “big village with the characteristic provincialism, open-air bazaars, bad roads, rural style dwellings and the overwhelming presence of peasants” (Bradley, p. 65). Eventually, “civilized” cities learned to live next to the “backwardness,” to a certain degree absorbing the most successful peasants as new members of the *meshchane* class or allowing their presence through the liberalized system of residence permits for temporary migrant workers (p. 66). Police administration learned and normalized the paternalistic practice of street level identity document checks, confirming one’s residency status within a geographic area and determining any geographic and/or social stratification belongings of any suspicious individuals. The identification and removal of those who did not belong to the civilized Western Russia for criminal, political, or anti-social reasons became a central mandate of the Russian police (p. 336). The most undeserving individuals, deviants, vagabonds, homeless, criminals, and political

prisoners were banished to Siberian exile (p. 290), and they would be deprived of the right to be assigned a temporary or permanent city residency.

Siberian exile was not simply a penal system but rather an instrument of autocratic social sorting, reinforcing center-periphery social sorting, where deserving and non-deserving individuals were located based on their documented and scrutinized identity (Etkind, 2011). Even though the non-deserving population could not return to the European center, they were pragmatically exploited to develop remote territories and to maintain obedience and loyalty to the autocrat (Etkind, p. 124). Bureaucratic dedication to the regulation and expansion of the exile population became a major economic project for imperial Russia, and required intensified scrutiny over the documentation of subjects and their movements within the Empire. Andrew Gentes (2008, p.14) claims that the exiled population expansion was crucial to the Russian autocracy for managing the risks of political unrest and controlling levels of urban criminalization, as well as extracting natural resources using free labour, all while colonizing new frontiers through Siberian peasantry settlements for former *katorga* labourers (penal labourers) (p. 14). The experience of exile to Siberia was associated with physical branding of the most dangerous criminals, and the prohibition to move back to the European part of Russia, even after serving their sentence. Following the Decembrists revolt in 1825, the exile penal system embraced the administrative prosecution of political prisoners who presented a risk to the regime (p. 15).

Schrader (2000) analyzes the administrative practices of identity management applied to maintain the separation of the exiled individuals from the European center. Exiles were stripped of their estate identity, social privileges and possessions, as well as the right to reclaim their identities and reintegrate back into society. As a bureaucratic practice of identity detachment,

their passports were taken away and replaced with an exile identity document and an appropriate record (Schrader, p. 20). In another study (2002), the author brings attention to the two consequences of the Russian penal system: first, it constructed the image of Siberia as "Russia's 'other' – foreign, wild, barren and outlaw" (Schrader, p. 23) with a banished population; and second, across Russia, the system produced a suspicion of people without passports as possible fugitives from Siberian exile (p. 28).

The institutionalization of the Russian modern state during its imperial period was defined by the need of the autocrat to govern and control its subjects across an immense geographical proximity and conditions, while relying on limited population and resources. The Russian passport system was implemented following the development of European bureaucratic practices to identify its citizens and control population movement for the purposes of taxation and extraction of other obligations. However, Russian geographic conditions presented a significant barrier to implementing the central passport bureaucracy in the European manner. The policy has changed to accommodate the size of the country and the need for the development of the Eastern territories, which are rich in natural resources. As a result, one of the characteristics of the Russian passport system is the preoccupation with the restriction of the individual within a particular geographical location; delegation of passport regulation to the police and other available power actors in the region; and an establishment of the Siberian exile system where every non-documented person, under a suspicion to be a criminal, is exiled. The Russian passport was not only used to document and restrict population movement but also to define and govern imperial frontiers.

4.3.2: Documenting and Regulating Population in a Serfdom Society

In 1719, Peter I was the first to issue special decrees regulating population movements with the use of a passport, which was adopted from the French word meaning "passing a port." The document facilitated the travel of its holder across borders and was an accepted practice of international diplomacy (Lloyd, 2003, p. 26). However, the practice of carrying a handwritten document that describes the person's name and origin and permits travel within the country was well established for the peasantry in Russia in earlier periods. This practice was reflected in serfdom and the regulation of peasants' movements, namely the 1649 Law Code (Moon, 2014, p. 84). Peter I centralized and bureaucratized this requirement, not for the purpose of protecting a traditional serfdom order, but for the purpose of effective money extraction and military conscription for his modernization projects; and, consequently, for building a sovereign Russia with significant power and influence in Europe (Moon, p. 114). Peter's passport regulation of 1719 was a strategic use of the modern Western policy solution that endorsed and legalized traditional serfdom arrangements as a significant element of the modernized Russian state.

The Russian internal passport system served two objectives of the modern state in "monopolizing the legitimate means of movement" (Torpey, 2000): facilitating the extraction of the direct soul tax, and providing a basis for an effective military conscription (Moon, 1999, p. 84). As a result, the freedom of Russian commoners was constrained not only by their landlords and the traditional practices of serfdom, but also by the burden of paying heavy taxes and restrictions on residency choices. This coercive attachment of the peasantry to the land through the passport requirement institutionalized the paternalistic and controlling attitudes among policy makers in Tsarist Russia. For example, they felt obligated to protect the peasantry from the evils of capitalism, prevent labour migration, and maintain a traditional social order (Eltis, 2002, p. 333).

Stites (2008), in his research on Russian serfdom society discusses the role of the passport in regulating social stratification: Orthodox nobility, *meshchane*[6], merchants, rich artisans, and public officials were elements close to a political regime, and as loyal and imperial subjects who conformed to social norms and expectations; and in return they not only enjoyed their lives with permanent passports without an expiration date in St. Petersburg and Moscow, but also had the ability to apply for an international passport to travel abroad. However, even within the modern and civilized, there were groups of people who were more strictly regulated. Women, *meshchane,* and politically active individuals would have conditional rights to the privileges associated with the passport and would have trouble obtaining an international passport. For example, the passport regime kept women under control of their parents and husbands, who would have to agree to issue a separate passport for their daughters or wives (Stites, 1978, p. 224).

On the opposite end of the passport hierarchy ladder, there were the least fortunate people without appropriate documents or those who had to conceal their original identity due to political, socio-demographic, or ethnic characteristics: Roma people, fugitives, vagrants, the homeless, and people grouped into the category of *Ivan Nepomnyashiy*. Ivan is a very popular Russian first name, and the last name is translated as "Person not remembering his past." This was an administrative category used by police for suspected vagrants or for people who've been sent away into Siberian exile (Schrader, 2000, p. 28). Public administration in the Tsarist and Soviet periods considered these people to be potential criminals, the cause of disorder and instability, and the reason for overpopulation and epidemics in cities. They were treated in practice as non-humans who did not have any rights because they did not have an identity

[6] The ordinary residents of town, the lower urban class that did not belong to other urban categories

supported by an official paper. Many of them would be subjected to administrative physical branding by the Tsarist bureaucracy due to their anonymous status within Russian society (p. 35). The Soviet bureaucracy would similarly target groups of *lishentsy* (those deprived of political rights), the homeless, the physically disabled, and migrants without permits (Rosenthal, 2010, p. 204; Alexopoulos, 2003).

The Russian international passport has always been a characteristic of higher social and economic status and has been carefully preserved institutionally up to present times. Although everyone could apply for a passport in theory, only some would obtain it in practice. Historically, in order to receive an international passport, the person would have to justify their travel purpose to the police and support it with documents, such as the need for medical treatment abroad, which required a doctor's note. The applicant must have a regulated status in terms of his military obligation. For example, the Passport Law of 1914 contains lengthy descriptions explaining how to apply regulations in particular cases; for example, "*what to do if a young man with poor health, but serving in the army, applies for a passport to go to a mineral waters site abroad"* (Rogovin, 1913, p. 80). The author further explains that a Governor General was empowered to make decisions about international passport approval for each individual case (Rogovin, pp. 91-95). Konstantinov (2006) suggests that bureaucratic fixation on regulating the movements of the majority of the population through permits and passports probably led to a permanent administrative backlog and the institutionalized practice of bypassing the system through corruption and nepotism. The Russian international passport functioned, in an administrative sense, as the tool for security clearance and class privilege. International passports were used as a disciplinary tool for the upper and middle classes to control their level of conformity to the state regime.

In modern Russia some of these practices are preserved; the right of free movement is still a privilege for law-abiding citizens. In order to obtain an international passport, a citizen must confirm that taxation and military duties have been completed, provide confirmation of employment, complete a criminal record check, have not filed for bankruptcy, and reside at the address of their permanent registration (Kalinina, 2021).

4.3.3: The Vicious Circle of The Passport Law Enforcement

The Russian absolutist regime found itself in a vicious cycle of passport regime failures, and stricter regulations seemed to be the only solution. Every attempt to modernize the passport system was based on traditional assumptions about the peasantry, namely that they were "backward" and "uncivilized" and tended to sabotage their responsibilities to the sovereign, such as military conscription and soul tax, through many actions including passport violations, forgery, corruption, and simply voting with their feet.

The evolution of the passport system in Tsarist Russia represents a continuing attempt to reinforce the objectives of the law from 1719 and to prevent a massive exodus of serfs and peasants away from their intolerable lives and serfdom. Nevertheless, in the period from 1719 to 1742, more than 400,000 male serfs escaped and went looking for a better life in Eastern Russia and Siberia (Hartley, 1999, p. 107). Historically, only male serfs were counted in the state census for the purpose of the male soul tax (Lapidus, 1978, p. 30). The number would be more significant if it included women and children. This massive resistance to Peter's coercive modernization reforms, soul tax, and military conscription consequently triggered more restrictive passport policies and tougher regulation of fugitives.

Additionally, to this popular resistance, the Tsarist administration was not equipped for this enormous task of documenting, tracking and restricting population movement and constantly failed to implement their restrictive policies within the Russian Empire. For example, legislation created in 1726 required one to apply for an official printed passport in the urban centers where the administration was located. Everyone who wished to travel over 30 km from their place of residence was supposed to apply for a passport (Bradley, 1985, p. 107). However Russian administrative offices were not present everywhere and many people would have to travel over 100 or 200 km to apply for their passports in district and gubernia offices, even when they needed to travel just a little further than 30 km, for example to sell their produce (Anisimov, 1993, p. 235). Moreover, passports were printed in St. Petersburg and local offices often did not have enough forms to issue passports right away (Franklin, 2010). The ineffective organization of passport administration and the geographical immensity of the state, paired with the strict passport regulations for the majority of the population, facilitated the institutionalization of passport forgery markets and corrupted relations between public officials, who were supposed to enforce the regulations (Franklin, p. 221).

The internal passport system before the revolution had a clear ideological objective of restricting the movements of the population, as citizen movement might jeopardize their obligations to the state. Over 80 percent of the population was targeted, mainly peasantry (Moon, 1999; Kotsonis, 2014), and they were concentrated in urban centers located in European Russia. Despite the negative effect that the restricted movement policies had on economic development and social equality, the policies were insulated from significant reforms due to the growing role of the secret police in enforcing the passport regime, and also the fact that the nobility could not imagine themselves face to face with the peasantry outside of the natural order of serfdom.

Tsarist passport regulations were extremely complex and contradictory, allowing bureaucrats to interpret them broadly and exercise arbitrary decision-making. It was basically impossible to implement and oversee the enforcement of all the rules; therefore, every local passport administrator enjoyed significant discretionary powers, which it used it to its own advantage (Franklin, 2010). As noted, the passport regime was governed through the rule of exemptions, corruption, and social sorting based on prejudice towards certain ethno-demographic groups. For example, the main legislation that regulated the Imperial passport regime was the *Law on Passports and Residency Permits.* This law was often updated and distributed in the form of a document that covered all the amendments to this law since 1724: 359 pages of permit and passport regulations for different categories of the population – Russian Orthodox (nobles, public officials, clergy, *meshchane*, merchants, rich artisans), Polish, Finnish, peasants, *inorodtsy* (indigenous people of non-European descent*)*, *Scoptsy* (a Russian religious sect that practices castration), Jewish, fugitives, and homeless people (Rogovin, 1913).

Every group identified in the passport regulations had a different set of rights and obligations within the state, and their status was fixed in the appropriate identity document. The passport served as an administrative discriminatory tool that authenticated the status of a person within Russian society. The document or absence thereof would signal to the public official or police officer how to relate to the individual and what kind of treatment this person deserved. In surveillance studies, this process, though less transparent, is referred to as *social sorting*: "identification and classification of individuals in order to determine who should be targeted for a special treatment, suspicion, eligibility, inclusion, exclusion and so on" (Gandy, 1993, p. 15; Lyon, 2003, p. 20; Thompson, 2008, p. 145).

4.4: The Soviet Passport as a Social Engineering Project

During the Bolshevik revolution of 1917, the internal passport system was deemed to be an oppressive instrument of the previous regime, and it was substituted in 1918 with an employment record book, which soon began to function as an identification document within populated industrial centers (Torpey, 1997, pp. 849-850). Overall, the period between 1918 and 1932 was characterized by the contradictory goals of the multiple identification policies that were trying to differentiate between social groups within the working regulations. The real process of change started with the Passportization[7] campaign of 1932 (Shearer & Khaustov, 2015), initiated by Stalin. The new passport policies had political and economic objectives that distinguished it from the policies before the revolution. These policies resembled modern scientific rationality and the idea of engineering an ideal society, such as those that had driven Bolshevik policies, but which inevitably resulted in violence, coercion, and the denial of individual autonomy (Holquist, 2001).

Politically, the new passport system was constructing a Soviet citizen identity by identifying the appropriate population and eliminating the "undesirable elements." Economically, it provided the basis for cheap labour exploitation supported by redistribution policies according to one's passport status. Practically, passports were introduced only in regime cities and borderline areas, where local bureaucracies exercised a great level of discretionary power in segregating those who could stay, work and make a living, and those who had to be relocated as an "undesirable element" (Kessler 2001, p. 488). The system triggered tensions between the growing need for an unrestricted labour movement and the intensification of "social

[7] The English translation of Passportization from *Паспортизация* refers to the Stalinist campaign to document urban populations in the 1930s and reduce social expenditures. This term is commonly used in historical studies on Stalinism.

cleansing" by the police; between urban passport holders and the passportless rural population; and between the rationalized goals of the central passport office and the personal interests of local incompetent bureaucrats.

During the initial phase of Passportization in 1932-1933, passports were issued in eight cities – Moscow, Leningrad, Vladivostok, Kyiv, Kharkiv, Odesa, Minsk, and Rostov-on-Don – and only to those who were employed and socially useful. The goal was to start a "cleansing" process and relocate criminals, kulaks, and other "unreliable elements" beyond the 100-km zones surrounding the regime cities (Baiburin, 2009). This legal justification of passports as a sorting mechanism to differentiate between the loyal and the suspicious individuals determined the discriminatory nature of the bureaucratic documentation of Soviet identity. Administrative practices of identification are central to the modernization policies of the early Soviet state, and were designed to create a new "Man," and to transform human nature. Every individual was expected to provide sufficient proof that he or she deserved a passport and a Soviet identity. Proletarian or public employment, a revolutionary background, and a working-class family history were important characteristics for obtaining a passport and the privilege of remaining in the city. On the other hand, any connection to the bourgeoisie class, kulaks (middle-class peasantry), "foreign" nations, "socially alien elements," or a criminal record would qualify a person for deportation to Siberia within 10 days (Baiburin, 2021).

Passport regulations served as a crucial bureaucratic instrument of Stalin's political repression between 1933 and 1953. It facilitated urban protectionist policies and provided opportunities for local bureaucrats to increase their power and influence. All agencies that were involved in either making decisions about passports or providing additional documents to certify residence, job title, family, or criminal history developed an arbitrary power over the population.

Great numbers of desperate individuals whose passport identity was flawed in some way made for a cheap labour force that could be conscripted for industrial employment in remote and under-populated areas.

The massive scale of internal deportations between the 1930s and 1950s was rationalized and organized bureaucratically through the passport system, as was the technical possibility of segregating undesirable passport identities (Shearer, 2004). The Soviet bureaucracy did not target particular individuals in this process, but rather social groups, coding their characteristics within certain passport identities, removing these people from the political center, and trying to make them useful in an economic sense by relocating them to virgin lands and developmental projects in remote areas (Shearer, p. 853). However, this forced migration proved to be rather ineffective and generated more costs in organization and enforcement than expected revenues (Polyan, 2001). The social costs of destroyed families and communities and growing paternalistic attitudes cannot be fairly estimated. Moreover, these people were never considered victims of the regime as their resettlement was not criminal but administrative. For the same reason, no one knows precisely how many people have suffered as a result of the restrictive passport regime throughout Soviet history. At the same time, passport holders in Moscow, Leningrad, and other regime cities were enjoying guaranteed levels of social and economic security and the socialist lifestyle at the cost of the passportless serfdom (Popov, 1996; Fitzpatrick, 1996).

4.4.1: Locating Soviet Citizens in Soviet Republics

After the revolution, however, Soviet bureaucrats and the Communist party were involved in the process of breaking tradition and building a new society. The passport system as

an idea was re-implemented according to the principles of scientific rationality. It became an organizing mechanism of the Soviet Union. The Passportization campaign allowed the regime to codify and construct the new identity of a Soviet citizen who had the right to work and live in a city, and have access to the socialist welfare state. The passport regulations and the effect they had on differentiating between Soviet citizens and the alien population were crucial for industrialization, collectivization, internal deportations, and political repression.

Soviet passport regulations targeted the Jewish through the nationality rubric or the Fifth Line[8] to identify not only religious but also ethno-cultural backgrounds (Ro'i, 1995, p. 114; Baiburin, 2017). The old practices of administrative discrimination and strict control over movement of the Jewish population in Tsarist Russia were reinvented in the Soviet passport system, despite the multinational policies of the central government. Hirsh (2005) documents the conflict between the new freedom to self-determine nationality as a progressive Soviet policy, and the actual practice of the NKVD (the secret police) to determine nationality based on the available information about ones' parents since the passport decree of 1938 (p. 275). Therefore, the passport system aimed not only to minimize the risks of political dissent by removing the "undesirable" population from urban areas, but also to justify and operationalize the xenophobic and racist prejudice of public officials towards the Jewish, Crimean Tatar, Ukrainians, Polish, and other ethnicities (Lapidus, 1992; Hirsch, 2014).

This rationalized ethnic and cultural intolerance became a counterproductive practice of local public bureaucracies. On the one hand, it facilitated the arbitrariness of decision-making as it was impossible to develop an objective procedure that would determine how to classify every single individual in the ever-changing society. This decision was rather personalized and

[8] Fifth Line within the Soviet passport refers to the space to indicate nationality or ethnicity as identity attribute.

informed by the denunciation practices that were encouraged by the NKVD. On the other hand, public officials functioned within local politics and interests that often conflicted with the central policy goals. Their application of passport law was driven by the similar "cleansing" logic. As a result, the discriminatory practices of relocation, restriction of movement, and denial of services became a significant bureaucratic procedure associated with passport regulations. Regulations helped to introduce xenophobia and irrational hatred into the legalized procedures of exclusion and discrimination. Both regimes were inspired to fixate identities, to find important characteristics that would attach a person to a position within society, and to prevent him or her from challenging the hierarchical order.

The categories of population, once defined and constructed as undesirable in regime zones, were internalized across the Soviet Union, both within bureaucracies and in everyday life (Shearer, 2004). The reaction to the growing number of outcasts was massive relocation conducted by the local administration to non-regime areas (Chernolutskaya, 2011; Polyan, 2001). Local passport administration offices were understaffed, incompetent, and they often misinterpreted regulations: many elderly and dependent individuals were denied passports and classified for relocation due to their inability to work (Chernolutskaya, p. 26). Categories of people relocated from the first eight cities would suffer second and third waves of relocation because local government offices wanted to avoid suspicious residents. Chernolutskaya further describes the hardships of people with a stigmatized passport identity as they suffered continuing relocations: "…their possessions were confiscated, and families had to walk with little children over 100 km, waiting for transportation for several days under the open sky and in hard weather conditions (p. 76). In 1934 alone, more than 100,000 people were relocated within the Russian

Far East and many of those cases were illegal based on the wrong interpretation of the passport regulations by local administrations" (p. 189).

Some authors describe the sorting mechanism of the Soviet Union's internal passport system as a division of all residents into three types of zones with different security requirements: "regime zones," "non-regime zones," and "extra-administrative zones" (Hirsh, 2005, p. 275). Regime zones were restricted to people with passports that were circulated by the secret police to "reliable" Soviet citizens. All passportless individuals, as well as "unreliable citizens," would ideally be relocated to non-regime zones, while extra-administrative zones would include labour camps, the Gulag, and secret urban centers that were excluded from the official maps. The information about a criminal conviction or a term in extra-administrative zones was fixated in the passport and prevented a passport holder from relocating to Moscow, Leningrad, and the capitals of the Soviet republic. This "cleansing" practice was in place until 1988 (Hirsh, 2005). People who suffered from their passport identity during Stalinism were never rehabilitated because they were never on paper as being repressed or prosecuted. They were not seen by law enforcement or the judicial system as individuals but as part of a group. They were denied the basic right to appeal, or to enter into any kind of paper-based relationship with the modern government. They were relocated by ordinary bureaucrats without any involvement of the judicial system.

Many of them chose to migrate and hide, suspecting that the only identity they might receive from the State would be an undesirable identity (Baiburin, 2012). For example, Fitzpatrick, in *Everyday Stalinism* (1999), refers to the Soviet citizenship campaign as a "large-scale concealment of social origin and misinterpretation of identity" (p. 137). Obtaining a passport provided the security of a new legal status, sometimes through bribes, document

forgeries, marriages/divorces, or adoptions (p. 133). To prevent this massive identity concealment or "identity masking," the state would rely on the growing discretionary power of the police and bureaucrats during the "unmasking" process that, in turn, relied on "denunciation by neighbors, colleagues, and schoolmates" (p. 135). The process of identity masking was a popular reaction to the restrictive passport policies and the arbitrariness of passport administration. In a sense, it can be viewed as social resistance to excessive state surveillance, and it was addressed by the state with the strictest regulations and punishment for non-compliance.

Baiburin (2021) describes territories regulated by the passport regime as "transparent" zones and territories beyond as "grey" zones, offering a dichotomy of urban control by police surveillance vs. control by restriction of movement (p. 98). Transparent zones were populated by people with passports, which granted them the right to work, study, live, and receive social assistance from the state. These people were often "masking" their Soviet identity to achieve this special status and the associated benefits. In the grey zone, people were preoccupied with identity concealment, hoping to obtain a status which would permit free movement in the transparent zone. The author concludes that the Soviet internal passport was designed to categorize the population as "clean" (i.e. checked) and "non-clean" (i.e. suspicious) individuals (p. 319), and that it helped create a social landscape where European and border territories offered a significantly better socio-economic lifestyle and more opportunities for its residents compared to central, rural, and Siberian territories. Another effect of the Soviet passport was that criminal activity was "geographically redistributed away from large cities" (Morton & Stuart, 1984, p. 249). However, the geographical containment of persons with a criminal past does not address the problem of criminality in society, and this practice helps concentrate criminal activities in certain geographic areas.

The cultural and institutional legacy of the cleansing power of the Soviet passport era persists today in Moscow and St. Petersburg, which are often referred to as "states within a state" (Light, 2010). The administrations in these cities are continuously reinforcing local passport regulations and procedural exemptions from the residence registration law, which protects their permanent residents from the possible dangers associated with the aliens' categories: labour immigrants, visitors, temporary residents (who are blamed for shortages in social and health services), traffic jams, criminal activities, and epidemics (Reeves, 2015). For example, the Moscow Social Card and the Universal Electronic Card were issued only for local residents with a permanent registration stamp in their passport (www.mos.ru/karta-moskvicha/). A number of authors compare the current passport registration regime in these cities with the restrictive policies during communism (Bovt, 2013; Light, 2010; Lonergan, 2013), and see it as an illustration of the long-lasting Russian practice of restricting the movement of unreliable people to the political centers, or at least limiting their access to public services based on their residential status.

4.4.2: Enduring Passport Practices from the Tsarist and Soviet Regimes

The Russian internal passport system follows fascinating historical trajectories that navigate between the uncontested policy visions of the country's leaders and the limited policy capacity of the state to implement them evenly across challenging geographic, economic, political, and cultural conditions. Passport regulations before the Bolshevik revolution were subordinated to the fundamental vision outlined by the reforms of Peter I in 1719: "no one may leave their place of permanent residence without a legitimate permit or passport" (Mood, 2002, p. 327). This vision was never challenged in terms of bureaucratic rationality and effectiveness;

rather, during the period between 1719 and 1914, passport regulations were reformed through minimal reactions to the pressures of social change and bureaucratic failures. This incremental character of policy changes was significant in preserving the internal passport requirement in Tsarist Russia, despite the contradictions it produced. On the contrary, Soviet passport regulations employed a logic of scientific rationality and focused on the narrow but effective — in a bureaucratic sense — implementing the passport regime within urban centers. Beginning with several important cities in 1932, the policies expanded across urban areas after WWII, and by 1974, the internal passport was a universal requirement across Russia.

Therefore, the scope and target groups of the two passport regimes were different, but the driving beliefs and assumptions about the need to restrict population movement were similar. Imperial Russia was trying to restrict the movement of peasants across the empire by requiring them to re-apply for a passport anytime they moved from their permanent location. Soviet Russia, on the other hand, excluded the immense peasantry from the passport regime and, instead, focused on the *passportization* (Kessler, 2001; Shearer, 2009) of those who were loyal to the regime — i.e. the urban proletariat that was close enough to the public administration and its social networks. The Russian passport was, consequently, transformed from a handicap for the oppressed in the Tsarist regime to a privilege for the proletariat in the communist regime. However, in both cases, the internal passport regime significantly harmed the Russian peasantry and, more generally, people who were traditionally removed and excluded from political participation. The internal passport requirement for a commoner in Russia institutionalized a feudal relationship between the absolute and his subjects, between landlords and serfs, and

between *nomenklatura*[9] and socialist workers. It manifested a type of primordial inequality of the Russian subjecthood that was reinvented at different times in different forms.

Several authors characterized the development of the Soviet passport system as a reinvention of the Tsarist passport regime (Popov, 1996; Garcelon, 2001). Passport legislation was implemented in Tsarist Russia to control the movement of peasantry and to enforce their financial and military obligations to the state. The monopoly of the Tsar's control over his subjects' movement was a cultural and political idea that reflected the natural order of serfdom. Despite bureaucratic ineffectiveness in maintaining this passport system and the failures to respond to social and economic challenges, the system was never seriously challenged before the revolution in 1917.

State identification systems in Imperial and Communist Russia were designed to distinguish between the population that was loyal and supportive to the state and the population that was prone to troublemaking. Both were institutionalized as a method of social sorting, which became significant for any type of social interaction. On the one hand, there were individuals who, through their everyday life activities, demonstrated to the State appropriate, civilized, social behaviour. On the other hand, there was the "suspicious population:" uneducated, traditional, exotic, which was always considered an indigent majority. David Shearer (2004) characterizes the Soviet passport system as "geographically specific and socially hierarchical," a system that reinforces the dichotomy of the elements "near and far" in relation to the absolute, or, later, to the political center of the Communist Party (p. 838). The passport system was designed to keep those groups apart and under surveillance.

[9] Nomenklatura – people who held administrative positions within important industries and the government

In general, while the Tsarist passport policies preserved the historical differences within serfdom society, the Soviet passport created new types of differences and inequalities. Both systems reinforced an absolutist model of the State, where power was not limited by the rule of law, and individuals were subjected to the arbitrariness of bureaucratic decision-making (Giddens, 1986). Although the scope and intentions of the passport systems in these two regimes were different, the continuity of the cultural importance of passport identity is apparent. Every person without a state documented identity is a potential suspect and, at the same time, a state-issued passport can conceal any identity (Bradley, 1985; Chernolutskaya, 2011; Baiburin, 2017). Therefore, everyone who had the ability would strive to obtain the desired passport identity, whether through corruption, forgery, or social exchange (Franklin, 2010; Fitzpatrick, 1999; Baiburin, 2021). The organizational implementation of the passport policies in the geographically fragmented Russian state allowed for multiple contradictions, which undermined the initial policy goals of the central political power.

4.5: Reforming the Post-Soviet State Identification System and Institutionalized Legacies

Overall, the social sorting mechanism of the internal passport, in the Tsarist, Soviet, and Post-Soviet periods, supports a continuing trend of classifying the population based on their documented identity information with a subsequent decision: either to allow the person to reside in certain geographical areas, or to remove him/her to the socio-geographic "dumping ground." To some extent, this practice is preserved today. In a cultural and institutional sense, it establishes the superiority of certain cities through the practice of routine passport checks by police, access to public services based on one's registration stamp, and regulated hiring practices which require employers to verify passport registration and sometimes, conscription status of the potential

employee. This geographic superiority poses a serious dilemma for public administrators and the police: try to maintain a sorting function of passport and registration stamps in a challenging social reality, or apply it sporadically and benefit from arbitrariness and bribery. As noted in comparative studies on identification practices, “attempts of total control are doomed to failure as it mutates under influences of the new social and economic circumstances” (Caplan & Higgs, 2013, p. 7). These mutations are contradictory results of the passport regulations. Practices that survived changes in the political regime become part of the institutional life of police, public administration, and citizens. Practices that are part of peoples’ everyday lives are culturally accepted as normal and appropriate. The analysis of post-communist reforms to the state identification system reveals that policymaking is often constrained by the institutionalized legacies of former regimes.

4.5.1: Liberalization of the Soviet Ministry of Internal Affairs

The Stalinist passport reforms were limited to extending the rights of all Soviet citizens to apply for and obtain a passport. Only in 1974, under pressure from the Soviet Ministry of Internal Affairs (Ministerstvo Vnutrennikh Del - MVD), was every person over the age of 16 granted the right to apply for and receive a passport without additional bureaucratic procedures (Kirichenko, 2014). Kirichenko argues that a new universal passport system for all Soviet citizens was driven by expanding industrialization and urbanization, which required significant migration within a country that was not limited anymore by strict state policies. On the contrary, the movement of labour, especially from rural areas, was facilitated and encouraged by the state (Kirichenko, p. 708).

However, the change in policy was not a sign of liberalization but rather an indication of the growing power of the Ministry of Internal Affairs in determining and implementing

citizenship policies and strengthening control over movement of the population. The Ministry of Internal Affairs has consolidated its position through the standardization of passports, the collection of personal information, and the policies and practices across all territories of the Soviet Republic and for all categories of the population. The Ministry implemented the new policies through local passport offices, who have direct contact with citizens. This involved verifying and updating citizens' standard personal identity information, issuing new passports, and managing movement of the population through documentation of the permanent and temporary residential address(es) of the passport holder (Kirichenko, p. 709). The practice of residential registration continued to limit and control free movement within the Soviet Union, as passport offices required evidence supporting a change in registration.

As a result, even after the collapse of the Soviet Union, the post-Soviet passport reform, which took place from 1997 to 2003, was primarily the responsibility of the Federal Migration Service (FMS), an agency of the MVD (Russian Federation Resolution nr. 828, 1997). Its high rank military officers, responsible for law enforcement, were also involved in justifying, drafting, and implementing the organizational regulations, authorities, and mandates under the Russian Constitution and Federal state identification system legislation (Semukhina & Reynolds, 2013). The reforms were internally driven by the institutional logic of preservation and expansion of the existing administrative practices, so political, cultural, and social embeddedness of the passport system's legacy revealed itself significantly as an outcome of the modernization. The Russian government failed to critically assess the rationale and need for the internal passport within the new realities of liberalization reforms and democratization. Primary address registration was not subject to liberalization. On the contrary, it was reinforced. Temporary registration was required for visiting other places within Russia for a period of 90 days or more, within three days of

arrival (Korenev, 1999). The accuracy of this registration stamp was important for daily life in Russian cities, especially in St. Petersburg and Moscow (Semukhina & Reynolds, p. 146), as identity verification was required during employment, and to apply for government services, such as education and public health.

The main goal of the passport reforms that took place from 1997 to 2003 was to introduce a new passport template for citizens of the Russian Federation, as well as to stop the circulation of old Soviet passports. The goal of exchanging Soviet passports for Russian Federation passports in six-year period[10] was to develop and circulate a new type of paper-based document within the same militia administration, but also to separate Soviet citizens who can be naturalized as citizens of the Russian Federation from immigrants who originate from the newly defined post-Soviet states. As a result, the organizational framework and practices remained unchanged: the residence registration, the role of the Ministry of Internal Affairs, the role of the local passport offices and their relationship with the police, as well as the distinction between internal and foreign passports all remained the same. Russian policymakers failed to liberalize the passport system and institutionalized identification practices by separating it from the law enforcement and national security agencies, and rather cemented a police-centered passport system for the next decades.

However, the technically updated document, with a new Russian symbol on the cover and machine-readable pages inside, has carefully preserved many things from the former passport systems. I found a video from an MVD press-conference, held on June 22, 1997, which depicted Vladimir Kolesnikov, the First Deputy Minister, presenting a technically updated

[10] The Soviet Union collapsed in 1991, but until 1997 citizens of the Russian Federation were still using Soviet passports for identification purposes.

passport that would replace the former Soviet passport and its negative Communist practices. The video demonstrates how powerful MVD officers were in rationalizing the old Soviet passport practices within the new liberalized legislation. Reacting to the critical comments from journalists regarding the preservation of the two passports (internal and international), and preserving the residence registration requirements, Kolesnikov explained that "every country has its own passport rules that have developed historically and culturally. We have a law about freedom of movement and residency, about Russian citizenship, a Housing Code of Russia and our passport regulations do not violate these democratic laws… we need to observe everyone's rights, that is why we need a residency registration…or otherwise imagine you come home and there is an unknown person who says he is registered at your dwelling" (Kolesnikov, 1997).

Despite his efforts, Soviet terminology and practices were present in his speech, emphasizing the path-dependency of the passport system. Instead of *private property,* the term *zhylploshchad'* (living space allocation) was used, and freedom of movement was carefully described as lawful and logical limitations of the registration requirement. It was clear that the system did not change at all, but instead, bureaucrats spent a significant amount of time since 1991 adjusting, translating, and negotiating old passport practices into the new 'democratized' system. The MVD presented two passports for international and internal use, and explained why the requirement of registration at one's place of residence was an important part of the passport system, and could be implemented without violating freedom of movement (Kolesnikov, 1997). This reform also addressed the new policy problem of differentiating between Russian citizens and immigrants from all post-Soviet republics. The practice of establishing Russian citizenship was related to the last stamp of residency registration on the Soviet passport, within the geographical borders of the present Russian Federation, as of November 6th, 1992 (Kolesnikov,

1997). Consequently, people who were privileged by the Soviet passport system and had a residence registration record in Russian cities easily obtained Russian citizenship. However, there were many cases where people did not have a residency stamp or had it in another republic due to their work or for other reasons. Therefore, although they were born in the Russian Socialist Federative Soviet Republic, they could not be granted Russian citizenship.

To address this problem, the MVD directed unresolved citizenship disputes to the President, who would issue a decree on a case-by-case basis. In 1997, there were 3,000 cases awaiting Presidential decree (Kolesnikov, 1997). Overall, the passport reforms that took place from 1997 to 2003 revealed the decisive role of the Soviet Ministry of Internal Affairs as a dominant policymaker, insulated from constitutional oversight, public inquiries, or consultations. As a result, Russian citizens received, basically, an old passport system that was slightly adjusted to satisfy the minimal requirements of the "democratic transition." The state identification system under the control of the Ministry of Internal Affairs proved to be resistant to changes.

4.6: Conclusion

This chapter has identified a number of historical legacies in the Russian identification system that resulted in conflicting identification practices based on strict, police-centered control of population movement within the country, and a rewarding system of social benefits for passport holders linked to their residential records stamp. This was a social engineering project to encourage civil obedience, where loyalty and appropriate behaviours were rewarded with a document symbolizing inclusion, and better standards of living.

The findings of this chapter are crucial for the analysis of the Universal Electronic Card as a reflection of the unique cultural, social, and political practices of identification that were

institutionalized historically. This historical analysis establishes the foundations of "local knowledge" regarding the Russian identification system, and its traditional practices which are accepted socially and culturally and embraced institutionally as appropriate. This chapter showcases the historical legacies of state identification policies and explains how formal and informal passport practices survived regime changes and policy reforms, reproducing a unique, passport-centered, political culture. The historical analysis of the policies and institutionalized practices of the passport regulations draws our attention to the uncontested assumptions and policy myths about the cultural meaning of the passport in Russia. This cultural meaning is crucial for understanding how the UEC innovation would, and would not, adapt to the institutionalized realities of Russian passport politics. Chapter 7 will illustrate how the historical legacies of the passport practices can be generalized through concepts of the Russian absolutism, subjecthood and imperialism and how these ideas can explain the contradictions and clashes of the instrumentalist perspective on eID innovation with the institutionalized practices of the state control over technology, territory, and population.

In the next chapter, I analyze the implementation of the Universal Electronic Card. The Russian government initiated the project based on the experience of the Moscow Social Card (MSC). In my analysis, I draw analogies between the Moscow government's implementation of this card and the Soviet and Tsarist regimes that were preoccupied with control over movement of the population within the capital. The analysis of the MSC project is important not only to understand why the Russian government viewed it as a good model which could be transferred to other regions, but also to recognize the historical trend of using progressive Moscow-based innovations to modernize the rest of Russia. Critical analysis of the Moscow Social Card's surveillance mechanisms and its consequences for the population uncovers embedded social

sorting, which reinforces the historical legacy of classification and separation of the Russians with Moscow identity documents deserving benefits based on their documented identity. I also identify the interests of the institutionalized MSC Card Cartel, and illustrate how its key stakeholders have influenced the justifications and technological design of the Universal Electronic Card. I document the achievements and shortcomings of the UEC Card Cartel through analysis of the special legislation, organizational framework, and technical design of the card, and problems with its implementation across the Russian Federation.

Chapter 5: The Universal Electronic Card Implementation: Bringing the Moscow Social Card Experience to the Regions

5.1: Introduction

This chapter connects the case of the Universal Electronic Card (UEC) project, active between 2010-2017, with the preceding implementation of the Moscow Social Card (MSC) in the late 1990s, introduced as an electronic multifunctional identification and transactional instrument. The Russian government considered the MSC project to be the most suitable and practical policy solution to learn from and apply to federal reforms of the national identification system (Borodina, 2013). This example of the policy diffusion as a process of learning from early adopters to help shape policy (Shipan & Volden, 2008) not only helps to identify the important drivers for the Universal Electronic Card, but also, based on experience from the Russian capital, illustrates the historical importance of the state and its functions in establishing an appropriate state identification system.

This chapter describes and analyzes commonly available facts about the implementation of the UEC as a policy instrument. I apply an instrumentalist perspective and demonstrate how the UEC legal framework and technical infrastructure were driven by the Moscow Social Card experience. I show how the key stakeholders were focused on digitizing government and municipal services for city residents across Russia as the first step towards the national electronic identification system. I argue that the public-private partnership, "Joint-stock company Universal Electronic Card" ("JSC UEC") is a Card Cartel that operates on similar principles as the Moscow Social Card Cartel, but on a different scale. To support this argument, the chapter first describes the Moscow Social Card's technical infrastructure, design, and organizational framework, and shows how the UEC mirrored this approach. The Moscow Social Card is not only an electronic

identity document, but it also supports the provision of social assistance in the Russian capital, traditionally provided in the form of free services or in-kind benefits (such as transportation, food, medical services, drugs) to certain social-demographic groups (retirees, students, veterans, mothers of small children). Following this, I apply a critical perspective, demonstrating how historical legacies of Russian state identification practices, with their classifications and hierarchies of the urban population, facilitate surveillance and social sorting, segregating deserving populations, observing their behaviour, and rewarding them with beneficial services or limiting access to others.

5.2: The Significance of the Moscow Social Card

The first Russian Universal Electronic Card was issued in 2013, but the prototype had existed in Moscow since 2009 in the form of the Moscow Social Card (*sotsyalnaia karta moskvicha*), an electronic identity card which regulated access to social services as well as access to public transportation for specific demographic categories of the population. Initially, the Moscow Social Card was designed to ensure a broad and inclusive policy of social guarantees, as was the case in the Soviet Union.

Historically, Moscow was a city with a higher standard of living and a more comprehensive system of social guarantees compared to the rest of Russia (Brainerd, 2010). The population of Moscow was continuously growing during the Soviet Union, but after the liberalization of the city registration regime in 1997 and the loosening of restrictions for labour immigrants from the post-Soviet state in the 2000s, Moscow has seen dramatic population growth. The total population grew from approximately 9 million in 1991 to 12 million in 2015 (Rosstat, 2015); however, some argue that almost 1 million of the Moscow population were not

documented and constituted illegal immigrants (Reeves, 2015; Schenk, 2018). Subsequently, the ever-expanding resident population substantially challenges the existing welfare system. However, the population is only one side to the problem; the other is a communist legacy of in-kind benefits. Social assistance in the Soviet Union was delivered through the system of "in-kind benefits" or *l'goty* (financial privileges or discounts based on eligibility), such as free transportation and health care, allocated to various categories of citizens, regardless of their actual economic situations (Henry, 2009, p. 54). It was a way of recognizing personal contributions to the country: war veterans, work heroes, mothers, public officials, or police officers. Instead of rewarding them financially, the system rewarded them with free social benefits fixed to their personal identification documents. This system was able to survive the Soviet Union collapse and was extended across post-Soviet states (Henry, p. 61).

One of the most negative consequences of this legacy was the preservation of free transportation services for all of these categories of people, and widespread falsification of the *l'goty* documents. For example, before the Monetization reforms of 2005, there were 70 categories of *l'gotniki* (individuals eligible for benefits and discounts) in Moscow, roughly 60% of the city's inhabitants, who had the right to use municipal transport free of charge or with a substantial discount (Maltseva, 2012). Free social benefits and services became a burden for municipal budgets and infrastructures across the country, but at the same time the continuity of this policy remained a political priority at all levels.

In 2004, the federal government implemented a new policy of social benefit monetization, replacing formerly free services. The new realities of the market economy required that people entitled to social benefits would be counted, sorted into categories, and addressed differently. The Moscow government was the first city council in the Russian Federation to

advance control over the redistribution of benefits to certain social groups, and implemented an electronic social registry and the Moscow Social Card for this purpose (Moscow Government Resolution 962-ПП, 1998). The success of the card was acknowledged at the Federal level and, in 2010, the idea of electronic identity cards, as a tool of providing governmental services for the entire population, entered policy debates (Commission for modernization and technological development of Russian economy, 2011).

The Moscow Social Card was mentioned for the first time in official documents back in 1998 as part of the anti-crisis policies. Since 2002, it has been embraced as a tool to support the technological modernization of public administration within a regional program called "Electronic Moscow" and a federal program called "Electronic Russia" (Sister, 2003). Although the Moscow Social Card was officially framed as a tool of the e-government reforms, its implementation had little to do with the transformation of the state identification system. Instead, it was an opportunity not only for tighter fiscal control over welfare spending by providing it only to residents with a verified record of place of residence (resident registration), but also for the facilitation of the e-commerce practices that were thought to be a solution to the current economic crisis.

The smart card was created to popularize cashless payments within the Moscow economy, and protect the most vulnerable citizens of the megalopolis after the biggest currency crisis in the Russian Federation in 1998 (Chiodo & Owyang, 2002). The currency crisis resulted in massive devaluation of the ruble and defaults on public and private debt. Moscow policymakers suggested that the card would become a solution to two problems: (1) it would allow for the collection of more accurate and timely information about individuals using social benefits, making the welfare system transparent and efficient; and (2) it would facilitate the

development of the cashless economy and minimize the risks of currency fluctuations (Moscow Government Resolution nr. 962 ПП, 1998). At the time the policy was developed, this innovation resonated with the practice of food stamps within the realities of growing unemployment and a high inflation rate, rather than with the technological revolution in the public administration. The focus was on the payment function of the card: the government would deposit financial benefits to the cardholders, and they would be able to pay for public and private services using the MSC as a payment card (962 ПП, 1998, art. 1.9-1.10). The interpretation of this ambitious vision of a policy instrument that would provide multiple solutions to a whole range of social problems illustrates how the post-Soviet government was trying to reclaim central bureaucratic control over multiple policy sectors.

Additionally, the technology of the smart identity card was interestingly connected to the modernization of the Moscow transportation system that opted for electronic passes in 1996, to allow greater control over the free and discounted transportation services for retirees, veterans, students, and some public sector employees (Gayev & Marchenko, 2003). The Head of the Moscow Metro, Dmitry Gayev, was appointed general designer of the Moscow Social Card in 2001 (Moscow Government Directive nr. 585-РП), and until 2011 was responsible for the "multifunctional design of the card as the most cost-effective strategy that will allow cardholders to access transportation services, pay for municipal services, regulate access to medical care, and, possibly, grow into new functions in the future" (Marchenko, 2005, p. 23). One of the practices related to this idea was the continued attempts of the city government to implement regulatory control over all possible spheres of city life through the digitalization of old bureaucratic processes, reinventing a centralized management role for the city similar to the communist approach to urban management.

Russian experts have identified common problems plaguing the financial management of municipal infrastructure in the Russian Federation through an enormous centralized hierarchical public institution – *ZhKH* (*zhylishchno-kommunalnoe khoziaistvo*) – and failed de-centralization reforms (Bashmakov, 2004; Ivanov, 2011). ZhKH is responsible for water management, electricity, garbage removal, snow removal, heating, gas, elevator management, building management, civil engineering, and so on. Every resident must pay this monopolistic organization for home utilities, and residents have no choice or control over the quality, price, or amount of services used. All of the services are obligatory; no opt-outs. The Moscow Government introduced the Moscow Social Card to facilitate payments to this institution, basically enforcing citizens' obligations to finance the current municipal infrastructure but also providing municipal discounts to some groups.

The status of belonging to the privileged groups with discounts could be acquired through a bribe, or it could be a part of the employee benefits of public officials. In 2014, there were 3.6 million Moscow residents who do not pay full price for municipal services; they received a Moscow Social Card that documents their right to municipal discounts from 30% to 100% (Popova, 2014). Popova argues that the existing system is not transparent or accountable, may be influenced by corruption and contributes to ineffective pricing policies where people who do not qualify for a municipal subsidy and cannot apply for a Moscow Social Card pay double the market price. It is true that more people switched from the traditional methods of payment using cash to the online banking system. However, this transition to digital transactions benefited few financial institutions, as Moscow government selected a bank to support MSC.

Thus, a Card Cartel was initiated when the Moscow Government decided to add a digital payment function supported by Visa Electron, and managed by the Bank of Moscow (Dorokhov,

2003). This transition monopolized the public sector's financial transactions, including transaction fees for payments supporting social benefits and municipal services. Between 2003 and 2010, management of the MSC has significantly increased the Bank of Moscow's number of clients, roughly by 6 million (Global Mass Transit Report, 2011), contributing not only to increased financial surveillance of card holders and recipients of public services, but also facilitating institutionalization of the Card Cartel.

5.2.1: Card Design, Technical Infrastructure and Personal Information Policy

Another goal of the Moscow Social Card is the collection and systematization of socially-significant information (Moscow Government Regulation, 962 ПП, 1998; 585 –РП, 2002). However, the scope of information collected within the MSC system is defined by the technological capabilities of the cards and associated infrastructure rather than any data protection or privacy regulation. The unrestricted character of the smart card is framed as an advantage, and the methods of data collection and sharing mechanisms are not discussed in much detail in public documents. On the contrary, the idea that technological progress should not be restricted is prevalent; any information about the socio-demographic characteristics of Moscow's population, their behaviour involving the use of monetary and non-monetary benefits reflected in smart card usage, may provide important evidence and inform new targeted programs of social assistance and facilitate infrastructural development in Moscow. Analysis of the MSC's technological design, connected databases and policies regulating the collection, use, and disclosure of the cardholder's personal information, supports the statement about intentionally broad purposes of the card design, including the possibility of reuse for other lawful purposes.

The regulatory acts outline that the Moscow Social Card is based on the *Uniform Registry of Social Beneficiaries* and contains sets of databases including *personal information* of the card holders and *records* of the social benefits provided, along with the financial benefits (pension, child benefits, subsidies, stipends), non-financial benefits (use of transportation, medical services, public school services), retail discounts (loyalty program for cardholders), and online access to e-government services (Moscow Government Bylaw nr. 780-ПП, 2014). Eventually, every time the cardholders swipe their cards in the reading devices, the electronic record is generated and then accumulated in the appropriate database. However, it is not only public administration that has access to the information generated by the cards, but also the private sector that provides payment services for the card, including the Bank of Moscow, Visa Electron, and Master Card. For example, Visa has filed several patent applications that provide analytics based on transaction history: "the transaction profiles provide intelligence information on the behaviour, pattern, preference, propensity, tendency, frequency, trend, and budget of the user" (Steele, 2015, para. 5).

Between 2002-2016, the Moscow Social Card was available exclusively through the municipal "Bank of Moscow" and in cooperation with Visa Electron. The card, branded with VISA Electron and the bank logo, was used across Moscow to distribute pensions and other social benefits. The cards had a magnetic stripe with 16 memory sectors; three consisting of general information and 13 designated for a separate government department and protected by private key access (Rosan Finance, 2003). The fact that personal purchasing history was collected and analyzed for consumer surveillance and the development of personalized products and ads is not mentioned specifically in the regulations. However, on the official website of the Moscow Government (2016), in the section pertaining to the Moscow Social Card, there is an

offer for those wishing to join the registry of the businesses providing services to the population receiving social assistance, and to thus be included in the "Moscow Social Registry". This type of partnership offers technical and marketing support, including access to analytical reports containing aggregated data generated from the use of the Moscow Social Card. Moreover, the purchasing history of the welfare population is interesting to public administration, namely to better control social benefits spending. In 2019, this cooperation moved towards the system of digital certificates, with points awarded to eligible citizens which can be exchanged for products or services sold by Moscow businesses. This points system is also processed through the Moscow Social Card. The use of points is monitored and any exchanges involving alcohol or cigarettes are blocked automatically (Department of Labor and Social Protection of Moscow Residents, 2020).

In 2014, the Moscow Social Card (MSC) became a more technologically advanced card in cooperation with MasterCard. The new card is multifunctional instrument with an EMV (Europay, Mastercard, and Visa) micro-chip and touchless PayPass technology, supported by a mobile Android application for banking transactions (Moscow Social Registry, 2015). The EMV chip would allow more information to be kept on the card and would support more applications, therefore increasing the functionality (Il′in, 2014). This involvement of the private sector in the technological design and service of the government identity card creates challenges not only for the protection of the cardholder's personal information, but also for sufficient data security.

The Moscow government delivers the MSC project through a network of public-private partnerships, and the process of data-sharing is addressed within *The Moscow Social Registry Data Processing and Security Policy* (2014). This document repeats many positions of the

Federal Personal Data Law from July 2006 (nr.152-FZ), which also identifies Roskomnadzor,[11] a federal agency under the Ministry of Digital Development, Communications and Mass media, which is generally responsible for censorship of the Russian internet but also for protection of personal data of Russian residents. In 2015, the Personal Data Law was amended, providing more control functions to the Roskomnadzor and the ability to conduct audits of the IT firms and internet providers operating in Russia to ensure that "collection, systematization, accumulation, storage, updating, and disclosure of personal data of Russian citizens are performed through databases located in Russia," including in response to to direct privacy complaints (Turovsky, 2015). The problem is that this is the same institution that conducts state surveillance over social communications, blocks internet content, and cooperates with security agencies and the judicial system in providing evidence of extremism and pornography cases. Some experts even suggest that the most important and time-consuming function of this institution is political censorship and persecution of the opposition (Turovsky, para. 4). Furthermore, article 6.3 of the MSC privacy regulation states that "personal information collected by the Moscow Social Register can be accessed without informing the person by the court, police and security agency based on their motivational inquiry" (The Moscow Social Registry Data Processing and Security policy, 2014). As a result, the personal information of the cardholders is not protected and can be accessed routinely by state agencies, including law enforcement, without knowledge of the card holders.

Another problem of this personal data policy is that it regulates identity information management only within the Moscow Social Registry, a municipal organization that delivers the Moscow Social Card program and manages the *Uniform Registry of the Social Beneficiaries*. However, this organization functions within a broader framework of organizations, including

[11] The Federal Service for Supervision of Communications, Information Technology and Mass Media.

ones from the private sector. It is an organization within the *Moscow City Department of the Informational Technologies* that also oversees five other information and technology-related organizations and programs: E-Moscow, InfoCity, Moscow Municipal Telecommunication Agency, The Consumer Market Analytical Center, and The Production and Technology Municipal Center. These organization have legitimate access to the information collected by the registry and provided to the third-party organizations for legal purposes directly related to the delivery of the Moscow Social Card program. The Moscow Social Registry publishes a regularly updated list of service providers, elements of personal information shared with them, and associated purposes of use (Moscow Government, 2015). All of these organizations are interconnected, but at the same time, function within the different domains of city politics. The functional division of the municipal organization is partially influenced by the decentralization reforms but also preserves some of the historical institutional practices, especially in terms of the collection and monitoring of different types of urban information. There is a lack of clear separation between personal and public information, basically in terms of information management – all information available to the city is deemed critical for policymaking and never addressed within privacy protection standards. This leads to the monetization of personal information without the individual's consent.

Finally, the most recent example illustrating the surveillance capabilities of the MSC and the practice of unregulated collection and processing of the personal information of cardholders for new purposes, was a targeted reduction of Moscow transportation usage by certain categories of the population during the Covid-19 pandemic. On October 9th, 2020, the Moscow Mayor issued a decree to block social Moscow Cards with transit pass functionality for K-12 students (as schools were temporarily closed), people over 65, and people with chronic diseases (Moscow

Mayor Decree, 97-УМ). However, it was established by reporters that over 33,000 people, not belonging to the identified categories, had their cards blocked for unclear reasons (Kork, 2020). After a series of complaints and media engagements, the municipality has officially confirmed that cards were temporarily discontinued for pregnant women and people with chronic illness based on the information included within the Moscow Social Data Register (Buranov, 2020).

In 2021, the Moscow Government officially extended use of the Moscow Social Card to support vaccination mandates for travelling on public transportation, and blocked all the cards for unvaccinated users with the exemption of people with certain chronic diseases, pregnant women, and those recently recovered from Covid (Interfax, 2021). This example illustrates technological function creep, when broadly defined design of technology provides new possibilities for reuse of the collected personal information without the knowledge or consent of individuals.

Another example is the preventive arrests and conversations with some students in the Moscow metro on Russia Day (Meduza, 2022), which can be explained through a panoptic concept proposed by Gandy (1993): the invisible and comprehensive surveillance of individuals based on classification (MSC cardholders who are also students), evaluation (were any of these students involved in any protests previously), and sorting (using facial recognition and surveillance cameras in the metro to locate the students on June 12) for application of disciplinary measures defined by the political elites in control of the MSC panoptic sort functionalities. These examples are a departure from the initial idea expressed by Dmitry Gayev, the general MSC designer, that electronic identity cards would simplify the use of public transportation and increase efficiency of public spending.

The messiness of the organizational functions and information policies requires a standardized approach to the identity information management system, in order to provide a regulatory framework for data-sharing principles, data protection, and security programs. Without this city-wide identity information management framework, the Moscow Social Card project could not provide an efficient level of data protection, meaning that it is not only personal information that is at risk but also any government information. The weak privacy policy, paired with the strong e-commerce orientation of the Moscow Social Card policy-makers, contributed to the development of the unique policy environment that focuses on market expansion activities and population surveillance to further the agenda of the political elites who are in control of the surveillance tool.

In this environment, technological standards, commercial organizations, and public officials have come together to form an identification oligopoly regarding the means of identification – the Card Cartel (Bennett & Lyon, 2008). Given the corrupt practices within Russian public-private partnerships (Roi, 2014), including e-corruption in public ICT initiatives (Truntsevsky, 2019), one may expect that the Moscow Social Card Cartel may be involved in practices of clientelism, non-transparent bids and tenders, monetization of the data generated by the card, and privatization of the profits extracted from the collected data and used for new commercial purposes. The next subsection addresses these risks in more detail.

5.2.2: The Moscow Social Card Cartel: Privatizing Profits and Socializing Costs

The evolution of the Moscow Social Card project triggers the question of whether it was necessary to implement the identity card as a payment instrument involving Visa and MasterCard. It is not clear which social or welfare problems the payment card has addressed

successfully, as the Moscow Government has never produced evaluation reports outlining the social and economic outcomes of the project. The only available feedback is that the MSC cardholders were very satisfied with the cards, and that the government was able to maintain discounted transportation fares for a number of categories of population, and organize a network of over 3,300 retailers with discounted products (5% - 10%) and services for the cardholders (Moscow Government, 2014). In 2020, over 5 million MSC holders could obtain a discounted service in over 7,600 retail and service businesses around Moscow, including pharmacies, groceries, supermarkets, gas stations, dental clinics, insurance agencies, etc. (Moscow Government, 2020).

The latter achievement is an ordinary market-driven practice in many Western jurisdictions where grocery stores and supermarkets implement loyalty membership cards, as well as flyers and coupons with discounts to attract customers. However, what the MSC project has achieved is building businesses and generating profits for the private sector, as well as facilitating the development of e-commerce, banking, and the technology industries. Bennett and Lyon (2018) identify three components of the new identification system: (1) the corporation, particularly the banking industry and the practices of e-commerce; (2) technical standards, associated with the high-tech innovations of plastic card producers and IT industries; and (3) the nation-state (p. 12). However, the MSC case provides evidence of how the Cart Cartel is organized on the municipal level instead of the national level. Here, newly developed identification practices support and enable urban politics, as there are more services and points of interaction with the public, impacting their everyday lives and serving city governance goals.

As mentioned, the Moscow Social Card is managed in cooperation with the banking sector. The project has significantly increased the number of Bank of Moscow clients and

services (Global Mass Transit Report, 2011). The Bank of Moscow was a designated bank for the Moscow City Government and its public-private partnerships, meaning that municipal fees and payments were processed exclusively by this bank until 2016. The bank has been governing the project since its inception in 1998. In 2013, the Bank of Moscow was subject to a merger and became a part of the VTB Bank. Currently, the Moscow Social Card is issued by VTB Bank as a banking card (Moscow Government, 2022), supporting financial transactions and direct deposits of social financial benefits, pensions, and student scholarships. In addition, the card can be used to pay for municipal services and utilities through ATM machines, as a transit pass, to book medical appointments, and as a retail discount card.

For example, before the merger with VTB Bank, the Bank of Moscow delivered a corporate presentation summarizing the commercial interest of the financial organization in continuing to support the Moscow Social Card project, despite associated costs (Bank of Moscow, 2013). The presentation outlined that, even though the MSC project was associated with annual financial losses of 6.5 million rubles (approximately $217,000 USD) – as cardholders have limited financial capacities and no savings – the bank was still able to generate profit from the data generated by the MSC payment applications. This is the only bank with the exclusive right to administer pricing information and transactions for municipal and e-government services (an application that allows cardholders to pay for their municipal services, fees, and fines). Also, selling this information to other banks and organizations generates a profit of 50 million rubles (approximately $1.7 million USD) annually (Zaikin, 2013).

In terms of the technical standards, the UEC Card Cartel was heavily relying on microchip technology. The standards in smart cards are developed by the plastic card producers, traditionally developed by the telecommunication industry. Smart cards are directly connected to

the first prepaid phone cards and to similar technology used in credit cards. Over time, this technology has travelled to the governmental domain, enabling secure authentication of government clients (Rankl & Effing, 2010). It was assumed that the technology used by credit cards to facilitate e-commerce has been so extensively tested by the banking industry that now is the time to implement it for public administration purposes.

Initially, the Moscow Social Card was built on the experience of the Moscow metro electronic pass cards. A Moscow-based organization, Sitronics, that was already issuing public transportation passes, was selected to produce plastic cards that met the technological requirements for the MSC. Sitronics was established in 1997 as part of the ex-Soviet microelectronic manufacturer Mikron in Zelinograd (Frolov & Yu, 2006). Sitronics, just as any good post-Soviet privatized enterprise, was producing many things, including electronics, computers, mobile phones, sim cards, home appliances, and televisions. Over time, market competition narrowed the ambitious plans of the owners and eventually they concentrated on publicly financed projects. Two of these were related to the Moscow Government, particularly electronic plastic cards for the metro and the Moscow Social Card. However, in 2010, it turned out that the head of the Moscow metro and general designer of the Moscow Social Card, Dimitry Gayev, along with his son, Vladimir Gayev who was the head of the smart cards department at Sitronics, had developed profitable ventures that helped them monetize and privatize their involvement in public projects. The Russian media has extensively covered Gayev's family businesses and ownership, including private patents on the technology developed with public funding by an individual in a public service role (Agapov, 2011; Filipov, 2012).

These political and family connections between the top managers of private industry and Moscow public officials are among those that were targeted by the federal government, more

specifically by the Putin regime, in 2010. At one time, all the fraudulent activities of Gayev, Luzhkov, and Borodin, who respectively represented all three parts of the Moscow Card Cartel, were subjected to criminal prosecution (Krainova, 2011). As a result, all the old networks and individuals lost their influence. However, the corruption revelation did not become a reason for stopping the Moscow Social Card project. In contrast with the initial, family-scaled public-private partnership in the area of transportation management, where electronic cards were used mostly as a technological token to support transit fee payment, the latter development brought in a banking sector with the potential to manage and support electronic cards as a financial transaction instrument when Sobyanin became mayor in 2010.

In 2014, after a transition period, the Moscow Government announced a new smart card technology and interface for better and faster services. Alioth Ltd., a private Russian plastic cards manufacturer, was chosen through a city-organized competition to produce advanced cards supporting the Europlay, MasterCard, and Visa (EMV) standards in authenticating transactions, enhanced with the NFC (Near Field Communication) touchless technology as part of MasterCard's PayPass system (Moscow Government, 2014). Consequently, all Moscow Social Cards bore the MasterCard symbol and could be activated by tapping on the payment terminal. The competition was widely criticized by Sitronics, its parent company Sistema, and Rosan Finance, the previous producer of the Moscow Social Card supporting Visa standards that cooperated with the Bank of Moscow (Sergina, 2014). Manufacturers were criticizing the requirement of the card payment technology to support the wireless transfer of data through near-field communication, pointing out that only one Russian company could produce this type of card – Alioth – resulting in a lack of competition in the public procurement process. There was potentially a way for Alioth to advocate for the unique technology and maintain the payment

functionality of the Moscow Social Card. Igor Vasil′yev, the Head of Alioth, outlined a great future for the multifunctional NFC cards in 2012. In one of the industry journal interviews, he predicted that the company would be involved in main identity card projects in the country by the end of 2014, including smart cards for e-government (Vasil′yev, 2013). Interestingly, the goals and applications of the Moscow Social Card projects have remained the same as they were when framed by previous leaders.

There are perhaps several reasons why, despite the corruption scandals and technology shifts, the Moscow Social Card remains similar to the conceptual idea outlined by the Moscow City Government in 1998. It is still multifunctional and mostly has the role of a payment method. The project became an important part of the Moscow welfare system with significant public investment. Altering it too much would have defeated the initial purpose of the project, and moreover, it would be perceived as a waste of public funds. It has been made clear by the government and mass media that, in terms of addressing welfare problems, the smart card provides the best solution. Indeed, this is the very powerful role of the third component of the Card Cartel – political justification of the smart card technology. The Moscow Social Card provides political benefits for politicians. It allows them to showcase a technological token that facilitates urban life under the slogan of technological modernization. Moreover, many people evaluate their experience with the card positively, such as the generous Moscow welfare system, which differs significantly from the regional welfare programs.

The contradiction between the technological promise of the smart cards to modernize a welfare system, making it more effective and efficient, and the growing significance of private industry in shaping and delivering public policy, became a significant element of the Moscow Social Card. I argue that this contradiction predetermined the failure to modernize the post-

Soviet social benefits system, and at the same time, it secured the institutionalization of the powerful Card Cartel, driven by the endless business opportunities for the private sector to benefit from the new informational arrangements. Moreover, the MSC reinforces the practice of social sorting of Moscow's population based on their documented identity type and associated privileges. The Moscow Social Cardholders have access to better and more accessible services, not because of eligibility assessment – i.e. reported annual income or asset ownership – but because they belong to one of the positively framed social-demographic categories of retirees, students, or mothers of young children, and also because they live in one of the richest cities in Russia.

Overall, the analysis of the MSC demonstrates rather limited ability of the electronic identity cards to improve accountability of public spending and efficiency of public service delivery. The technology is ambiguous in its nature and does not necessarily facilitate institutional improvements; rather, it interplays with the institutional practices, legacies, and political culture. The technical implementation of the smart card system without altering the old institutional practices of the public administration will fail to transform the system. On the contrary, it will mutate under the influence of existing practices, resulting in arrangements that are way too expensive, ineffective and, moreover, will reinforce inequality and exclusion.

The Moscow Social Card experience demonstrates how electronic card cartels can accommodate a particular business (banking card) or technological (payment technologies) solution, and instead of facilitating good governance of social assistance, create an overly complex and expensive instrument to serve stakeholders' needs first whilst significantly limiting the options for citizens to manage their financial flows independently from government. The Moscow Social Card Cartel ensures that financial flows, both monetary and non-monetary, are

tracked, controlled, recorded, and that banking fees are applied in a centralized manner limiting any individual autonomy and/or ability to make an informed choice. The MSC Card Cartel reinstates problems of the social benefits system, and hides it behind the banking card "technological fix" without addressing the core problem of the Soviet in-kind benefits within the market economy.

5.2.3: The Moscow Social Card and the Soviet In-kind Benefit System

The Moscow Government's use of the MSC reinvents the Soviet practices of identifying, classifying, and sorting people into groups deserving certain benefits and conforming to certain behaviours. The first attempt to modernize insufficient and costly Soviet in-kind benefits, which survived the post-communist transformation, was the implementation of legislation transforming in-kind benefits into financial payments, commonly referred to as the monetization of benefits (Federal Law nr. 122-FZ). The reform was not successful due to growing inflation and lack of resources in the regional administrations. Between 2004 – 2005, Russian retirees and other categories of the population participated in massive protests against the reforms in Moscow, St. Petersburg, and across Russia (Henry, 2009). Thousands of people stood in Moscow's streets protesting the new regulations, blocking highways, and demanding strong and responsible government with a broad and inclusive system of social guarantees. The target of monetization reform was shifted to the periphery and, indeed, helped to reduce the amount of unaccounted-for welfare expenditures within the federal and regional budgets (Henry, 2009). Institutionally, people were used to the practice of social benefits related to their status, and it turned out to be a good political instrument to control their level of political loyalty and social stability, through the emphasis on their special status within the complex hierarchies in Moscow.

The segregation mechanism works on several levels. First, only people with a permanent residency stamp in their passport, proving their residential address is in Moscow, are qualified for the Moscow Social Card. Moscow still institutionally differentiates between people who live there permanently and own a property, and those who come to Moscow to work or study. This disqualifies a significant amount of the population for social services, including health care and education. Additionally, the Moscow social categories of *l'gotniki* or MSC cardholders enjoy a higher level of benefits compared to the regions. For example, if one person's municipal services cost more than 10% of their monthly income, this person is qualified for a discount in Moscow, while in other regions the cost would have to exceed 22% (Aburamoto, 2010). The second level of social sorting is concerned with the identification of the different groups in need of social assistance: retirees, young mothers, students, people with disabilities, and people with the right to discounted municipal services. Each of these groups has a different smart card, marked by different colours, providing access to different qualified services, and different application processes (Moscow Government, 2015). Noticeably, groups are framed positively, however nobody is reviewing whether those people really require assistance; rather, the assistance is deserved due to their socio-demographic characteristics.

Finally, there are also types of bureaucratically negotiated identities that require regular procedural examination to prove one's status (e.g. people with disabilities or financial issues). This is the third level of sorting with a high level of discretionary power given to the bureaucrats who will in each case decide whether one deserves a card. For example, there is a type of Moscow Social Card that qualifies some residents to pay less for their municipal services, such as condo fees, electricity, and so on. Some of these categories are straightforward but some may be open to bureaucratic interpretation. Another illustration of these negotiated identities is

issuance of the Moscow Social Card to police officers and employees of the Ministry of Internal Affairs (MVD), who would qualify to ride public transportation for free (Moscow Government, 2017). They could also possibly use the card for other applications as well; however, this is not discussed in the publicly available documents.

The MSC facilitates the expansion of the categories that require social assistance from the government beyond traditionally understood welfare needs. This practice bears a resemblance to population sorting as "elements near and far" within the Tsarist and Soviet passport systems. People belonging to the social categories that qualify for the Moscow Social Card are more satisfied with the system and/or can be encouraged to demonstrate loyalty, including through voting. The MSC is a privilege, available only to the categories of the population eligible for social assistance or financial benefits, and not available to the temporary residents of Moscow or people without permanent registration in the capital (Moscow Government, 2020). It is also not available to people who do not qualify for social assistance but nevertheless contribute to the local economy, pay taxes, and qualify for social services constitutionally. MSC holders have priority in enrollment in educational and daycare services, in case of the megapolis with the high proportion of population from all over Russia these services became scarce (Moscow Government, 2020). During the pandemic, the MSCs of non-vaccinated individuals and individuals not complying with the public orders to stay at home were automatically blocked (Interfax, 2021). Card holders could not use the card for public transportation or to access other services.

Finally, there is also the problem of social sorting among cardholders, differentiating between appropriate and inappropriate behaviours and suggesting punishments. This sorting is based on performance indicators. The cultural understanding of human rights in the Russian

Federation suggests that personal obligations should be settled before one can enjoy human rights. For example, the movements of a person who fails to pay their financial obligations to the state will be restricted. The MSC is designed in a way that the financial obligations of cardholders are regulated automatically every time they receive financial assistance from the state. For example, pensioners receive their pensions, and a certain part of it is directly deducted to pay for municipal services, to ensure that people will first pay their obligations to the state in exchange for the right of financial assistance. Another example is those who are allowed to use the MSC to pay for certain retail products, are only able to purchase healthy foods deemed to be appropriate to their identities and associated needs (Ishkov, 2013). The card is also designed to make sure that a cardholder will have money to pay; it is a Visa or MasterCard with an overdraft option (at a 24% annual interest rate). Some people complain that they cannot understand banking fees and overdraft regulations and endure financial losses due to their minimal financial support from the governmental. Normally, people on social assistance would not qualify for a credit card. However, government administers financial payments using MSC, that has hidden banking fees and charges that may result in increased financial debt. These complaints are addressed in the booklet for retirees published by the Russian Taxpayers Party (The retiree guide, 2014). This profit-generating mechanism is not discussed much anywhere, except in social media forums, where people seek advice on how to delink their cards from VTB banking services but maintain social services (banki.ru, 2019).

As a result, the card is not effective in addressing poverty and social disadvantages; moreover, it reinforces the social position of the positively viewed categories while ignoring poverty and socially disadvantaged groups. It not only reinvents the old Soviet categories of the population but also uses them in political propaganda and as a target of invisible control.

Knowing that the government can have access to any of the information generated on the card, cardholders are more likely to adjust their behaviour to meet the standards of the category to which they belong. Henry (2009) refers to Russians as those who value social citizenship more than political citizenship; therefore, good government should preserve in-kind benefits as a reward for appropriate citizenship. So far, the system has generated more costs than efficiency and effectiveness. While several social groups, based on their social-demographic identity, enjoy free or discounted services, there is a significant majority who are paying double, without the possibility of having any political influence on this income distribution scheme.

However, through the institutionalized MSC Card Cartel, which reinforces the power positions of Moscow's political leadership, the bank of Moscow and VTB bank were able to capitalize on the idea of the electronic identity card and technological progress it brings as an instrument of electronic modernization of the Russian state at the federal level. This idea was referred to in policy documents and programs dedicated to e-government reforms and modernization of the Russian state.

5.3: Implementation of the Russian Universal Electronic Card

The idea of the multifunctional national electronic identity card was first emerged in the governmental program "Electronic Russia 2002 – 2010" (Federal Target Program, 2002) The program mentioned the successful experience of the welfare benefit electronic cards in several Russian municipalities and regions, where smart electronic cards facilitate access to social services for particular social groups (Gayev, 2011). Optimistically, the program claimed that, by 2010, the Universal Electronic Card would "serve as a secure state-issued identification document linked to the electronic Russian Population Registry and enhanced with a biometric

function, including physiological features of the cardholder to facilitate access to medical services; social assistance, cashless payment function; and public transit pass" (Government Program Electronic Russia, 2002-2010). These card functions corresponded to the experience of the Moscow Social Card, where municipal regulations and programs were outlining the possibilities of transforming the Moscow experience to the national level. Moscow Mayor Sobyanin was the Head of the Governmental Commission, responsible for the coordination of public and private bodies which collaboratively deliver solutions for the national electronic identity card. Pragmatically, only after 8 years of policy discussions, consultations, and cross-departmental negotiations, the Universal Electronic Card was officially acknowledged within the special law regarding the provision of governmental and municipal services, but only as an online authentication technology, not as a national electronic identity document (Aleshkina, 2014).

5.3.1: Legislation, the UEC Design, and Functionality

In 2010, the strategic goals of the technological modernization of government institutions were specified in the new national program of the Russian Federation "Information Society 2011–2020," (Government of the Russian Federation, 2010 Nr. 1815-p), where the development of e-government has become part of the subprogram "Information State". Among the expected results of this subprogram are "(1) technological independence of the Russian Federation in the information technology industry, outstripping the growth of the Russian information technology market at the global level; (2) development of mechanisms for providing citizens and organizations with state and municipal services and information sharing using remote

telecommunication technologies; (3) increasing the openness, efficiency, and function of the electronic interactions between state authorities and local authorities, individuals, and legal entities, including at the cross-border level; (4) improving the ease of use by citizens, organizations, public authorities, and local governments of state (municipal) information systems and services, mechanisms of interagency electronic interaction, as well as the establishment and development of uniform quality standards, and bringing these federal agencies into interdepartmental electronic interaction in accordance with these standards, at the regional and municipal levels" (Government Program Information Society, 2011-2020).

Since 2011, the provision of electronic services became the most important goal of the reform for the state, municipal bodies, and institutions, and this goal was reflected in the new legislation. Russian Federal Law 210-FZ (2010) became the most important regulation prescribing the use of the Russian Electronic Identity Card. Before 2016, the law was regulating the organization of the UEC issuance process (s. 22-28). Since 2016, this law became less prescriptive in terms of the secure identification tools and instead implemented a more general language regarding the provision of public services in electronic form. This included the creation of the unified portal of public services (www.gosuslugi.ru), the formation of the infrastructure that provides the information technology used to provide government and municipal services, and managing the government information registries (s. 21).

The federal Law on the Organization and Provision of State and Municipal Services (210-FZ, 2010) defines the Universal Electronic Card as "a material carrier of the visual and electronic personal information about the cardholder, who can be a Russian citizen, a foreign resident, or a person without citizenship, and enables authorized access to the governmental and municipal services" (s. 22). The design of the card was approved at the government level and

included the following data and technological elements. As shown on Figure 3, the card includes multiple government-issued personal identifiers (social security number (SNILS) and state health insurance number (OMS), and bank account number linked to government services, all presented visually next to the person's photo, name and date of birth, and signature. The loss or displacement of the card would result in a significant data breach, leaking crucial data that can be used by malicious actors for identity theft and fraud. Based on the analysis of the data elements included in the Universal Electronic Card, the designers seemed to approach the principles of "universality" and "convenience" holistically.

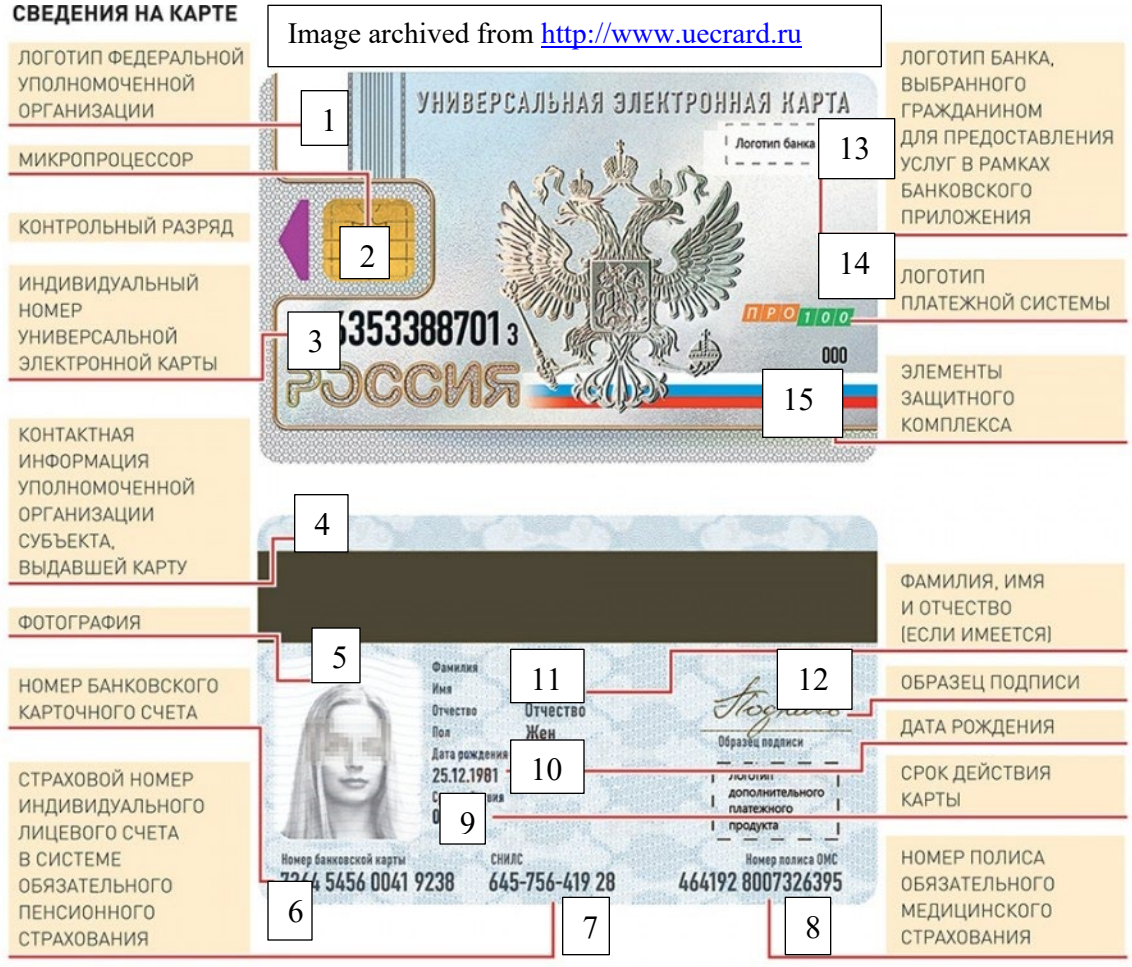


Figure 4 Russian Universal Electronic Card design

1. Logo of the issuing company (depending on the region)
2. Microchip
3. UEC Card number
4. Contact information of the issuing company
5. Cardholder photo
6. Bank account number
7. SNILS – unique individual pension insurance account number
8. Individual compulsory health insurance number (OMS)
9. UEC Expiry date
10. Date of birth
11. Last, first and patronymic name, gender
12. Signature
13. CSC/CVV – card security code
14. PRO100 – National payment system compatibility
15. Bank logo (depending on the region)

The government seemed not to prioritize addressing privacy and security risks, instead preferring to "put all your eggs in one basket" and adding eight unique individual identifiers into one document. The internationally established practice of managing identifiers issued by different government agencies is to keep them technically separate, which is not as convenient, but is a better way to control access to personal information based on the "need to know" principle (Stamp, 2011; Sloan & Warner, 2017). Additionally, the Western paradigm of privacy emphasizes individual control (Solove, 2012), where individuals have control over their own personal information, and able to make an informed decision how to share their personal information and with whom. Consequently, individual control supports the principle that the individual is always the source of information about themselves, not the third party that may have accurate and verified information about that individual. Therefore, governments must always collect information directly from the individual, if at all possible. These are foundational principles of privacy legislation in Western democracies (Bennett & Raab, 2017). Alternatively, the Russian state identification practices lead to the conclusion that individuals cannot be trusted unless they are in possession of a verified document provided by the authoritative third party.

The more verified information that document contains, the more legitimate the identity of the document holder. Therefore, the Russian internal passport is issued not only by the central government but also by state representatives at the local police passport office, which is responsible for administering permanent or temporary residence stamps in that passport, in cooperation with the landlord and property management authorities. The Universal Electronic Card contains an exhaustive list of verified identifiers produced by different government offices, reflecting the legacies of Russian state surveillance.

The government assured UEC applicants that only minimal information is included in the card, as required by the legislation, and only authorized individuals can access the card for the provision of state and municipal services by federal executive bodies, executive bodies of constituent entities of the Russian Federation, local authorities, and other types of service providers (Federal Law, 210-FZ, 2010). However, including such a combination of multiple identifiers on one card, visible to anyone who can get a hold of it, creates serious security risks, potentially leading to identity theft if the card is lost.

Another universality principle was applied to payment functionality. The smart features of the card included a microchip and magnetic stripe containing banking software applications, linking the card to the personal account in participating financial institutions. The digital signature option could be added to the microchip but would require a card reader and software to be purchased separately and downloaded to the home computer, to support the online exchange of the secure digital certificate (Krupin, 2013). At the time the card was distributed (2013-2016), cardholders could link their UEC cards to banking accounts in SberBank of Russia, Uralsib Bank, AK BARS Bank, Moscow Industrial Bank, and other financial institutions (para. 8). A distinctive feature of the UEC is the use of the domestic payment system PRO100 (pronounced

as “prosto” [in English - simply]). PRO100 operates only in the Russian Federation and was designed to address the earlier comments of the government cybersecurity specialists regarding VISA payment functionality, and the American microchip required for its support, which was part of the Moscow Social Card and was transferred to the UEC by default, due to the lack of a similar product within the domestic market. PRO100, the Russian domestic payment system, was developed by SberBank in 2012, specifically to support the UEC project, to ensure that data about financial transactions related to government services remains under the jurisdiction of Russian law. This requirement to ensure that data processed by technology must remain under the relevant state’s jurisdiction became internationally recognized under the term of data sovereignty, referring to the information being subject to the laws of the country where the information is located (Hippelainen et al., 2017, p. 645). This security requirement allowed SberBank to become the only provider and operator of the domestic payment system present in all regions of the Russian Federation, and serving 15 Russian banks.

In 2014, PRO100 was quickly considered by the Russian Government as a candidate for a national payment system. This was in response to US political sanctions, which temporarily disabled Visa and MasterCard functionality during the military occupation of Ukraine. As a result, many Russians could not use their bank cards. However, it was established that PRO100 was technologically built on the MasterCard M/Chip4 standard, in order to make the UEC compatible with international payment systems like Visa and MasterCard. Therefore full isolation, for example in the case of sanctions, would not be possible (Cnews, 2014). Instead, when most of the financial sanctions were lifted in 2015, the Russian government required any international payment system operating in Russia to integrate first through the National System of Payment Cards, which was also a Russian operator of the National Payment System “*Mir*”

(peace), a subsidiary of the Central Bank of Russia (Mironline, 2020). While this solution helped to limit the effects of the new sanctions of 2022, following further military aggression against Ukraine, it is unlikely to be successful long-term, as it is estimated that Russian banks' demand for microchips in payment cards is six time higher than the production capacity of Russian manufacturers (Kommersant, 2022).

A card microchip was not only supporting a unique payment function, but was fully embracing the "universality" principle of the UEC, and supporting the rich functionality of the connected services. Similarly to the Moscow Social Card, the UEC could support any function and applications integrated by the municipal or regional government and private organizations, depending on the availability of resources and technological support. During the policy announcement, Medvedev (2011) called for the Universal electronic card to be "a truly multi-functional instrument supporting domestic and international financial transactions and allowing Russian citizens to verify their identity online, receive government services, to use the electronic card as a driving license, to access medical services, and possibly, in the future, to vote in Russian elections online. The electronic card would really encourage young people to vote because they are more technology inclined."

In practice, however, the available functionality of the card would be dependent on the availability of digital services and connections accessible in the region. E-banking was supposed to be available by default, and SberBank would reprogram their banking machines in the regions to facilitate the processing of payments from and to the local government and cardholders. According to the official Universal Electronic Card website (www.uecard.ru, 2014), the card's functionality supported the use of the Universal electronic card to pay for housing and municipal utility services (garbage, water, electricity, natural gas, centralized heating, etc.); local

transportation (transit pass, including verification of discounts for students and retirees); medical services (registering online for doctor's appointments, ordering tests and accessing electronic copies of the test results, electronic medical history, electronic prescriptions and payments for drugs in pharmacies); fees associated with driving (payment of fines, insurance, state fees for driver's license, vehicle registration); and financial social assistance, which could be deposited to this card and used in approved stores for purchasing food. It was expected that the list of services would keep expanding and eventually include a digital signature and become a substitute for the national passport and driver's license (Medvedev, 2011).

The UEC was not defined by the legislation as a primary identity document that could substitute the existing internal passport. Instead, it was an additional eID that would function alongside the Russian Federation internal passport. The passport was still the document that met the highest identity assurance even though it was a paper document, but it included a witnessed ink signature from a procedurally verified citizen. It was a more secure document providing a higher level of confidence in establishing the identity of the applicant, as it relied on in-person identity verification. Notably, in cases where federal laws do not specifically require a national passport as proof of identification, the Universal Electronic Card could be used instead.

Despite the practical limitations of transferring smart ID technology from the Moscow municipality to the federal level, the Universal Electronic Card quickly became a national policy goal and was endorsed as a secure and convenient tool to access government services and process government payments and financial benefits. However, the card was not technically deployed by the central government; it was rather endorsed by the President and mentioned within the legislation as an obligatory instrument for electronic access to social services and benefits (Federal Law, 210-FZ, 2010). Practically, it was developed and supported by the private

banking sector, specifically by Russian SberBank and its subsidiary, a joint-stock company called “Universal Electronic Card” (UEC JSC). This is an example of a public-private partnership, where both parties would benefit: the public sector would improve citizen services online and optimize government spending, while the banking industry would obtain new clients and manage new types of transactions online.

5.3.2: The UEC Card Cartel: A Public-Private Partnership of SberBank and UEC JSC

My analysis of the reports submitted to the shareholders of the joint-stock company “Universal Electronic Card” (UEC JSC) in 2011 and 2012 supports the argument that the business managers expected significant financial return from the UEC project. In 2010, the Russian State Duma, one of the chambers of the Russian parliament, Federal Assembly, enacted Federal Law 210-FZ “Organization of Public Service Provision” to regulate the Russian Universal Electronic Card. In support of it, the Government of Russia issued the Federal Government Order 1344-p (2010) to establish a joint-stock company called “Universal Electronic Card” (UEC JSC), with a mandate of developing the technical infrastructure and managing the distribution of the electronic identity cards to eligible recipients. Subsequently, in January 2013, the first electronic identity cards were issued in five pilot regions of the Russian Federation.

According to Federal Law 210-FZ, the UEC was to reform governmental service provision and modernize intra-governmental information sharing practices using secure internet connections. At the same time, UEC JSC began a marketing campaign advertising the UEC’s secure and protected authentication process, and authorization of the cardholders in multiple spheres. Their emphasis was on the transactional functions of the card and the universality of its

usage, ranging from a bus pass to a debit card for certain governmental and municipal fees and payments, as well as for payment in certain government stores and pharmacies for people in need of social assistance (UEC JSC Annual Report, 2013). However in 2013, Dmitry Medvedev, the Russian prime minister, announced that the Universal Electronic Card would be an important step to a more relevant project – the Russian national e-passport that would be issued by the Federal Migration Service, promising that all the services and infrastructure would remain under the mandate of UEC JSC.

Shareholders of UEC JSC expected some state support, as the total project cost was estimated to be 170 billion rubles ($2.3 billion USD) (Krasnikov, 2013). Nevertheless, the UEC did not obtain any funding from the federal budget. The government decided that banks would be responsible for financing the operational costs of the project, including issuing and delivering cards. The government also concluded that it was not necessary to build an infrastructure, as the technological base existed built by Rostelekom within the framework of the Federal "Information Society" Policy Program. Due to the lack of dedicated federal resources and the unpreparedness of the regional governments, the participating banking institutions or shareholders of UEC JSC were expected to step up and cover initial costs by issuing and supporting new electronic cards to their clients. This scheme was presented as a long-term investment based on future returns. Potentially, when more Russian citizens across the country used the UEC regularly to access a growing number of government services online, as more and more regional and federal services would be linked to the UEC, the overall costs could be recovered through introduction of a small fee for each transaction supporting authentication. Public administrators would be able to significantly reduce the cost of paper-based citizen verification and eligibility for a particular service with one UEC transaction (UEC JSC, 2011). A

small transaction fee would be part of the administrative cost to local government, and would be paid back to the UEC JSC under a special service agreement (UEC JSC Annual Report, 2013).

Eventually, when new systems of information exchange would be developed between federal and regional systems, the federal government would be covering the transaction fees for federally funded services directly. The technological ability of the electronic identity card to record every transaction and keep those electronic trails transparent and protected from manipulation was a promising step towards eradication of corruption and limiting misuse of public funds by regional bureaucracies. Additionally, UEC JSC was marketing the idea of a secondary use of the information generated from the electronic trails and reflecting common and unique trends and patterns of the card user's behaviour, including their social-demographic characteristics. This information in a de-identified form could be sold on the market to private organizations and businesses, securing an additional source of revenue for the participating banks (UEC JSC, 2011).

Initially, it was assumed that the card would be received by all citizens except for those who had signed an official declaration refusing to accept the UEC. The start date for issuing cards was postponed several times, and in a response to religious criticism, obtaining a card became a legislated voluntary choice. Without secured federal funding, or at least the legislation guaranteeing it, some regions were not ready to implement informational systems that could process UECs and facilitate onboarding of the cards to the various programs and departments who provide services to citizens. Banks, for their part, were very slowly onboarding this project, despite the promise of future financial returns. According to the latest publicly available report from the UEC JSC, 20 banks joined the company (Annual report JSC UEC, 2013).

Under the federal law on provision of public services (210-FZ, 2010), an electronic card must be distributed free of charge to citizens, with the issuing banks covering the production and distribution costs. A SberBank representative mentioned in an interview with an industry magazine that on average, the cost of a transaction by Visa or MasterCard is $ 1 USD, and the cost of the UEC transaction is 300 rubles ($4 USD) (Aleshkina, 2014). According to the CEO of SberBank, Herman Gref, the multi-factor authentication function developed by SberBank could be implemented in the national electronic passport, which would be fully managed by the Federal Migration Service (FMS), but FMS was not interested in supporting integration of the payment instrument within a national identity document (RBC, 2014). This solution would most likely require technical interoperability between the information systems of private sector organizations (banks) and government agencies with a rather secretive mandate. This may explain the hesitancy of the FMS. Without FMS support, the card would not be recognized as an accepted identity document that meets the highest federal identity standards. Meaning that the UEC, by itself, would unlikely provide the highest degree of confidence that a person's claimed identity is their real identity. This hesitancy undermined distribution of the electronic cards across the Russian regions. Between 2013 and 2015, only 700,000 applications for the UEC were processed and only 600,000 cards were issued in a population of 144 million of Russians. At the same time, Visa and MasterCard issued at least 10 million cards across Russia (Dementyeva & Shestopal, 2015).

The banking infrastructure and financial investments from UEC JSC stakeholders, including SberBank and the regional levels of government, were critical drivers for the UEC project. The stakeholders' relationships were documented in agreements with UEC JSC and secured with the federal government's promise to link well-developed UEC applications to the

future national passport system. More than 40 agreements were signed with the administrations of the constituent entities of the Russian Federation, for the purpose of introducing the UEC in 40 regions. Implementation of the project involved creating the necessary e-government infrastructure (for the distribution of public services). In some regions the project created e-government infrastructure that could be easily updated to satisfy the interoperability requirements of the federal information system. That was developed simultaneously, to ensure that the UEC can be used by citizens of all regions to access federal services via www.gosuslugi.ru. Such synergy between e-government service providers and the UEC (based on a unique and verified key to access) was framed as a unique offer for citizens developed through public-private partnerships, and without any up-front spending from the federal budget (UEC JSC, 2013).

By 2016, the number of issued Russian Electronic Identity cards had reached 650,000 across different regions, mostly within larger municipal centers. Up until the end of 2018, the UEC was used to facilitate access and payment for municipal services, such as payments for utility bills, access to certain public services online, and public transportation passes (Yeremina & Tret'yak, 2018). All the work and investments by UEC JSC between 2010 and 2016 did not result in considerable achievements. The card was not in demand, partially because it could only be used as a payment card, and many of the applications that were originally planned to be implemented were still in development in many regions. The card has not become a universal electronic identifier recognized across organizations and different levels of government. One regional public official from Kaliningrad Oblast commented: "a lot of hopes were laid, a lot was hung on this card: a photograph, and SNILS, and a digital signature, but none of this was done" (Durov in Vedomosti, 2017).

In December 2016, the State Duma adopted a draft amendment (471-FZ) that abolished the universal electronic card as "a tool for providing state and municipal services to the population," starting January 1, 2017. Legislators quietly excluded the UEC chapter from the law on the provision of services (210-FZ) without any legislative deliberations or discussions. SberBank's CEO commented that UEC JSC would continue providing services in the regions through development of UEC solutions that support public transportation passes, payments for municipal services, and school lunches (Vedomosti, 2017). As for a national electronic identity card, there was a plan regarding development of the federal e-passport starting in 2021; however the implementation target dates were changed multiple times with a projected new start date for the issuance of the first documents in summer of 2023 (MVD, 2021).

In 2017, with the cancellation of the UEC project and re-centralization of the previously independent Federal Migration Service under MVD oversight by Putin's Presidential Decree, the Ministry of Internal Affairs finally obtained its own project – the e-passport. History came full circle and technological innovations of the state identification system went under the full control of the MVD. This outcome signifies a dramatic departure from the business model of the UEC Card Cartel, and reinforces the idea of the state monopoly on means of identification as a critical element of the Russian identification system.

5.4: Chapter Conclusion

The Universal Electronic Card should be viewed within the context of the post-communist reforms, which aimed to introduce Western market principles and technocratic optimization to public administration, while preserving the traditional and cultural significance of a socially-oriented state. This context of Western modernization through technological

reforms mobilized political forces and local political elites to undergo initiatives that reformed traditional systems of social guarantees based on residential status, by means of electronic identity cards with payment functionality, enabling cashless transactions.

The policy structure and strategy of UEC implementation reflected the Medvedev government's attempt to advance the role and influence of economic liberals and technocrats within the Russian state, providing multiple opportunities for new types of public-private partnerships as part of technological modernization. In other words, the vision of the card itself and state-provided opportunities within this policy was a driver for multiple actors, including corporate private bodies, to be involved in new political and economic activities and contribute to the development of the "Card Cartel" (Bennett & Lyon, 2008), or an "oligopoly of the means of identification" (Torpey, 2000) as a state-initiated project, facilitating the growth of the Russian digital economy.

The Russian government approached the development of the Universal Electronic Card similarly to the Moscow Social Card, in terms of its city-based application concerned with the rationing of public services only to the documented residents of the Russian capital. Innovation evolved in the Russian European center – Moscow – followed by attempts to multiply the solution in different regions as a method of supporting municipal governance and ensuring accountability of public spending on social programs. It was an attempt to better control financial resources flowing from the center to the regions. The card was not dictated by local needs, and local administrations were rather instructed to sign the agreements with the UEC JSC.

The Russian Universal Electronic Card does not follow a linear process of technocratic policy implementation. Even a top-down model of Presidential decrees and financial support by the most prominent Russian banking institution, SberBank, was not enough to use a developed

solution – the Moscow Social Card – to modernize and digitize the Russian state identification system. Instead, from the very beginning the seemingly apolitical promise of its instrumental rationality was questioned by State security officials who initially refused to certify a technology using an American microchip, even for temporary usage at the federal level (Lukatsky, 2010). The promise to modernize Russia, using an imported technological innovation, quickly became a problem for political solutions, encouraging alternative interpretations of the proposed technology and facilitating temporary exemption to the existing security standards (Lukatsky, 2011).

Chapter 6 addresses these tensions in more detail through identification of the four interpretive policy communities with different views on electronic identity cards, shaped by their institutional and organizational agendas and beliefs. I document ideas expressed through official statements and comments by the key policy players within those identified communities. I explain how those ideas can be classified along the lines of the two models. The first model, the Oligopoly of the Means of Identification, relies on market solutions to government problems through public-private partnerships with the banking and IT sectors. The second model, State Monopoly on the Means of Identification, is concerned with the enforcement of government control over electronic identity card technology, from design to production and implementation. The tension between these two models captures the politics of technological modernization of the Russian state: the Russian government can either be part of the globalized world or be a "truly" sovereign state based on imperialism and far-right populism (Paris, 2022), but it struggles to reconcile both.

Chapter 6: Playing the Meaning of the Russian Electronic Identity Card: Interpretive Policy Communities and Competing Ideas

6.1: Introduction

Chapter 5 outlined problems with the implementation of the Russian Universal Electronic Card. While government programs and legislation defined the criteria and organizational framework guiding this innovation, the "lift and shift" of the Moscow Social Card experience was challenged by the socio-economic and institutional circumstances of federal and regional politics. Traditional analysis of institutions and institutional legal framework would not be very helpful for the analysis of UEC outcomes, simply because the plan did not follow the traditional bureaucratic process of policymaking. Instead, it was a policy idea full of assumptions about applicability of the MSC model to contexts outside of Moscow governance, the progressive nature of eID technology, and the ability of the banking sector to create a cost-recovery model supporting government identification systems.

The problem is that the UEC was supposed to be implemented as a federal top-down direction and was framed as a rational solution developed by Medvedev's team of modernizing technocrats. In practice, this idea quickly became subject to numerous interpretations by regional and federal administrations required to catalog their services and to utilize the UEC for provision of services online, while limited in their technological and organizational capacities to do so. In other words: "the idea is ours, but resources are yours." Inevitably, the complexity of these processes and the involvement of actors from different organizational and institutional settings resulted in multiple interpretations of the meaning of the eID innovation, and formulation of the whole new variety of ideas reflecting different contexts and which challenged the original goals of technological innovation. This work employs interpretive policy analysis and focuses on the

networks of policy communities, their key stakeholders, their interpretation of the eID technology, and knowledge creation. It is crucial to understand the meaning that people attach to the UEC, which in turn would determine how the UEC would function in practice.

In this chapter, through closer analysis of the development of the Universal Electronic Card idea and how it is portrayed publicly by government officials through statements and policy documents. I reveal complex relationships between ministries, departments, and policy actors engaged in policymaking, political critique, and even policy sabotage. I have identified four distinct groups of actors within four institutional settings, engaged in the framing of different interpretations of the UEC. This engagement cannot be captured through formalized political competition or standard policy development, as it was not subject to parliamentary debates in the State Duma, nor was it debated as a budget item. The innovation was announced and justified by Dmitry Medvedev, the President from 2008-2012, who assigned the delivery of this project to the Ministry of Economic Development and the Ministry of Digital Development, Communications and Mass Media. The project would be delivered through a non-negotiable public-private partnership. I explain how, in reaction to the proposed innovation, key stakeholders in the Ministry of Internal Affairs and certain representatives of the opposition parties and the Russian Orthodox Church engaged in policy sabotage, trying to undermine the innovation through criticism and resistance. I argue that the idea of the UEC became politically contested as the direction of this innovation was negotiated between different political factions, acting as interpretive policy communities. Through analysis of the interpretations, I identify powerful but false dichotomies employed by the key stakeholders in support of their view of the UEC innovation. These dichotomies are based on competing myths and beliefs and are used to simplify the message and justify a particular model of the eID, whether through a business model

of the UEC Card Cartel, or a conservative modernization embracing the institutionalized passport legacies.

6.2: Interpretive Policy Communities and Their Views on Technological Innovation

The Russian Federation has always been a challenging subject to explore using Western political science concepts. The discussions have often focused on the problematic electoral system (Golosov, 2017; Goode, 2010), weak civil society (Sundstrom & Henry, 2016; Chebankova, 2013), ineffective and corrupted public institutions, and authoritarian political leadership (Engelstein, 2009; Laruelle, 2016). The observed inconsistencies with the democratic ideals are often approached through a concept of democratic transition, including attempts to predict whether that transition is going to be towards democracy or authoritarianism (Umland, 2012; Kolsto, 2016; Ambrosio, 2016; Ahram & Goode, 2016).

Policy decisions in Russia are not achieved through democratic deliberation in the State Duma or transparent government policymaking, nor do they necessarily result from authoritarian Presidential decisions (Sakwa, 2010). How can one explain the failure of the Russian Universal Electronic identity card even though the President, State Duma, two ministries, and the most significant private bank were officially supporting the project, even though there were mandates, a legislative framework, and publicly announced dates of implementation? Conversely, how was the military occupation of Crimea possible in the absence of broad political consensus, support from the economic sector, policy planning, and programs? Surprisingly, only two months after the start of the occupation, most of the Crimean population were documented as citizens of the Russian Federation, some forcefully, by mobilized Russian passport authorities (Kommersant, 2015). The perspective on factional politics and political struggles connects these two events

involving state identification practices as certain appropriate solutions serving the interests of distinctive groups within the state. I reveal a messy policy reality that cannot be explained through instrumental rationality or even bounded rationality, but requires the exploration of a whole range of perceptions such as widespread fears, myths, and conspiracies reflected in policy justifications and interpretations made by key policy stakeholders.

Using the literature that defines the distinct and homogenous groups of political influence within the Russian state (Staun, 2007; Sakwa, 2010), and through extended observation of policy justifications and conversations surrounding the UEC project, I identified and labelled four groups. First, economic liberals, who adopt instrumental rationality and propose the UEC as an apolitical tool of Russian modernization with a unique revenue model, that would inevitably make the Russian Federation a leader in global e-government and result in a new political elite in a newly established digital economy. Second, technocrats from the Minkomsvyaz (Ministry of Digital Development, Communications and Mass Media) who adopted incremental steps and develop practical technical solutions to address one problem at a time and to ensure connectivity and system interoperability within the government and across the federation, while preserving control over internet providers and facilitating law-enforcement access to the telecommunication companies' servers. Third, *siloviki,* represented in crucial ministries overseeing natural resources, the military, the police, and international relations, are limited in this analysis to those associated with the Ministry of Internal Affairs, which inherited Soviet passport practices and manages internal population movements for the purpose of national security. Fourth, conservatives and traditionalists*,* involving members of the Russian Orthodox Church, members of the Izborsky Club, the Russian Communist party, and the Russian Liberal-Democratic Party. Representatives

of these organizations opposed the UEC using global conspiracy theories and anti-Western sentiments.

I approach these four groups as policy communities and analyze their behaviour through interpretive policy analysis. Policy communities are stable networks of policy actors from both inside and outside of government (Stone et al., 2001), formed based on the shared values of the desired policy outcome (Rhodes, 1997). Interactions between policy communities correspond to the ever-changing social reality of policymaking much more than the institutional approach. These policy communities think and act within a particular narrative created around an important policy idea and supporting beliefs, in order to create new knowledge and make sense of their policy engagements. I will unpack and interpret how these communities made sense of the electronic identity card innovation, and how their choices and actions created new knowledge about possibilities of such innovation.

6.3.1: Economic Liberals and the "All-in-One" Universal Electronic Card

"UEC is a capital-intensive project, and its financial model should attract private funding and investments. The private sector, particularly the banking industry, will support technological infrastructure and the distribution of smart ID cards. Government compensation will be available as a tariff-based model, depending on the quantity of transactions processed with the card."

Elvira Nabiullina
Minister of Economic Development of Russia
February 2011

Politically, the faction of economic liberals was formed at the end of the first presidential term of Vladimir Putin (2008) as a result of growing international trade and access to global financial markets, but also in response to Putin's nationalization of the oil and gas industry, particularly the Yukos oil company. The UEC was a political decision by the economic liberals

in power that promised measurable change while preserving the political status quo during Medvedev's Presidency (2008 - 2012). As a G8 country, Russia wanted to show the world its potential to become a global leader in ICT reforms and e-government.

The significance of the Russian Universal Electronic Card is revealed through policy discussions and the engagement of many actors. It was never discussed as a specific technological solution for one institution, like the electronically enhanced passport was. Instead, it was presented as an umbrella solution covering a "wide spectrum of policy opportunities within multiple institutional settings that are crucial for Russian technological development" (Gref, 2011). It was not a tool to fix the policy problems with state identification practices. It was a policy invitation addressed to the new technology industries and financial elites to work on applications of smart card technology. An invitation to cooperate, open for public and private institutions, including international actors was pronounced by the Russian president who engaged with the UEC as his political promise (Medvedev, 2011). The promise was to establish new types of mutually beneficial public-private networks based on information and communication technologies.

The business model idea was proposed by Russian President Dmitry Medvedev, who announced the government plan to implement a national electronic identity card during the meeting of the Commission for "Modernization and Technological Development of Russia" in February 2011. President, Dmitry Medvedev, liked to be referred to as a technology and internet "geek." He became one of the first Russian politicians to actively use social media and his smartphone to communicate his political stance. On many occasions, he felt confident enough to speak about technological opportunities for the smart identity card, and the project itself was

soon associated with him and his political allies. Notably, mass media began to frame the UEC as Medvedev's project (Krupin, 2013).

In 2011, Medvedev's speech focused on three elements of the national eID: the smart card itself, the software applications available through the card, and the readiness of the government to implement new systems of cross-governmental information linking to streamline government services. Medvedev proposed a new regulatory framework to enable public-private partnerships (PPP) to support the provision of public services utilizing information and communication technology, and to coordinate compliance of the technological token of the card, software, and card applications under federal regulation. In support of the PPP, Medvedev stated: "I have doubts about the ability of the state to create such a unified system that will digest all this. So far, based on the information provided by both the government and Sberbank, I think SberBank's position is more motivated. When government departments begin an innovation, internal contradictions arise that need to be resolved. It seems to me that the degree of readiness of banks to implement this idea is higher than the degree of readiness of the state. Especially if we talk about banks: these are structures - not extraneous agents of economic activity. These are structures that are also controlled by the state as a shareholder" (Medvedev, 2011).

The first step in the proposed policy was the card itself, based on the assumption that the development of e-services could be completed simultaneously and should support any other forms of authentication and identification. The Universal Electronic Card officially became a political promise and a symbol of Medvedev's modernization program. His speech provided reinforcement and legitimization for the innovation, locating it within the national policy framework despite its weak regulatory status. Medvedev stressed that the government would not pay anything for this innovation, and would rather rely on the revenue model developed by the

financial sector; therefore, the card would become the most essential identification document in the country.

Institutionally, the faction of economic liberals aligns with the Ministry of Economic Development and the SberBank of Russia, which are responsible for development of the card's design, production, and providing infrastructural support for its operation. The Ministry of Economic Development is responsible for regulating and developing policies related to socioeconomic and business development in Russia. Between 2000 and 2007, Herman Gref was the Minister responsible for the liberal economic reforms in the Russian Federation, and was a major advocate for Russia being a part of the World Trade Organization, and was speaking publicly against the monopolization of the oil and gas sectors of the Russian economy. In 2007, he was appointed president of the state-owned SberBank, and was one of the critical stakeholders responsible for the development and management of the Universal Electronic Card.

Gref characterized the role of SberBank in this project in the following way: "Why banks? Because we follow the interests of our clients, and the state follows us. An attempt to create now a state infrastructure as an alternative to private one will lead to an absolute failure of the project. Five hundred or even fifty thousand terminals produced at public expense is, in my opinion, a misunderstanding of the scale of the project. It's unrealistic. This will never work. There are 800,000 terminals and ATMs in the country, and only existing banking network will be able to ensure the availability of this service at this stage" (Gref, 2011).

Both Gref and Medvedev would always emphasize the unlimited functionality of the card in their public statements. The "all-in-one" card was designed to become a tool to support identity verification and assist in establishing eligibility of the holder for particular services and discounts. It was also a financial instrument and therefore was designed in a way that was

flexible enough to enable future development. The list of applications was always open to options for added services and private partners providing those services. This functional flexibility was promoted by the SberBank through the agreements supported by the public-private partnership between regional governments and a joint-stock company called "Universal Electronic Card" (UEC JSC), who had a mandate to develop technical infrastructure and manage distribution of the card. This arrangement was reflective of the logic of commerce: anything that can be recorded as a transaction can generate revenue and can be added to the card. By 2014, in 20 regions the card was used to support payments for municipal services, to pay for a bus pass, to visit a doctor, and to enroll children to school. Among those regions five were leading in total numbers of issued and maintained cards: Lipetsk Oblast, Tulsk Oblast, Komi Republic, Chuvash Republic, Astrakhan Oblast (JSC UEC, 2014).

6.3.2: Technocrats and the "All-Access-One" Electronic Identity Management System

"We can provide secure access to the government websites and information systems through a secure method of online authentication using any modern authentication technology, for example mobile ID. The most important goal is to digitize the government services, the tool that enables online access is secondary."

Igor Shegolev (2010),
Minister of the Communications and Mass Media (*Minkomsviaz*)

While economic liberals were making sure that the Universal Electronic Card was implemented based on the financial model proposed by SberBank, the *Minkomsvyaz*[12] was occupied with finding reasonable technological solutions to support the provision of government

[12] *Minkomsvyaz* is commonly used in sources, even though the Ministry was rebranded in 2018 into The Ministry of Digital Development, Communications and Mass Media.

services online, and provide practical but secure access to government services consistently across the Russian Federation.

Igor Shchegolev, Minister of Communications and Mass Media from 2008 – 2012, stated that “his Ministry is convinced that the central element in the provision of public services in electronic form should be the state system of interdepartmental interaction and information exchange. Of course, the processing of the services themselves should be handled by the state" (Shchegolev, 2011).

One of the first problems was that, in order to provide the highest level of identity assurance, the eID needed to be machine-readable, to recognize credentials on the card, recognize the list of the activated applications, and exchange encrypted and protected information. As nobody was confident when exactly the UEC would be distributed to a critical number of users, the goal for technocrats was to build a customizable Single System of Identification and Authentication (ESIA) that would support different ways of online authentication, ensuring that access was provided on a “need-to-know” basis. Authorization of access to government digital systems can be completed using multiple options based on different factors of authentication: password-based access, using banking cards, biometric identity, or mobile ID with the help of the mobile application.

The front end of the ESIA would provide an access portal where individuals would authenticate themselves, but there was a need for back-end development as well, which would connect individuals to the right government database or allow them to update their personal record within a government informational system. The ESIA was supporting interoperability of information exchanged through a portal, in order to connect a citizen with the government entity online, where both points of communications would be verified and confirmed by the Single

System of Identification and Authentication. Technocrats were therefore focused on developing technology that would “join up” the government, improve data quality, and remove record duplication. They quickly realized that it does not matter what kind of secure key the citizen is using, a mobile card through a mobile application, or the Universal Electronic Card through a card reader. To maintain the quality of transactions, they all needed to access one centralized portal, where all government services are documented through registries of programs, services, and their jurisdictions.

The enrollment in ESIA is voluntary and supported for government entities or individuals interested in using Single System of Identification and Authentication. Citizens would register their personal or organizational accounts and provide information about their systems. During the registration process, the data is checked against existing state registers. When citizens are registering their personal profile accounts online, they need to confirm that their identity was verified either through an authorized body (e.g., individuals obtained their activation code from the Russian Post or Rostelekom), or using a qualified electronic signature, supported by the device issuing a signature verification key provided by the accredited certification authority.

Technocrats developed technological solutions supporting any type of access. According to this logic, the most important part of the e-government was not an electronic identity card but a standard secured portal that would connect government programs with their clients, to which that card or another instrument will provide a key, and that key can be trusted based on the verification process. This system was developed independently from the UEC project and was designed to support integration with different identification instruments, either UEC, MobileID or any other approved third-party identity provider. Technocrats were building “All-Access-One” system, where technology would be employed to support variety of authentication

solutions based on the different identity attributes depending on the role of the user. The same person may need to access government information systems in different roles, which require technical separation: as a unique private individual, as a government employee, as a government contractor. The Ministry of Digital Development, Communications and Mass Media relied on international standards and technologies enabling Federated Identity Management. In the beginning, technocrats relied on Security Assertion Markup Language (SAML) 2.0, an XML-based technical standard for exchanging authentication and authorization identities between security domains. Over time, more applications connecting to ESIA were requiring a more flexible solution, and the Ministry moved to the OpenID connect, which was simpler to implement and allowed clients to confirm an end user's identity using authentication by an authorization server.

The observation of technological specification portals where the electronic identity card holder could log in, confirms that technocrats speak a universal language and are concerned with the similar technical problems as their Western counterparts. There is growing interest and utilization of open-source protocols and standards, which are managed by international associations uniting technology enthusiasts dedicated to a particular standard, software, or product. They are updating these protocols, and fixing bugs for the benefit of the wider community of developers. This collective action of technological solidarity (Reina-Rozo & Medina-Cardona, 2021) towards free knowledge, and exchange of best practices and solutions is inevitably becoming a part of the recognized technological development and was evident in the case of the initiatives implemented by the Russian technocrats and their contractors.

6.3.3: The Siloviki and the "One-for-All" National Electronic Passport

Siloviki, in Putin's regime, are men in uniform with a background in the secret police, the military, and law enforcement (Taylor, 2017). They protect Putin's position and maintain the legitimacy of his presidency. Not all of them belong to the interpretive community of the electronic identity card innovation, but most of the employees involved in the national identification system are siloviki. All Ministry of Internal Affairs staff wear a uniform and graduated from a special law-enforcement educational institution. Siloviki are responsible for the management of residence registration documented in the internal passport (in Russian, "*propiska*") and enforcement of the regulated movement of population within the country, as well as issuance of both international and internal passports under the jurisdiction of the General Directorate for Migration Affairs at the Ministry of Internal Affairs (*Ministerstvo Vnutrennikh Del - MVD*). Traditionally, MVD regulates migration flows within Russia, and controls the free movement of Russian citizens between different cities, regions, and outside of the country.

Between 2012 and 2017, the agency of the Federal Migration Services (FMS) was removed from the jurisdiction of the Ministry of Internal Affairs under the direct jurisdiction of the Russian Government. One of the reasons was to support the implementation of the Universal Electronic Card, and the head of FMS, Konstantin Romodanovsky (2005-2016) was participating in all public committees and hearings; however his speech was often redacted from the released documents as confidential. In 2016, Federal Migration Services was returned to the jurisdiction of the Ministry of Internal Affairs by Presidential Decree. Romodanovsky was the only representative of FMS involved publicly in electronic passport development, and under his management, FMS developed a document prescribing standards and design of the Russian electronic passport. Unfortunatly, the document was classified and never posted online.

The involvement of siloviki in the project, managed by economic liberals and technocrats, was documented but their position was not publicized until 2014. In 2014, the occupation of the Autonomous Republic of Crimea, a territory of Ukraine, resulted in growing disagreement between economic liberals and siloviki factions and their interpretations of the national identification system modernization. Global financial powers responded with economic sanctions. Under pressure from the United States Department of the Treasury, Visa and Master Card suspended their services (Nelson, 2015) for a number of Russian banks working in this territory. As a result, the technological narrative of progress and innovation during Medvedev's presidency transformed into a politicized debate about the old confrontation between the West and Russia. The promise of technological compatibility of the UEC with the international payment systems, based on an American microchip, was no longer an acceptable or appropriate policy solution.

Political commentaries opined that the current design of the UEC undermines Russian national interests to remain in control over post-Soviet territories and support the Russian speaking population (Vedomosti, 2015). This anti-Western discourse became very prominent in the media and policy discussions about the possibility to distribute the Russian Universal Electronic Cards to the population in Crimea to facilitate integration with the Russian public sector slowly disappeared The narrative of population control through the identification card has intensified during the first month of annexation, revealing a contest between electronic identification, which would mitigate costs and preserve financial security, and a traditional passport system which would be a more reliable marker of national identity.

The first immediate step was a rapid and costly transfer of Russian passport services and staff to the territory of Crimea and an intensified process of massive passportization

(Krym.Realii, 2014). Initially, the UEC was presented as one of the most cost-effective solutions to address the paralyzed financial sector on the peninsula and a challenge to provide identity documents to a new population (Popov, 2014). However, the national electronic payment system PRO100 was still under development, and SberBank, a founder and operator of the UEC, had to close and relocate all its international branches located in Crimea to avoid financial sanctions.

Fast passportization of the newly "embraced population" (Torpey, 2000) was crucial to the political legitimization of the occupation, and important for financial and administrative support of the welfare groups dependent on the Ukrainian government. Within weeks Russian passport officers started processing passport applications in all Ukrainian passport offices across Crimea. Simultaneously, Ukrainian Post offices were utilized to establish money transfers for retirees and social beneficiaries who had obtained new Russian passports and therefore a new national identity. People flooded the occupation administration buildings hoping to obtain a document that, even in the case that annexation failed, would secure them with financial benefits, and ability to travel and work in the Russian Federation. The occupation of Crimea was not solely a military operation and not the result of a "referendum." It was also preceded by an annexation by passport (Artman, 2014), a long-established process of the national identity documents being distributed to the foreign national with some Russian background and through Russian diplomatic offices. Similar strategy was employed on occupied territories of Donetsk and Luhansk Oblasts, where as much as 35% of the local population obtained Russian passports by the end of January 2022 (Burkhardt, 2022). This number was used as a political justification for protecting Russians abroad by means of military aggression against Ukraine, including calls for physical and cultural genocide of Ukrainian population.

During this process of "creeping annexation" (Artman, 2014; German & Karagiannis, 2018), the Russian passport acquired symbolic and cultural meaning making its possession desirable and valuable. The success of this old-fashioned paper-based identification practice managed by the Federal Migration Services demonstrated practical benefits of the legacy system not compatible with the global technological and financial payment standards like the UEC. The UEC innovation turned out to be so dependent on the global financial and technological industries that Herman Gref publicly denied a proposal to distribute the UEC in Crimea (Amic.ru, 2014), because the card was licencing MasterCard technology M/Chip and SberBank could not afford American sanctions limiting work of MasterCard in the Russian Federation.

This administrative operation of passportization increased the power of the siloviki and the significance of the FMS agency. They proved that documentation of the Crimean population as Russian citizens was deemed paramount to the new Russian imperialism, and more important than finding solutions to the problem of overdependency on the Ukrainian transportation network, energy, resources, and the financial security of residents in Crimea. Initially, crowds in passport offices consisted predominantly of ethnically Russian citizens of Ukraine, retirees, and beneficiaries of social assistance. During this period, passport offices were simultaneously distributed within an existing network of the Ukrainian post offices in Crimea after one month of occupation. The second wave of passportization targeted Ukrainians and Crimean Tatars population, who were deemed by the occupational administration to be foreigners and required residency permits, which was nearly impossible to obtain despite the existing procedure. In order to have access to the job market, social insurance, health insurance, and public services, everyone was supposed to apply for a Russian passport. Overall, passportization was finished quickly, as opposed to taking 5-7 years. However, there is no agreement about how many

passports were issued and whether their issuance was legal even under the Russian legal framework not to mention under international law. There were reports and complaints about passports being selectively revoked, in addition to corruption, violations, and mistakes (Kommersant, 2015). The Russian passport in Crimea again became a reflection of the passport legacies as state monopolization of the legitimate means of movement (Torpey, 2000), where the state reinforces its sovereignty over newly acquired territories through control over people identity and mobility, sorting "elements near" (Crimeans who applied for a Russian passport) and "elements far" (Crimeans who kept their Ukrainian passports and avoided initial wave of passportization).

In 2017, the UEC was officially discontinued and the monopoly of the state on means of identification was supported again with the decision to assign a new project – the national e-passport – to the Ministry of Internal Affairs and the Ministry Digital Development, Communication and Mass Media. The siloviki and technocrats united to deliver a new plan that would be easy to onboard to the already created ESIA portal and associated infrastructure. The electronic identity document is a substitution for the existing paper-based internal passport; a plastic card containing similar personal identity information (MVD, 2020). This new passport would be issued by GOZNAK, a joint-stock company that manufactures banknotes, postage stamps, paper blanks for passports, birth certificates, marriage certificates, and other security documents in the Russian Federation. The passport would contain the microchip produced in Russia at Micron (Micron, 2021). The biggest difference between the Universal Electronic Card and this new card is the limitation of personal identifiers printed on the e-passport (Figure 4). Linkages from the passport to other identifiers like SNILS, medical insurance numbers, or driver's licenses would be possible through selective inclusion of that information on the card

microchip per the individual's request. Another significant element is the lack of the payment capabilities with this new card. The new e-passport does not capitalize on the universality principle of eID and instead focuses on the identification function. At the same time, citizen's residential registration address is included, and individuals would be required to apply for a new e-passport every time they move. Which again reinforces the legacy of the state monopoly on the means of identification.

Figure 5 Russian Federation Citizen's Identity Card

1. Legal Last Name	8. Card Holder Signature
2. Date of Birth	9. Issuing organization code
3. Gender	10. Issuing organization name
4. Place of Birth	11. Residential registration address
5. Issued	12. Biometric photo
6. Expiry Date	13. Machine-readable zone (MRZ)
7. Identity Document Number	

Note. The image is a proposal of the new electronic passport presented by the Federal Government official, Maksim Akimov at the government briefing on implementation of the national identification document in the Russian Federation (2019, July 17) http://government.ru/news/37379/

6.3.4: Conservatives/Traditionalists and "None for Us". The Case of Global Conspiracy

> *"A total, market-based, "digitization" of public services is a threat to the Russian national security, constitutional rights and a very safety of every individual."*
>
> Olga Yakovleva, 2013
> Association of the Orthodox Lawyers[13]

The policy community of conservatives/traditionalists is not as cohesive in organizational or institutional terms as the first three. Its members mobilized to resist the implementation of the electronic identity card and represent a variety of organizations: the Russian Orthodox Church, the Communist Party, the Izborsk Club, and a network of not-for-profit organizations against digital slavery, vaccination, and juvenile justice reforms. They are not a classic example of political opposition. Rather, they act in Russian politics as Putin's regime supporters, playing the vital function of the orchestrated or puppet opposition. They provide means, venues, and opportunities for the general population to disagree with official policies while being under the control of the various organizations involved. They share some ideational concepts with the anti-globalist's movement, conservatism, Russian monarchists, and communists (Laruelle, 2016). These conflicting movements are united via their anti-Western and antiliberal orientation and their advocacy for modernization that embraces Russian traditions and history – Slavophilia (Engelstein, 2011).

While the Ministry of Communication and Mass Media and the Ministry of Economic Development were actively framing the new electronic ID as an apolitical and progressive technocratic solution, promising to solve old problems of the paper-based bureaucracy, this

[13] Olga Yakovleva is an influential activist within the movement. She's the author of the most books and articles on the subject, a documentary film-maker, and one of the contributors to the online website: ProtivKart.ru [against cards].

group would criticize it as a process of Westernization and globalization. The fact that the role of the Ministry of Internal Affairs and Federal Migration Service was diminished and reduced to the recipient of the final policy solution did not insulate these agencies from the policy struggles. On the contrary, they engaged in alternative and creative ways to reinforce the traditional monopoly of the Russian passport bureaucracy and to prevent the identity card oligopoly from realization.

It is essential to understand that without informal support from the siloviki, traditionalists would not have demonstrated such significant opposition to the Universal Electronic Card. The siloviki identified potential UEC opposition among several groups and shared their position through quasi-democratic institutions of the Russian government. First, the Communist Party of the Russian Federation and the Russian Orthodox Church engaged in the political mobilization of the anti-UEC movement. Second, the Federal Migration Services developed an alternative national e-passport policy framework without the payment functions or private sector investment. I argue that both are not separate events; rather, they are two sides of the same coin – a "policy sabotage" (Brehm & Gates, 1999) supported and strengthened by the siloviki policy community. This sabotage was based on two strategies: first, unpacking the political meaning of the UEC and mobilizing a popular movement against the card, and second, developing a concept of the E-passport and framing it as a safe alternative.

One of the most visible groups involved in deconstructing the political meaning of the UEC through an organized social protest was the Russian Orthodox Church. Their strategy highlighted the privacy concerns associated with technology and the protection of personal information of Russian citizens from global financial and technological institutions. The Church's leadership issued an official position and addressed it to the Russian State Duma summarizing the dangers of the electronic identity card: "There is a reasonable concern in

society that the use of a lifetime personal digital identifier in the form of a code, card, chip or the like may become a prerequisite for everyone's access to all vital government services and social benefits. The use of an identifier, coupled with modern technical means, will make it possible to exercise total control over individuals without their consent - to track their movements, purchases, payments, medical procedures, provided social assistance, other legally and socially significant actions, and even details about their personal life" (Russian Orthodox Church statement, 2013, para. 3). Furthermore, questioning the legitimacy of the card's technology: "The Church considers unacceptable any form of coercion of citizens to use electronic identifiers, automated means of collecting, processing and recording personal data and personal confidential information. The realization of the right to access social benefits without electronic documents must be provided with material, technical, organizational and, if necessary, legal guarantees. The Church considers inadmissible the forced application of any visible or invisible identification marks to the human body" (para. 5) The reference to the identification marks in relation to the human body is a reference to biometrics such as fingerprints. This Church criticism was different from their previous public involvement, advocating for government restrictions on abortion or Orthodox religion lessons at all public schools. The Church also never commented publicly on political surveillance conducted by Russian law-enforcement, but they were specifically successful in advocating against the UEC as a threat to personal privacy.

The official Church authorities instructed priests to work with Church members across the regions, to organize public hearings in larger cities, to mobilize public protests against the UEC, and to write letters to the government and elected representatives asking the government to stop the implementation of the UEC. It is interesting that some official meetings and public hearings were attended by representatives of the Ministry of Internal Affairs, who would

participate in discussions and clarify that the protest is not against identity cards or passports in general, which can be very useful tools for protecting the security of our society, just like the Soviet passport was (Public consultations, 2012). The Church was also organizing protests, involving its members who were questioning the Western technology used in the development and design of the UEC (Yakovleva, 2013). Their pressure was successful and the possession and use of the UEC was made voluntarily in 2013. In 2017, when MVD announced a new e-passport project, it was specified that passports in the form of the eID are available only on a voluntary basis, and people may continue using existing paper-based identity documents.

Along with the Russian Orthodox Church, Gennady Zyuganov (leader of the Russian Communist Party) and Vladimir Zhirinovsky (leader of the Liberal Democratic Party of Russia) both criticized the new Universal Electronic Card, and proposed the return of the Soviet passport, which would define one's nationality or ethno-cultural background. The Communist Party also collected signatures from people advocating the preservation of the old Soviet passport. These people wanted the old passport to be recognized by government institutions so that they could access services and maintain Soviet identity, which in turn was capitalized by two parties as their shared values of Soviet nostalgia (KPRF, 2015).

The anti-UEC movement, a bizarre combination of Communist activists and the Orthodox clergy, was never able to attract significant crowds but enjoyed multiple opportunities to express disagreement and amend policy. This movement against the Russian Universal Electronic Card was a partially successful political performance orchestrated by the siloviki, in different institutional settings. Formally, the movement was organized through the mobilization of particular social groups and their participation in round tables, meetings, and the drafting of resolutions. The movement did not have a recognizable political leader but rather a number of

experts and public activists (Yakovleva, 2013; Orlov, 2012). It was supported by websites (protivkart.com), books (Tsareva, 2018), movies on Youtube channels (SlovoTV), bloggers, and protests marches. This information was distributed among the population through the network of Orthodox churches, which would be responsible for the mobilization of participants in particular public events. Those events included public hearings and round tables (Grishenko, 2014), interviews (Yakovleva, 2013) and recorded public protests (Moscow, 2011; Cheboksary, 2012). Russian journalists conducted some investigations revealing that the movement was working by the "empty shell" principle, where its representatives like Galina Tsareva or Olga Yakovleva despite many public engagements, did not have a real office, or were very hard to reach for interview (Voeikov, 2012; Karpov, 2015). It was impossible to understand the formal organizational structures or its financial sources. However, despite the murky background, representatives from these movements were often included among official public speakers during the UEC meetings in the State Duma (Karpov, 2015). They were also often endorsed by some Church leaders and their books and interviews were published on the religious websites (pravoslavie.ru).

6.3.5: Mapping Interpretive Communities in Policymaking of the Russian Universal Electronic Card

Each of the identified factions promoted their own view of the identification document summarized in Figure 6.

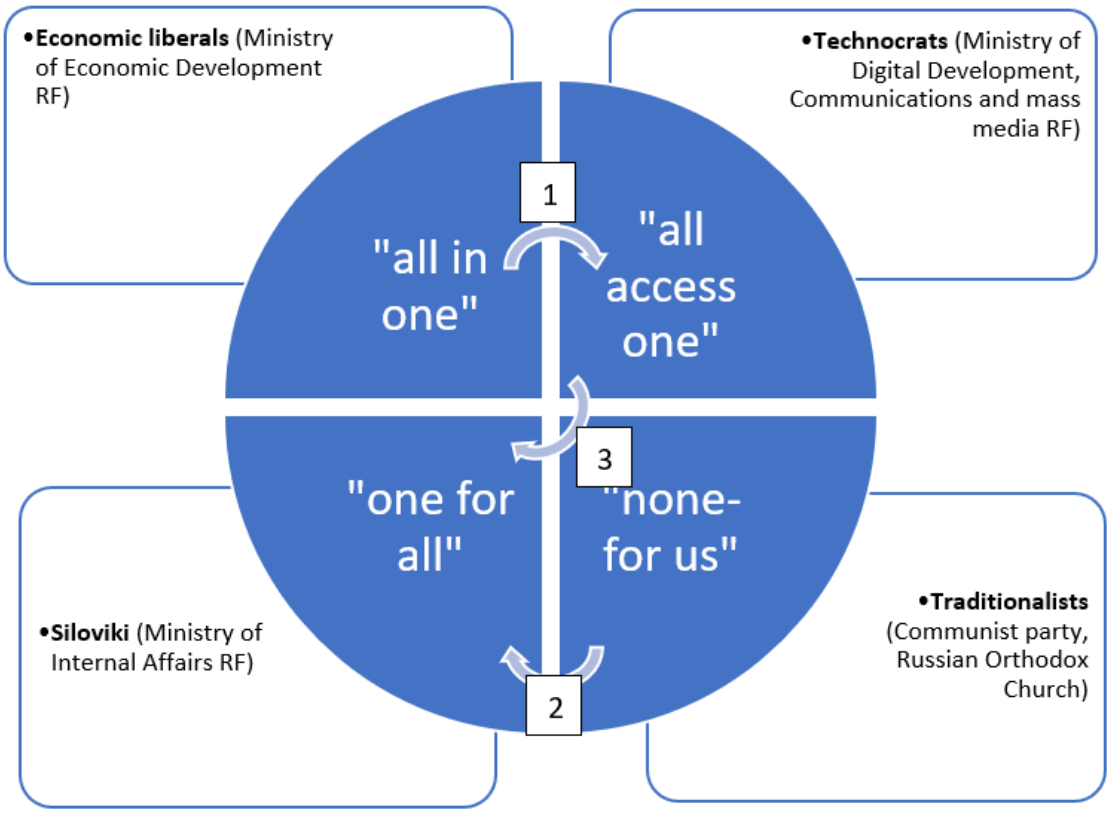


Figure 6 Interpretive communities and four views on the electronic ID

The UEC business model attempted to break down the historical continuity of identity practices on several levels: exclusion of the traditional expensive passport bureaucracies; challenging the siloviki faction within the Presidential decree, and reinforcing the power of economic liberals; and finally liberalizing identification practices through breaking down the hierarchical and centralized bureaucracy into horizontal and flexible public-private partnerships, which would develop technological tools for the identification, authentication, and authorization of citizens. This not only required public funding but also promised profits for all parties involved. It was a drastically new and challenging policy provision. The technocrats responsible for building an informational infrastructure of government portals were not strictly limited by the card design or functionality. They were building it simultaneously with the regional

developments of the UEC JSC, understanding that before the UEC was fully onboarded by each regional administration, other instruments of online authentication and authorization could be supported.

Most significantly, Figure 6 illustrates the difference between economic liberals and technocrats in terms of their view of the model of electronic identity, and the policy relationship between them. Economic liberals are trying to maximize profits through the concentration of multiple identifiers and functions in one card. The "all-in-one" UEC should substitute all traditional instruments as the most convenient and multifunctional solution, one that can be used every day by everyone. This idea is being transformed through the technocrats' interpretation of electronic identity management, where all existing identity instruments can support access to one portal, and where portal security and access management are of supreme importance. The position of technocrats on the flexibility of the authentication tools was negatively impacting the uniqueness and necessity of the multifunctional solution (Figure 6, arrow 1). It was not so easy to implement this technological innovation for a number of reasons: the UEC was proposed as a business model of policy innovation that should have been implemented outside of the traditional bureaucracy but within a new high-tech Ministry of Communication, and could be contrasted with the traditional reforms of state identification policies, managed within the Ministry of International Affair and overseen by its Federal Migration Service.

The Russian national identification administration, controlled by the siloviki interpretive community, opposed the UEC proposal as a market-driven solution, embedded in the international e-commerce system, and undermining Russian national security and sovereignty. Economic liberals and technocrats, unable to receive security clearance for internationally supported technological solutions in smart cards, shifted the policy goal from reforming a

national identification system to incremental changes at a regional level. The Russian Government supported the plan to establish a nation-wide network of public-private partnerships dedicated to the implementation of the secured online authentication and authorization solutions enabled through electronic identity cards. public-private partnerships would bring together the banking industry, federal and municipal governments, and smart card manufacturers to design and deliver regional electronic identification solutions to repeat the experiment of the Moscow Social Card across the regions. According to a statement on the official UEC page: multiple eID projects with the Moscow Social Card functionality tested across the Russian Federation would be satisfactory enough and could facilitate the development of the smart card technology sufficient for use at the federal level.

Economic liberals and technocrats are responsible for the economic and financial management, macroeconomic stability, and credibility of the Russian Federation in the international community. They are competing with the ever-growing power of the siloviki, Putin's strongest allies, rooted in the enduring legacy of the KGB in providing political leadership in the areas of energy, defence, and security. Characteristically, the ever-changing policy trajectory of the Universal Electronic Card was a reflection of the factional struggle between these two political groups that have held different ideas and beliefs about the state identification regime. Economic liberals proposed the new smart card, which can be delivered by the private sector, while the Siloviki would like to maintain a state monopoly over the new technology. Economic liberals and technocrats were embracing the ideas of the e-government reforms and proposed a model of identity management using new information and communications technologies, such as smart identity cards, as a solution to the inefficiency of

the Russian public administration. The Universal Electronic Card was framed as a seemingly depoliticized solution, but the struggle was indeed political in nature.

This initial focus on the UEC as an authorization technology was a reflection of the separate institutional mandates between the Ministry of Communication, responsible for the implementation of the Electronic Russia program, and the Federal Migration Service, responsible for administering the internal and international passport of the Russian Federation, and enforcement of migration regulations. State identification practices and their legacies, explored in Chapter 4, were simply outside of the competencies of the Ministry of Communication, as well as technocrats' innovative ideas concerning the development of the ICT technologies and new systems of identity management within the Russian public administration.

The troublesome implementation of the UEC was a result of the drivers pushing forward the electronic identity card technology and counterproductive forces that challenged justifications and rationale behind it. The proposed business model of the UEC was challenged through political contestation of the puppet opposition and administrative sabotage by siloviki. While the Ministry of Communication, which fully controls the internet, communications, and e-government administrative reforms, was responsible for the ICT reforms and development of the shared technological standards across regions and bureaucratic hierarchies, the Federal Migration Services was reinforcing its position in preserving hierarchical and centralized control over passport identity, where the identity document served to manage population movement within and outside of the Russian Federation.

However, this illustration provides yet more evidence that the two ministries were addressing similar policy areas separately using different strategies, institutional authorities, and offering solutions that benefited their administrations. Their policy engagements reflect

administrative and political competition to control the development of the new types of identity systems enabled by ICT technologies.

6.3: Views on the Technological Innovation and two Models of State Identification Systems

Smart electronic identity cards are often utilized in jurisdictions that rely on the liberal principle of oligopolies on the means of identification, where functions and information are shared between government and the private sector, whilst protecting that information. In Russia, this very principle of shared cooperation and responsibility met resistance, and the longer it took the electronic identity card to take off, the more significant was the formulation of the alternative vision, which reinforced the state's role in the security of identification practices, thus undermining market-driven solutions. The business model of the UEC experienced constraints on an institutional and ideational level. The Russian state cannot share information with the market because this undermines traditional understandings of hierarchies, national interests, and sovereignty.

The use of the case study method intended to capture the complexity of the object of study from different perspectives, to understand how the phenomenon of the electronic identity card is socially constructed, how its implied rationality is limited by conflicting interpretations, ideas, and myths about its appropriateness, and whether it is legitimate in various cultural and political contexts. Myths are the stories that help us explain the world (Segal, 2004). Mythology helps us to make sense of something that does not make much sense, like the rise and failure of the Russian UEC. Yakovleva (2013) criticizes the Russian government's approach to modernization as Westernization. She outlines a number of assumptions that are not analyzed

critically as they should be: “the need to implement an eID as an inevitability of the technological progress”; “all developed Western countries implemented eIDs and we are learning from them”; and “self-modernization, an opportunity, an improvement that would inevitably spread to different spheres.” Similarly, the opponents of the UEC were citing ccommon fears as based on popular myths or narratives – “technology and science are used to control population” (Tsareva, 2017), “Western countries promote electronic identity cards to take control over Russia” (Ovchinsky, 2017), and “Today they give us electronic IDs and tomorrow vaccines with nanochip” (Tsareva, 2013).

Interpretive policy communities refer to different myths when they create and translate persuasive messages to the public, seek public approval, or are looking to shock the public. Sometimes those myths inform policy decisions when they are internalized as values and beliefs by the members of the policy communities. Those myths then become an integral part of the policy language and process. In particular, policy myths expressed by the members of the four interpretive communities inform two dichotomies: technology vs bureaucracy and sovereignty vs globalization.

6.3.1: Technology vs. Bureaucracy: E-Government and the Oligopoly on the Means of Identification

A policy myth supported by e-government in general and the electronic ID is that technological modernization would enable transformation of the classic “iron cage” of the Weberian bureaucracy. However, the process of introducing e-government regularly comes across organizational resistance and is accompanied by numerous failures. These failures are usually explained by the outdated skills of public officials and their unwillingness to work in

new ways. But if we look at the ways the MVD was opposing a banking solution to the eID, specifically its compatibility with the technological standards of the international payment systems, it becomes clear that with the introduction of e-government is concerned not with efficiency, but with legitimacy. E-government modernization is often presented as a false dichotomy, one that either preserves the old ways of inefficient bureaucracies by staying away from modern technology, or one that creates a digital user-friendly government by implementing scalable and progressive internet-based technical solutions.

First, this false dichotomy ignores existing political problems and conflicts in the system, trying to simplify them as problems of the old-fashioned red tape bureaucracy which can be fixed with a modern technical instrument. However, without knowing exactly what problem needs to be solved, it will be complicated to select an appropriate technical solution.

Second, when this false dichotomy does not disappear after years of modernization, the choice of technology is not subject to scrutiny. Instead, new technological concepts are proposed to ensure that technological imperatives are catching up with the new innovations. The Russian government replaces the concepts of e-government or electronic Russia with the new term – digitalization by renaming the Ministry of the Telecommunication and Mass Media into Ministry of Digital Development, Communications and Mass Media in 2018. The failures of the UEC are addressed with the new Russian e-passport, which was designed by Russians, for Russians. Again, the administrative practice of the Russian state identification is not subject to modernization or liberalization reforms. Only its means, the eID, will be modernized using digital technology.

The interpretive communities of the economic liberals and technocrats are high-ranking officials who make decisions on the implementation of state systems, as well as representatives

from the IT industry, IT expert communities, and technology salespeople. Each of these groups is distinguished by its own kind of "dangerous enthusiasm:" government officials exaggerate the potential of information technologies right up to their "idolization," IT campaign leaders suffer from technophilia (Ullman, 2012) – a belief that using the latest technology can solve any problem, experts are prone to administrative fashion and tend towards fashionable solutions to chronic managerial problems, and salespeople are required to advertise the benefits of the product with the goal of selling it. It is easy to notice that there is no end consumer among them: neither ordinary employees of authorities who have to work with new technologies, nor ordinary employees of IT campaigns who will be responsible for technical problems, nor actual citizens who will be using electronic government.

The problem is that the MVD department, which is responsible for passports, was not involved in the decision-making because they were defined by the government as a target of change, not an agent of change. As a result, if the main decisions are approved centrally, and the experts participating in the discussion are interested in strengthening their institutional positions by supporting the project, and potential end-users are completely cut off from making decisions (Collingridge, 1990, p. 13), then before the system is implemented, the negative consequences of its implementation cannot be calculated. After considerable funds have been spent on its implementation, it is almost impossible to make any changes, and therefore the project has to continue to move at times in the opposite direction, ignoring the issue of efficiency.

Economic liberals and technocrats responsible for the Russian Universal Electronic Card used a whole series of techniques aimed at supporting the ideology of e-government and addressing the lack of efficiency in the existing identification system. The prospect of the UEC had limited application to institutionalized problems, focusing instead on electronic services that

are simply information services, at best online authentication methods to access those services. This, and not the constant emergence of new innovations in the field of information and communication technologies, explains the continuous multiplication of e-government models: each time the desired future is called something different, it is based on the same belief that new technologies can lead to a revolution in public management.

Proponents of technological innovation share beliefs in the absolute positive impact that Electronic Identity Cards are going to have, and ignore the costs required not only to implement the technology, but also to maintain it and protect the security of the newly developed information systems. The myth of the electronic ID as inevitable progress was supported and communicated by economic liberals and technocrats. The analysis of the documents proposing and planning the implementation of the Russian electronic identity card supported and re-stated several myths: the myth that the e-identity card is a new and better identification document; the myth that information technology is a source of progress; the myth that these technologies improve efficiency and efficacy; and the myth of an enlightened citizen whose need to influence the government would be met through the "electronic office" or "one window." These are precisely the myths that have little in common with the real "muddy" implementation of the Universal Electronic Card, but which were regularly reinforced with every newly updated deadline for implementation.

6.3.2: Sovereignty vs. Globalization: Conservative Modernization that Sustains the State Monopoly on Identification

The idea that conservative modernization sustains the state monopoly on identification is based on a false dichotomy. You either integrate fully into the global network and lose your

technological sovereignty, or you maintain sovereignty and support full control over information. The siloviki and traditionalists adopted this perspective on the Universal Electronic Card and e-government as a criticism of technocratic ideology – the myth that the Electronic ID is part of a global conspiracy (Thomas & Zhang, 2020).

This dichotomy is based on the assumption that the spread of new technologies and supporting economic structures is fundamentally changing the entire management system of global socio-economic processes (Larina & Ovchinsky, 2013). On the one hand, there are new opportunities for total control over the behaviour of citizens on a global scale. On the other hand, it makes possible the emergence of private cross-border systems for managing economic, social, and political processes that affect the national interests of states and their associations (Ovchinsky, 2017). The basis for such systems is provided by global social and trade information networks and cryptocurrencies, the internet of things, and other impersonal information transactions, which take international trade and finance outside of national jurisdictions and their regulatory frameworks. However, the statement that the Russian government must only use Russian built technology to protect its sovereignty from the negative impacts of the globalized technological markets is a false dichotomy. This dichotomy was instrumental for the interpretive community of conservatives/traditionalists, and arguably assisted their attempts to mobilize protests against the UEC. The most recent statement by the Russian government went further stating that either Russia would develop technological sovereignty or disappear as a state (Medvedev, 2022).

One of the global conspiracy myths, utilized by the Russian Orthodox Church, was that global corporations were specifically targeting the personal information of Russian citizens in order to have better control over Russian territories, resources, and people. Another example is

the ideological work of the Izborsky Club[14] and in particular one of their regular contributors to its propaganda magazine "*Russian Strategies,*" Vladimir Ovchinsky.

Ovchinsky was a leading policy advisor on reforms within the Ministry of Internal Affairs since 2012, including reforms of passport legislation. While there is no official record of his statements as an employee of the Ministry, there is an abundance of his writing in magazines and non-fiction literature which can explain the advice he provided to the Ministry. He has produced a substantial list of non-fiction literature alarms about the dangers of Western technology for Russian sovereignty. He argues that those who control the technology have unlimited power (Ovchinsky, 2017, p. 4). He argues against a digital revolution because growing technology improves the ability to implement surveillance systems to monitor and control peoples' behaviour. And the problem with that is that this surveillance is not happening within jurisdictional borders but globally (p. 18). He is concerned that we are witnessing private corporations, most often American corporations, developing independent informational systems to control economic, social, and political processes outside of the national regulatory system. Similar materials, books, and articles were published with the support of Izborsky Club members, recognized political leaders, and some public opinion leaders.

Therefore, it is not surprising to see how Russian interpretive communities connected to the state were concerned with personal information, not in terms of rights, but in terms of national security and identity. The state is responsible in a paternalistic way for the information of its citizens, because they are Russian subjects and not global citizens with the universal right

[14] A broad coalition of politicians, members of the Russian State Duma, academics, and government policy employees united against liberal and Western-oriented reforms.

to control their personal information. The Russian state is concerned with the personal information of its citizens and their information needs to stay on Russian servers.

The privacy implications of the electronic identification system are central to critical interdisciplinary research, and reveal themselves in the Russian case in a surprising way. First, critique of the UEC employed similar language to the critiques of capitalism: that it is a tool for global information surveillance and American imperialism, through the expansion of American technology solutions and servers. These issues are very important: who is responsible for the governance of information processed by multiple organizations in different countries? What would be the building blocks of global technological governance, and what would be the power balance? So far only the European Union was able to enforce its own regulations through the General Data Protection Regulation (GDPR) framework. Before the recent military aggression against Ukraine, the Russian Federation was sometimes successful in enforcing its informational rules on global technological giants. However, the problem of how to balance sovereign rule over the population within a nation territory and universal informational human rights (the right to know and the right to privacy) remains, especially where the sovereign controls and manipulates the interpretation of those rights to support an authoritarian regime.

6.4: Chapter Conclusion

This chapter has outlined ideas about electronic identity innovation expressed by the four different interpretive policy communities, and has analyzed their views on innovation as a symbol of technological progress, which are expressed through multiple conflicting interpretations regarding the practicality, legitimacy, and morality of this technology. By mapping factionalism in the making of policies for the Russian Universal Electronic Card, I identify two antagonistic policy models targeting reforms of the state identification system, based on the technological solutions of the electronic identity card. The first model, business modernization of the public administration based on the *Oligopoly on the Means of Identification,* which relies on the banking and IT sectors, favours market solutions to government problems through a public-private partnership. The second model, conservative modernization which enforces the *State Monopoly on the Means of Identification*, is concerned with the enforcement of the state control over electronic identity card technology, from design to production and implementation.

The growing contradiction between these two models was an unintended consequence of a policy choice to isolate the Federal Migration Services Agency, responsible for the internal passport system, from the decision-making process, while preserving their authority over legislation and policies governing citizen identification. Instead of reforming the existing system, the group of technocrats from the Ministry of Communication and the economic liberals from the Ministry of Economic Development took exclusive control of the UEC's design and implementation as a private alternative to the national passport, hoping that practical usability and convenience would transform it into a federal identity document. In other words, they hoped for "function creep," that more institutions and people would trust their smart card with the high-

level technological security developed in the banking sphere, and would choose it over the traditional paper passport for identification purposes. However, the policy trajectory created two persuasive ideological concepts about the function of the state identification system, each developed within a specific institutional and legislative framework, political power, and ideational context.

The next chapter gathers the findings from this analysis of institutionalized legacies of the Russian passport system, and illustrates how they can be applied to explain the failure of the UEC, but also why this failure did not result in abandonment of the idea of electronic identification. Instead, the Russian government now approaches the idea of an electronic identity document from the position of state control and technological sovereignty. This chapter also explains Russian sovereignty as a paternalistic model of informational rights and privacy protection. This model reinforces the need of the Russian state to embrace its monopoly on the means of identification through technological sovereignty.

Chapter 7: The Fall of the Russian Universal Electronic Card and the Problem of Data Sovereignty

7.1: Introduction

The previous chapter has established the conflict between two models of electronic identity card development. The business model of the Oligopoly of the Means of Identification is based on the assumption that state identification systems should be less about the state and more about integration of the available and tested private sector solutions to facilitate digital identity verification. This model relies on the idea of proportional risk management and is informed by the international e-government movement. This model does not take into account political factors and tends to view technology as a neutral solution selected rationally by decision makers to meet their organizational requirements. The second model is concerned with the role of the state against the forces of globalization, and adopts a more traditional view of modernization. This model is concerned with the security of government information and is critical about outsourcing government functions and systems to the private sector, especially in the context of the globalized technological solutions. The security of information is achieved through the full control and ownership of the information collected by government agencies with government directly and fully responsible for its protection. This model views state as a monopolist of the information flows in the society from the perspectives of the state control of the sources of information for the purposes of national security and social stability.

In this chapter, I will attempt to connect the ideas expressed by the identified policy communities to find similarities and connections with the historical legacies of the Russian passport system. I hope, therefore, to propose some more general theoretical ideas that transcend

history and remain influential in shaping and directing the modernization of state identification systems.

Even though the legislation prescribing the transition to the use of the UEC was in place since 2010, the Russian Electronic Universal Card policy was marred by optimistic announcements and slow progress. In February 2011, the Government announced that the first card would be issued on January 1, 2012, and the project would be fully implemented by January 1, 2014, based on the assumption that the system of cross-departmental electronic information sharing would be in place by the middle of 2012 (Commission on Modernization and Technological Development of the Russian Federation, 2011). However, the system was not implemented in 2012, as it failed to receive a security clearance certification from the Federal Security Service (FSB). The card's implementation was postponed until January 2013. The FSB had a special department responsible for information security within the Russian Federation. All public sector computer systems involving electronic exchange of information require certification from this department. The FSB certification would confirm that technological innovation was not only in compliance with the legislation, regulations, and government security policies, but also ensured that informational sovereignty of the state is protected from external forces (Lukatski, 2011).

The year 2013 was a year of new challenges and new policy players. First, the project failed to provide sufficient financial incentives for participating regions and private sector institutions to cover the costs associated with the card's infrastructure. Many regions withdrew from the project due to financial difficulties, while SberBank, the most prominent Russian bank, remained the only financial investor in the JSC UEC. From the beginning, the project generated

massive financial losses (UEC Financial Report, 2011, 2012), which in turn required the leading investor to foster the technological design of the card, embracing the broad spectrum of payment applications linked to a national payment system (PRO100). Second, the Russian Orthodox Church engaged in the mobilization of grass-roots opposition to the Universal Electronic Card. Church representatives referred to the card as a foreign interest instrument of electronic and financial "slavery" which undermines Russian sovereignty and traditions (Dymova & Al′kina, 2013).

Finally, in September 2013, the Head of the Federal Migration Service, Konstantin Romodanovsky, announced that his agency was working on the development and implementation of the new electronic passport with e-signature capability, which would facilitate online access to government services, including a pilot project starting in 2015 and full-scale implementation at the federal level in 2016 (Romodanovsky, 2013). It took almost another decade after that announcement, when in December 2021, the government officially confirmed that, starting in 2023, the Ministry of Internal Affairs would be issuing new electronic passports in the form of a plastic card (TASS, 2021). The UEC project managers responded to the initial announcement by Romodanovsky critically and characterized this step as "duplicating and undermining all the technical progress and private sector investments into the UEC project" (Popov, 2013). As a result of these pressures, the status of the card has changed from mandatory as per legislative requirement (Federal Law No. 210-FZ, 2010) to voluntary, through the formal requirement to document opt-out documented in the new art. 26 (210-FZ legislative update, 2013). However, even with the opt-out option, economic liberals still aimed to implement the UEC as a fully supported solution across all regions. The lawyers and activists were instructing citizens how to complete an opt-out documentation and where to direct it (Yakovleva, 2014).

Eventually, even opt-out procedure failed to institutionalize and the status of the UEC became ambiguous.

After 2014, the tensions between the traditional and business models of the national identification system and the associated institutions intensified after the annexation and occupation of the Autonomous Republic of Crimea, a territory of Ukraine. Global financial institutions responded with economic sanctions. Under pressure from the United States Department of the Treasury, Visa and Master Card suspended their services for a number of Russian banks working in the Crimean Republic. As a result, the technological narrative of progress and innovation during Medvedev's presidency transformed into a politicized debate about the Cold War confrontation between the West and Russia during Putin's return to power.

7.2: The Historical Roots of the UEC Policy Failure

Chapter 4 of this dissertation interpreted the evolution of the Russian passport system as a process of reinvention and reintegration of the fundamental values of state power within political modernization. These fundamental values or ideas are Russian absolutism, Russian subjecthood, and Russian imperialism. They refer to the philosophical assumptions about power relations within society and help to interpret the enduring political goals and administrative practices of identification in different political regimes. Additionally, the persistence of these three foundational ideas helps to explain how state identification practices contributed to the social and political formation of the Russian state.

State formation and its ability to establish a sovereign power over the populated territory depends on the ability of the state bureaucracy to generate and preserve knowledge about the population under its rule (Giddens, 1986; Scott, 1999; Torpey, 1998). Torpey (2000) developed a

passport theory of state formation which emphasizes the ability of the modern state to introduce a monopoly for the legitimate means of population movement. Passport systems allowed modern nation-states to impose restrictions on population movement but also "to embrace its citizens" and to facilitate the process of their identity construction (p. 12). With a requirement to apply for and possess a legitimate passport, the modern state was able to rationalize the extraction of military service, taxes, and labour; differentiate between law-abiding citizens and suspicious foreigners; and embrace the diversity of its subjects and maintain social order based on the process of surveillance and supervision.

This theory explains the historical commitment of Russian policymakers to the internal passport system since the first legislation of 1719; however, it does not accommodate the negative results: policy failures, narrow applications, forgeries, resistance, and corruption. The developments that undermine legislative initiatives in the Russian case contrast with the state-centered passport theory with the agency-based explanations, which elevate an account of the discretionary power of Russian passport bureaucrats and police in translating and implementing state passport rules within a fragmented Russian society. Chapter 4 outlined the everyday practices of the passport regime, which either challenged the state monopoly on the freedom of movement or, more often, transformed the passport's function to exercise power and domination over Russian society. Consequently, the practical interpretation of the passport regime by local authorities and police resulted in multiple conflicting interpretations regarding the rational goals of the central authorities.

The argument is that the evolution of the passport in Russia is a process of contestation between Western modernizing logic and the realities of the absolutist state. Giddens (1986) describes an *absolutist state* as a hybrid regime that is prone to modernization but also maintains

the traditional order of the class-divided society, which is a representation of the absolute power over its subject population (p. 75). The government is such state may be developed in a modern sense, but the ruler is "a personalized expression of the secularized administrative entity" (p. 94). The sovereignty of the absolutist state has no limits and there are no boundaries but frontiers of the absolutist rule which are constantly disputed and contested (p. 89). The relevance of these characteristics in the Russian case is discussed in some Eastern European scholarship where the authors attempt to conceptualize the authoritarian, illiberal, and imperialistic practices of the Russian Federation that survive history and reinvent themselves (Oleinik, 2010; Rozov, 2012; Umland, 2012; Radu, 2008; Sanborn, 2014).

I argue that this contestation between modernization attempts and the historically illiberal nature of political power in Russia has resulted in particular state identification practices which carefully preserve Russian absolutism, Russian subjecthood, and Russian imperialism in the form of unchallenged assumptions about power relations within society. The uniqueness of the Russian passport system was shaped by the geographic position between West and East and territorial expansiveness, the center-periphery flow of absolutist power, contradictory bureaucratic implementation, the growing role of police enforcement of passport regulations, and constant attempts to colonize and civilize the "otherness" of internal subjects, both Russians and non-Russians. The most significant features of the Russian passport system include: (1) the failure to transform complex and contradictory passport rules into standardized impersonal procedures, which consequently reinforces bureaucratic arbitrariness and state absolutism; (2) the institutionalization of Russian subjecthood as a denial of political agency and personal autonomy, and the reinforcement of a paternalistic relationship between citizens and state; and

(3) as a colonizing tool, the Russian passport served Russian imperialist ambitions within the state and outside its borders.

Russian absolutism can be understood as a "power that is grounded in itself and does not flow from external sources of any kind" (Rozov, p. 43). Policies inspired or initiated by the autocrat are directed at self-reproduction, not social, economic, or political goals (Oleinik, 2010, p. 76). For example, the objectives of the first passport law in 1719 survived bureaucratic failures and inefficiencies because it was a modernizing vision of the emperor, and therefore the bureaucratic apparatus employed practices that often undermined the fundamentality of the principle of law, but seemingly supported this vision. Because they struggled with bureaucratic inefficiencies, the privileged population would petition the Tsar (or his representative) to grant resident permits in Moscow, which would be more efficient (Lonergan, 2013, p. 32). The Russian absolutist regime and its practices of passport governance "succeeded by an administrative order that rejected legality and harnessed the professional disciplines to its own repressive ends" (Engelstein, 2009, p. 20). The Soviet police used the passport system as a tool of urban cleansing and mass purges; and although their practices contradicted the Soviet Constitution, their legality was rarely contested.

The policy development of the UEC resembled the absolutist tendencies of the top-down model, orchestrated in Moscow and deployed across regions without any consideration or consultations with politicians at the regional level, or the bureaucratic institutions that had to implement it. The card was first presented by the President, the source of the power in Russia, who communicated to all of the relevant stakeholders that this objective is not subject to deliberation, and it was approved by the President. Similarly, JSC UEC was established with a presidential decree. The survival of the internal passport regime in Russia is possible due to the

unlimited absolutist power of the political center, able to justify this policy reinforcement despite conflicting policy ideas, costs, and inefficiencies, and with limited and controlled policy discussions or consultations.

I adopt historian concept of the subjecthood in Russia (Lohr, 2006), as a perspective on current practices of citizenship in the Russian Federation in the context of failed democratization and weak civil society. As historical chapter revealed, the Russians were subject to the arbitrariness of the absolutist regime and its bureaucrats during the Imperial and Soviet periods and were treated by the paternalist Russian state as lacking sense of agency. Historically, Russian policies on banned emigration and controlled movement within the state produced "a sprawling multiethnic empire, where people were relatively rightless subjects of an autocratic Tsar or Soviet leader" (Lohr, 2012, p. 3). These rightless subjects was not homogeneous; instead, passport practices carefully segregated subjects who could be close to the autocracy – nobles, state servitors, and merchants – as opposed to subjects who had to be kept at a distance – lower urban groups, peasants, and the non-Orthodox population (Steinwedel, 2001, p. 74). The Soviet passport system segregated "elements near and alien" (Shearer, 2004), and that corresponded with the loyal working class versus the suspicious anti-Soviet element that should be removed and relocated. This was the result of denial of individual autonomy and the determination of status and identity. Furthermore, subjects may lose their citizenship arbitrarily if a passport clerk decides to confiscate the passport claiming its illegality, therefore revoking citizenship (Salenko, 2012, p. 18). This dependence of citizenship rights on the passport and the information in it illustrates how the idea of subjecthood is realized through these identification practices.

Finally, the Russian military occupations of Transnistria (1994), Georgia (2008), and Ukraine (2014 and 2022), as well as the annexation of Crimea, brings our attention to the

significance of Russian imperialism and control over a territory whose population are deemed Russian subjects to Russian absolutist power. An absolutist state recreates the image of its far reaching and contestable frontiers due to its historical connection with its subjects – *"Russian Speaking," "Soviet,"* and *"Slavic Orthodox,"* population based on the "ethnicity" rubric contained in a Soviet passport (Sasse, 2007; Akturk, 2010). In the 2000s, Russian embassies and consulates were actively circulating Russian passports to Georgian and Ukrainian citizens who were born in the USSR, spoke Russian, and lived in the territories that are occupied today – a process known as "creeping annexation" through passportization (Artman, 2014; German & Karagiannis, 2018). In 2022, Vladimir Putin signed a decree offering Russian citizenship through passport application for all citizens of Ukraine. Imperialism is realized through the practice of colonialism which, in the case of Russia, is well documented within passport regulations. The history and modern practice of Russian military conquest to the West and the automatic proclamation of all individuals in the sovereign states to become Russian subjects as ordered by presidential decree provides an illustration of the unique Russian subjecthood of the autocracy, reflected in coercive administrative practices of the population movement to colonize remote geographical areas and to reward the loyal population with their desired residency (Garcelon, 2001; Lohr, 2012; Yekelchyk, 2019). Passport legislation in imperial Russia was elaborated each time the frontiers of the Empire were extended, to include new categories of the population who were not foreigners, but not Russians either.

This autocratic and coercive control over territories, resources, and population resulted in the powerful identification practices that locate and fixate subjects geographically, emphasizing their dependence on the autocrat but also prescribing their place within the Empire. The Soviet passport system has reinforced the colonizing effect of the Community Party's political

imperialism, using the nationality rubric (Hirsch, 2005). Not only was it categorizing the population according to bureaucratically prescribed nationalities, understood in a primordial way, but it also helped to organize subjecthood hierarchically based on the national privileges of access to economic resources, job opportunities, education, and political careers. Therefore, passports in Russia were not serving the universal function of segregating citizens from non-citizens; instead, it was a system that involved a complex hierarchy of different categories within the population that at the same time served as an instrument of colonial control and conquest. The Russian passport failed to function as a neutral administrative document; rather, it is a significant token supporting minimal trust for social interaction, and it provides information about the holder that allows the state, but also other organizations and individuals, to place the passport holder on the ladder of social hierarchy. Everything is important for building trust with the state: your place of birth, your stamp of permanent residence, your marital status, your conscription status, and your readiness to provide a passport for a random identity verification check.

Russian absolutism, Russian subjecthood, and Russian imperialism which structured and justified many state identification practices should be treated as useful historical ideas that contribute to political inquiry, but not as rigid explanatory concepts. Although they may lead to sweeping generalizations, when they are used attentively, they help to see the underlying logic behind returning political goals, solutions, functions, legacies, and practices. They also help one to face the reality that the Russian internal passport system, despite its repressive past and a technological future, was never subject to a wide political reform aiming to liberalize its administrative function in the Post-Soviet Russia. The passport reform of 1997 was merely focused on the contents of the passport but did not intend the relaxation of the complex residency

rules limiting freedom movement of the passport holders. It is out there as part of the unquestionable natural order of things, as a sign of privilege or a stigma of the outcast, as one of the main institutional elements of Russian identity, governmentality, bureaucracy, and police and social interactions.

7.3: Two Models of the State Identification System and Ability of the State to Control Citizens' Information

In Chapter Six I showed that technocrats were working on building horizontal connections and interoperability, and were concerned with accessing the system online and supporting access with digital identity verification. They needed the system to accommodate as many users as possible and to support integration of the different identity credentials to satisfy role-based access requirements. Technocrats also were not concerned with the revenue model as a public agency. The design of the "All-Access-One" was not limited by a particular identity card; rather, it was built as an application accepting a variety of digital credentials, as long as those credentials were verified. economic liberals were concerned with the revenue model of the UEC, and required many users to use many services, both private and public, with one card, while technocrats were focused on building horizontal connections across government silos responsible for different services and sectors, additionally improving communication between the regions. The technocrats' work on common standards, data elements, centralization of informational flows, and interoperability was critical for e-government and the consistency of electronic access to public services. Alternatively, liberals were following business standards of profitability and enforcement of banking technical standards to secure the position of only one provider/vendor. The idea of cost-cutting transferred into the practice of a double pay for the

final user. Russian taxpayers already paid for the technocrats' work and additionally banking sector would be charging their authentication services to the Russian government each time the UEC was used.

For a taxpayer, the expectation was that the service would be free, but the UEC JSC solution was linked to other hidden costs. To provide a free UEC card to a citizen, banks would sign agreements with regional governments to modernize their municipal services through digitization. Agreements were not negotiated and instead had conditions which were unfavourable to local authorities, who were told by the federal authorities that the agreements must be signed "as is." As the biggest investor in UEC JSC, SberBank would include transaction fees for the use of banking machines, and would further subcontract technological design, installation, and maintenance of the card readers in local transit, schools, and public administration buildings. Because regional government were too slow with onboarding the UEC, SberBank created more products to address the slightly different needs of the different socio-demographic groups within different public contexts. These included "*Strelka"* (trans. arrow), a reloadable bus pass for citizens without social benefits similar to the Vancouver transit card Compass. SberBank also developed a project that eventually became a subsidiary company "*Ueshka"* (trans. a diminutive of UEC). Since 2012, the company is managing school security program, where parents and school boards would cover the costs of tracking services for their children through a security gate – a tap with the Ueshka card on a gate with a security guard would record when children entered and left the school (ueshka.ru, 2022). In 2015, SberBank in cooperation with the municipal programs of school lunches implemented a biometric payment system "*Ladoshki*" (trans. a diminutive of palms). This biometric system allows children to choose lunch in a cafeteria and scan their hand to pay for it or to get authorized for a free lunch.

More than 600 schools across Russia are using this system and hundreds of thousands of children are involved. (Pozychanyuk, 2020).

With these programs, more and more public services that used to be delivered by the local government began generating profit for a third-party organization providing digital identity technology. The digitally verified identity is an extra step that in the past was either completed by the bus driver or a teacher. In addition to selling digital identity solutions, private sector is also selling the licensed software, technical infrastructure, triggering ever-lasting technological maintenance costs and vendor lock-in. So the card for citizens was funded through taxpayers dollars, which were taken from somewhere else. Local governments were trying to manage those additional costs by increasing public transit fees or requiring parents to sign agreements with the organizations that provide and maintain school security gates, which resulted in creation of a whole new industry.

An expansion of third parties serving the new business model also contributed to erosion of government control over public information, including the protection of personal information. Every time the card is used, a record is created. Many records can be analyzed to determine trends, patterns or to track a particular individual. This information can be used for the public good, to inform new evidence-based policies, identify fraud, and misuse of public money. But because this data is a shared responsibility of all the parties involved, the ability of the government and public organizations to maintain data under applicable regulations and legislation is challenged by the contract with the service provider. In the past, the educational bodies were in a full control of the information about attending children. Teachers were responsible for tracking attendance and progress of students and the school's administration managed the cafeteria. With the new system, these records are duplicated by the security gates

and biometric readers, and the data is extracted and shared with bodies responsible for education and subsidized lunches, as well as with the private sector organizations interested in school analytics, as collection, use and disclosure of personal information is based on the recorded consent of the parent. Again, there may now be better control over the financial spending and effectiveness of a school's administration through transparency. But there is also a trend to privatize and monetize this information by the company providing the services.

Another problem with eID is that its application is limited to a highly dense urban population. The success of this oligopoly on the means of identification depends on all issued cards actually being used for their intended purposes. The assumption was that if millions of Russians would use the UEC several times a day, the project would not only be self-sustainable, but will save public money and generate financial return on investments for participating banks (Gref, 2011). The problem is that outside of the rich urban centers, Russian government services do not exist in everyday life. There are remote places with no public transportation, small schools, small hospitals, or no hospitals. Many Russians only need to interact with government institutions occasionally. Which is also true in many other countries. While people do use banking payment cards almost every day, the assumption that this logic may be expended to improve the exchange of information between citizens and government institutions is not well founded. The offer technically only worked for big cities with a healthy economy, but this "all in one" model of eID required not only that the card is issued, but that complex infrastructure supporting the card is built and maintained. It turned out to be very physical – if a card is needed to open a gate, we must create a gate in places where digital transactions are not an everyday practice. So instead of facilitating an open and transparent relationship between the individual and e-government based on public trust, eIDs, in a sense, created a feeling of a gated community

built on zero-trust security approach. Zero-trust is a cybersecurity model which means that internet systems must suspect every visitor and every online request as a potential malicious actor until their identity is verified and confirmed (Campbell, 2020). Trust but verify (trans. *doveriai no proveriai*) is also a popular Russian proverb.

Medvedev failed to recognize the contradiction between the traditional goal of regulating movement within the state, and the modern goal of making life easier for the card holder as seen by the private sector. The traditional model was managed by law enforcement. The business model was managed by economic liberals, bankers and entrepreneurs, concerned with profits and interested in monopolistic solutions where each use of the card generates a small fee, similar to Visa and MasterCard. This cost-recovery model is not uniquely Russian. One may speculate that when the siloviki realized that they would have to pay SberBank a small fee every time the UEC cardholder wanted to use the card to update registration address, the perspective on the innovation changed. Eventually, the siloviki strongly advocated against any payment function within the e-passport developed in 2017, to limit interconnectedness of the card and its dependency on private sector and associated financial costs.

The business model of an oligopoly on the means of identification generated concerns among technocrats as well. Technocrats were focused on the centralization of information flows through state hierarchical control of resource distribution from center to periphery. It was promised that the UEC would provide opportunities for regions to get new funds from the Federal government for IM/IT improvements to enable new connections between information systems, and reduce duplication of records across different systems. However, the technocrats communicated that instead of waiting for the UEC to be fully implemented, they needed some substitutions to manage the new digital access points to government services and associated

systems, which can be changed in the future when the eID is ready. Their approach was based on the idea of accepted digital credentials with the most practical currently available solution that is flexible, scalable, and adoptable – open-source identity management tools. Instead of manufacturing and managing the electronic identity card, they chose the path of mobile IDs where the identity of individual is verified and linked to their email and mobile phone number, and digital access points are built using multi-factor authentication. The idea is that all approved methods of authentication can be supported; in a way technocrats were aiming at creating a system that is technology agnostic. Meaning it would support different technologies and providers of digital credentials, for example supporting access through mobile phone, email or personal insurance number (SNILS). This model was also supported by the Ministry of Internal Affairs, as they maintained their role in identity verification and were an authoritative source of the verified identity in this model.

Both had different goals: technocrats were ensuring government systems interoperability and improving information technology networks connecting central government and regional authorities, including secure online verification with minimal acceptable standards for verified digital identities, while economic liberals were focused on the card's potential to generate profit. The ability of the UEC to generate profit was linked to the availability of services requiring a swipe of the card to record a transaction. Therefore, the UEC became a physical token that could be tapped or scanned at the point of entry, a bus, a school security gate, a cafeteria. It also needs to be readable, meaning machinery is required to read it and provide access. The "all access one" model of the electronic identity management system, developed by technocrats, was reducing the requirement for face-to-face interactions, and digitizing exchange of credentials through the individual's mobile phone, which is regularly updated and maintained by the owner. Maintaining

security of the digital authentication was a shared responsibility between mobile phone owners, internet providers, identity authorities, and the Ministry of Telecommunication. The "all in one" Universal Electronic Card, instead of reducing *face-to-face* interactions between citizens and government through online services created new multiple points of physical contacts with the *card-to-machine* interactions for services that naturally can be out-sourced and often do not require a high level of identity assurance. In other words, verification of the government issued ID to facilitate access to some public services is not normally required. For example, we do not have to prove our identity with a very high level of identity assurance (i.e., a national ID with photo) to ride a bus, visit a doctor, enter a school, or purchase a government-subsidized school lunch. The tension between "all-in one" and "all-access-one" approaches to digital identity architecture within the oligopoly of identification model really placed the practicality and revenue model of the UEC under the scrutiny of multiple stakeholders at the federal and regional levels. The compromise was to allow SberBank to sell their "all-in-one" UEC to the people first and later to integrate a tested tool within the new IT system built by technocrats. The flexibility of the "all-access-one" electronic identity management system allowed technocrats to search for alternatives that are more cost-efficient, and allowed government to implement immediate technical solutions while keeping costs of technological maintenance under control.

However, in the long run, this solution did not satisfy siloviki, who recognized a challenge to their institutionalized power over population movement control, and their legacy as an authoritative source of citizens identity. While siloviki are present in many government and public bodies, and some private corporations, they would not tolerate interoperability of the national security systems with others, as it would mean more transparency of their operations. They did not like the idea of a technocratic Ministry gaining power, because it is already

responsible for cybersecurity and regulating traffic on the Russian internet. Publicly, however, they were advocating for a secure Russian solution to the e-passport, meaning Russian technology, Russian software, and Russian hardware. This approach was labelled as *technological sovereignty*, meaning absolute independence from the global technological companies and standards (Andreieva, 2014; Faltsman, 2018). However, the success of the systems built by technocrats was possible because of access to the globalized network, and shared knowledge of the open-source contributors from around the world, like OpenID protocols which support secure online verification. Technocrats were able to bypass strict government security reviews by building a minimal viable product with the least cost, re-using software code from global shared libraries instead of building code from scratch, and handling security risks proportionally to the type of information involved. Technocrats endorsed opportunities provided through the globalization of technologies and standards, while the siloviki perceived globalization as limiting and undermining sovereignty of the Russian state. The inability to reconcile those different perspectives and opportunities undermined the implementation of the UEC.

The idea of an electronic identity card was interpreted through two conflicting models proposed by different policy communities. First, the business model is an oligopoly on the means of identification, inspired by Western ideas regarding digitization of government and optimization of identity management. This model was partially supported by technocrats who hoped to develop a new sector and inspire technological development in the Russian government. It was also reflected in the organizational structure of the UEC Cart Cartel, involving UEC JSC, SberBank and technological standards of the payment card and microchip industries. The other model is concerned with the institutional survival of the Russian state in a

globalized world. The community of siloviki strongly advocated for a state monopoly on the means of identification, while concerned with the issues of legitimacy and national security of the UEC. When the state collects information, it must be limited to the legitimate purposes of the state, it must be managed responsibly, and responsibility for a failed security must be enforced. The state must legislate authorized and lawful collection, use and disclosure of personal information to establish and verify individual identity, supported by security controls which are regularly applied to the government's information systems and databases. These are universal principles that enable the state to effectively rule in the new identification regime. All citizens are accounted for, and appropriately treated within the state machine: paying taxes and other dues, having access to services, and receiving state assistance. In the case of the Russian Universal Card, the state role in documenting its citizens has weakened and the monopoly of SberBank has strengthened at the same time undermining legitimacy of the state identification system. SberBank could collect information about UEC cardholders and maintain full control and ownership of citizens' personal information, preserving the right to extract any additional value from collected data and analysis.

7.4: The Problem of Ownership, Control, and Security of Personal Information

One of the unintended outcomes of the contestation between the two models was issues with control and security of personal information. This problem was not informed by the Western liberal perspective of privacy as a human right, where the use of collected information is limited by the legitimate purpose and controlled by the individual. It was not defined as freedom from extensive surveillance by government. In Western jurisdictions, privacy legislation is more

about empowering individuals or bringing back the balance of power between bureaucracy and individual through protection of informational rights and freedoms.

In Russia, the evolution of privacy legislation is more linked with legislation surrounding confidential government information. Privacy legislation needs to have special regulations and exemptions. It works alongside information security legislation and defines the institutions and departments responsible for information security. Information security capitalizes on the ideas of Russian versus foreign ownership, government versus private control, and custody of personal information of Russian citizens. The Russian view on privacy is reflected within a general legislative framework that is concerned with the security of any information within the Russian state. It stems from the legacy of Soviet information policies that were concerned with state censorship, and managed by the Ministry of Communications (1994 - 2004), which was also responsible for managing communication. Therefore, it upholds the existing regime by controlling information messages and flows, similar to the Ministry of Truth in George Orwell's classic 1984 (Orwell, 1949). Today, it is the Ministry of Digital Development, Communications and Mass Media of the Russian Federation. One of the agencies, Roskomnadzor, conducts internet and mass media surveillance but also enforces Personal Data Law (nr. 152-FZ, 2006). The Russian state protects the privacy of its citizens based on the principles of paternalism – i.e., the state knows what is best for Russians. The Roskomnadzor carefully separates radical and hateful content that incites violence and undermines order from communication channels through internet censorship based on the "all-encompassing paranoia" (Soldatov, 2016). It also conducts regular audits and reserves the right of access to servers of any technological company operating in a Russian territory and even issue a ban to operate in Russia as in the case of the LinkedIn (Rumyantsev, 2017), to protect the personal data of Russians from big corporations (Vasil'ieva

& Medvedev, 2017). The privacy of Russians is protected, just as Russian language, culture, and moral traditions from the interference of the Western world. It is not a liberal model of privacy, but rather a paternalistic model of privacy, similar to how parents protect the privacy of their children through control and surveillance, sometimes using modern solutions like a GPS tag or mobile phone spyware.

Russian subjecthood and absolutism shapes governmental practices of privacy protection in Russia. Privacy protection can be grounds for law enforcement to enter the internet provider's buildings and explore their servers to confirm that data is protected. It is also a tool of political manipulation, for example, to fine Google and Microsoft for refusing to store Russian data on Russian servers and maintaining the backdoor for law-enforcement access (Shvets, 2019). The Russian Federation also implemented the "right to be forgotten" legislation, which allows Russians to demand removal of a search engine's links to personal information deemed irrelevant or inadequate (Federal Law nr. 264 -FZ, 2015). The initiative was framed as a harmonization of Russian legislation with the EU General Data Protection Regulation (GDPR). In practice, it became an additional censorship tool that allows high ranking politicians to request the removal of information from the internet that they consider an invasion of privacy or that may damage their reputation, like corruption scandals. Russian government rewards political loyalty with limited public scrutiny. Paradoxically, the general population have less privacy and may be subject to criminal prosecution for what they post online. The political question is about who gets what in Russian society. Politicians and well-established private sector players enjoy the right to be forgotten, and usually do not need an electronic identity card to access social services.

Another problem is personal information ownership. Once it is collected by technology providers and possibly processed by a third-party, the responsibility for the protection of this information becomes shared. These are very important questions that concern not only the Russian government, and not only because of national security. They bring up the importance of data sovereignty as a principle that all data collected from the users of the system is subject to the laws and governance structures within the sovereign territory it is collected from (Vaile, 2014). This principle was formulated in response to Edward Snowden's public disclosure of the NSA files (2013), bringing to light the illegal spying on Russian citizens by US law enforcement through American telecommunication companies operating globally, such as Microsoft, Apple, and Google (Baezner & Robin, 2018). Today, partially due to the impact of GDPR and partially due to government security requirements to keep government information within the jurisdiction of its legislative control, this principle is the guiding architectural principle of cloud-based services and platforms (e.g., Government of Canada Cloud Adoption Strategy, 2020). The Russian government capitalized on the Snowden story strategically, providing him with a political asylum and blaming US and its technological companies for benefiting from the global internet market and from Russian people and resources. The Russian data sovereignty discussions about taking back control and ownership of personal information collected and monetized by American capitalism does have a popular support. This support was reflected in the active mobilization against the UEC project, and in the policy justifications of technological sovereignty as a main principle for modernization of the Russian state identification system. The state monopoly on the means of identification employs this technological sovereignty in the latest design of the e-passport (Figure 4).

Russian surveillance, when based on technological sovereignty, is acceptable and supported because it is paternalistic state surveillance, a panoptic model. The policy community of conservatives/traditionalists embraces paternalistic state surveillance as an important mechanism that keeps the social fabric of Russian society managed appropriately given Russia's unique geography, history and culture. The localization of the population, according to their historical and ethnographical roots, is seen as one of the positive outcomes of the Soviet passport. Benefits of the electronic card are available only to those to can prove their historical attachment to the locality. Moreover, Russian subjecthood reinforces the idea that the personal information of Russians is owned and controlled by the paternalistic state to maintain existing order and prevent popular dissent and violence. Subjects cannot control information about themselves as they have no sense of agency, but the state uses the same logic to ensure that subjects do not have any determination regarding use of their information. Personal information of Russian citizens is under the ownership of the Russian absolutist state. This practice is ironically concerned with the privacy laws and regulations just as additional tools to isolate, control and manipulate flows of information for the purpose of preserving the absolutist power of the political regime.

7.5: Conclusion

Some could argue that the Russian Universal Electronic Card failed due to the corruption or inefficiency of the Russian administration, or limited resources coupled with the immense geographical area with populational gaps across larger areas. This case-study highlights the significance of other factors.

First, the UEC's revenue model was an economic failure. SberBank could not integrate the business plan model that would generate profit. There was an assumption that people would use a multifunctional card more regularly and that each transaction would be commissioned. In addition, data would be extracted and monetized. However, in practice what seemed to work in Moscow could hardly be implemented in other regions with smaller economies, smaller regional budgets, and smaller populations. Parties involved in the UEC card cartel started questioning their return on investment. Regional authorities voiced disagreement with the payment schedule and growing fees for services that could not be implemented, due to the lack of technological infrastructure within their administration. Additionally, individuals on social assistance and retirees were regularly losing cards and forgetting passwords. The amount of technical and client support required for users became an unexpected new cost that could not be shared with the local administration, and instead was delegated to the staff at SberBank branches. The failure of the business model and the overarching theme of e-government not only did not improve efficiency but also could not cover its operational costs. However, the system's proponents have argued that transparency of public spending has increased in education and healthcare, as card users were generating more accurate and verified data than ever was available in the past.

Second, there were political reasons behind the failure. Stakeholders within interpretive communities were lacking a shared and common vision of the final policy outcome. Each stakeholder quickly decided to work on their own project. SberBank and UEC JSC started issuing cards in the regions and signing cost-recovery agreements with selected regional authorities. Regional authorities were hoping that when the project was federalized, they would stop paying for the services and would qualify for additional federal funding for the technical modernization of their administration. Moreover, the siloviki community were concerned with

national security and would halt all developments that did not use technology made exclusively by Russian companies for the Russian government. Technocrats adopted open-source standards and ready-to-use solutions, and created a system that worked without an electronic card and could be accessed in several ways, including through email, phone, and other acceptable verified credentials.

The third reason was Russian data sovereignty. The proposed oligopoly on the means of identification turned out to be incompatible with the idea of Russian data sovereignty and its attempt to control personal information, with the overarching goal of censorship. The idea of the UEC JSC to govern multiple bodies, some of which are subject to international agreements and technology standards, was not consistent with the idea of technological sovereignty. Moreover, the federal government feared the cybersecurity issues associated with the centralization of the interoperable systems across state levels and private banks.

However, the idea of data sovereignty should not be viewed only through the lens of non-democratic states attempting to control the online behaviour of their subjects, as is the case in Russia or China. It is relevant for international relations in today's interconnected world. The question of who owns personal information could become increasingly important in the international trade of that information. More nation-states could articulate the issue of sovereign control over citizen information collected by the growing oligopoly of technological giants who offer accessible digital solutions under inflexible terms of use and privacy policies.

Chapter 8: Lessons from the Russian Universal Electronic Card Case Study

What lessons can one draw from this case study of the Russian UEC? In Chapter 2, I classified research on electronic identity cards under three perspectives: (1) an instrumentalist perspective, concerned with electronic identity cards as tools of e-government reforms; (2) a political perspective emphasising the importance of policy drivers and justifications for the implementation of the eID depending on different factors; (3) a critical surveillance studies perspective, concerned with the power of eID technology to facilitate state surveillance and lead to social sorting and discrimination.

All three perspectives have directed my enquiry, informed my analysis of the primary sources, and helped me interpret my observations. My findings allowed me to determine the applicability of various academic findings and theories on the subject. Which observations and statements in this literature were confirmed, which were not? What elements of the UEC case study were not satisfactorily explained by this literature?

8.1: Lessons for the Instrumentalist Perspective

E-government is certainly a powerful concept that goes beyond its research application, as it has a promise and a prescription for positive change. This promise is conceptualized through seeing technology as an instrument of progress that can improve the problematic functioning of old institutions. It is prescriptive, as use of each instrument (e.g. a new software, application, cloud platform, or electronic identity card with a card reader) is accompanied by measurable criteria or key performance indicators for any type of organization within any political context. Technological investments in public administration in advanced democracies are supposed to lead to more efficient management of public funds, while in developing democracies, they are

also supposed to improve transparency, accountability, and trust in government. Research is concerned with the factors that undermine or facilitate the positive outcomes of e-government.

Some Russian researchers on e-government employ a critical view on the concept as an abstract ideological Western construct that promotes the standardization of the public sector across different countries, for better control and predictability of government bureaucracies, but also for market expansion for products and consulting services supporting e-government projects. These ideas were also consistent with concerns about the Universal Electronic Card being a tool for expanding the influence of the Western hegemony, expressed by conservatives and traditionalists.

The e-government literature, through its focus on standards and unified solutions, tends to overlook the significance of the socio-economic, political, and cultural differences between states. An electronic ID is a tool for identity verification supporting the delivery of e-government, helping to standardize government services and change the ways citizens are verified remotely. The findings in this literature also support the argument about expansion of technological security standards and protocols into regulated policy processes, which challenges the idea that the state is the only agency to verify the identity of its citizens. It technically argues for the diminution of the state apparatus through the automation and digitalization of state services.

Despite instrumentalist claims about the ability of eID to enhance security of e-government services, the issue of uncertainty in the security of remote identity information management was not resolved by the UEC in the Russian Federation. On the contrary, developed solutions highlighted security concerns and introduced costly cybersecurity controls, previously managed by the traditional means of “in-person” verification by street level bureaucrats. Instead

of building trust through online accessibility, digital services in certain cases have tended to undermine the trust built through human cooperation and assistance. In the case of the Russian Federation, conservatives and traditionalists were advocating for the rights of marginalized groups and religious minorities who need assistance with technology and with understanding complex government procedures through "face-to-face" interactions with public officials. They would argue that in order to build trust, government should be represented by people, who can be contacted in person and available to provide assistance in traditional ways. Another problem with cybersecurity was linked to the global standardization of electronic identity cards and e-authentication methods. Standard solutions across different countries could have similar security vulnerabilities which could be exploited by hackers. The Russian government hopes to develop sovereign technology according to Russian standards and in the interest of the Russian government and people, protecting them from foreign hackers, including state sponsored hackers.

At the same time, the Russian government was still not quite sure how to achieve the highest level of identity assurance with the electronic identity card without an individually configured card reader – an additional and costly device connected to a personal computer that would provide an encryption key to protect the information involved in transactions with the electronic identity card. The complexity and cost of this technology has become a real constraint, preventing cards from becoming a reality in many jurisdictions. This is evident not only in Russia, but also in Canada and other countries where e-government is now going through a rebranding as digital modernization to deal with the shortcomings of electronic government reforms (Digital Nations Charter, 2021). The digital modernization of government operations only intensifies the problems of legitimacy, and the misalignment of traditional identification

systems and processes supported by legislation. Legitimacy is a real problem to the extent that governments often establish unique digital authorities which are not very well integrated into existing hierarchies and mandates, and are tasked with achieving such alignment. The government builds new structures responsible for digital innovation that duplicate traditional functions without focusing on the issue – whose mandate and responsibility should it be to design and build secure and compliant information management and technology solutions? And, most importantly, who will be accountable and responsible for the increased security risks and who will be enforcing security regulations in shared public-private partnerships?

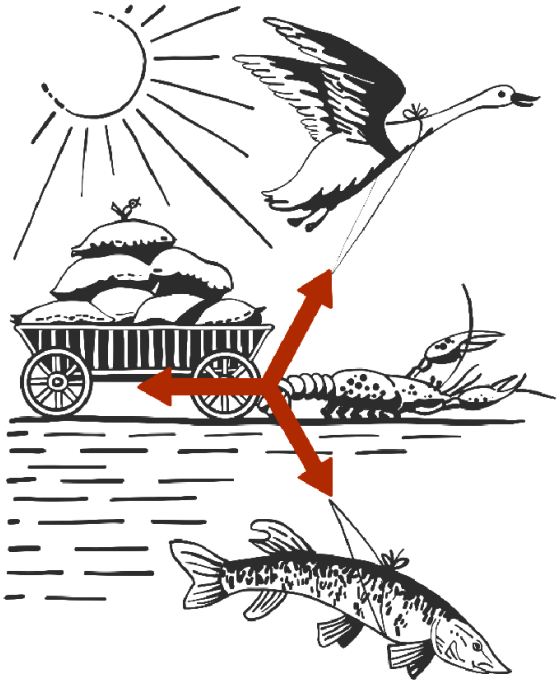
From the instrumentalist perspective, the lack of the instrument, or the digital tool, is always a problem and self-justifiable investment. With the assumption that technological modernization can eliminate manual processes within siloed departments, instrumentalists overlooked the sources of state identification systems problems, institutional legacies, outdated policy and regulatory frameworks defining those departments and requiring political reforms. Similarly, in the Russian case, instead of reviewing and modernizing legislation on internal passports, a Soviet legacy, which would require serious political upgrade of the Ministry of Internal Affairs, the government, through a presidential degree created a public-private partnership UEC JSC, empowering SberBank to design and deliver technology available as a cost-recovery model to regional authorities and promising to modernize government bureaucracies across the Russian Federation without federal funding. The Government provided nothing but a promise to UE CJSC to substitute the internal passport with the Universal Electronic Card as soon as pilots in the regions were be completed and use of the UEC was be popularized.

8.2: Lessons for the Political Perspective

The problematic assumption in this literature is the view that the state bureaucratic apparatus is a homogenous and stable structure which is, depending on its structural configurations, hierarchically organized or horizontally interconnected and will shape the justifications and directions for technological innovation in citizen identification. The state is seen here as a machine, where each structural part has its function, supported by tools and institutionalized practices, and they all together act in accordance with the legislative framework, policies, and procedures authorizing and prescribing their functionality over particular jurisdictions. As such, the state proceeds with implementing electronic identity cards supported and shaped by this existing structure. This literature accounts for the interests of political groups, the public, the lobbying from technology firms, and influence of the international technological standards that will shape the outcomes of the electronic identity card innovation. But these groups are external to the state and their impact may or may not influence political leadership, who, in turn, will adjust the implementation process through communication to public servants. The state machine will work on adjustments through its structures, mandates, processes, and people.

Observing the implementation of the Russian Universal Electronic Card, the importance of key stakeholders, their institutionalized beliefs, and their interpretive communities is revealed, no matter their position within or outside the state bureaucracy. These communities interpret the state functions in their everyday actions and long-term projects. They compete for the expansion of their mandates and operational funding, and they not only define their own structural positions within the state but also do everything possible to make it the most important part and to define and control integration with other parts. So instead of the established Western metaphor of

bureaucracy as a structured iron cage of rationality, a metaphor described by Ivan Krylov (1814) in his Russian fable “The Swan, the Pike, and the Crawfish” would better describe how the Russian state implements technological innovation. Each animal pulls/pushes the wagon in a different direction (up, backward, down) and therefore cannot move the wagon.



Source: Schwartz-Ziv & Volkova, 2021

Figure 7 The Swan, the Pike, and the Crawfish, as a metaphor describing state politics of the Russian UEC.

Similarly, in this case study, I hypothesize that diversity within the state functions as a source of conflicting drivers because technological innovation is being interpreted by ministries and departments through their own perspectives on their mandates and functions, including institutionalized practices, and policy myths and ideas. The Swan would represent the economic liberals and technocrats, flying off with the multifunctional Universal Electronic Identity Card, with the vision to replace all the government-issued documents and identity verification processes from the past with one card funded by the banking sector, relying on the market-based

revenue model and linking personal finances to taxation, public obligations, and social assistance.

The Pike is the siloviki, pulling the electronic identity card idea into the dark waters of secrecy and national security governed by the Ministry of Internal Affairs, and developing an alternative solution, an electronic passport that would substitute the paper-based internal passport of the citizen of the Russian Federation and could only be used for identity verification and regulation of movement within the country. The goal for the modernized electronic passport is the security of Russian society, as it fits the mandate of the Ministry of Internal Affairs. Their idea of an electronic identity document is a tool that is integrated with the existing state identification system. Its functionality is limited to identity verification, it is fully manufactured in Russia, including the card's microchip, cryptography, and the software supporting integrated databases, and is not funded by the private sector, which limits dependency on Western technology and standards, and protects the Russian state from international influence.

Finally, the conservatives/traditionalists take the idea of international influence and inflate it into a Western technological conspiracy. Just like the Crawfish, they back away from the whole idea of technological innovation as a Western surveillance project, an attempt to connect to each individual Russian through an electronic identity card and to track every single move and decision with the purpose of controlling and manipulating the Russian territory, its people, and its rich natural resources.

The political perspective of the electronic identity card was instrumental in identifying those different forces pushing and pulling the Universal Electronic Card in different directions, reflective of their own interests. What was missing are the interests of those responsible for the security of government information and accountability of government spending. Those

communities can be quite powerful in pulling back and slowing down technological innovation simply by following approved government standards. They are the counterforces existing within the state itself. Government audits, security reviews, privacy compliance reviews, and the general structure of departmentalism and function-based separation of information flows, concerns with information classification and security risks, along with ever growing dependency on expensive technological vendors and contractors, all constitute an internal source of state resistance.

The case of the Moscow Social Card and the Universal Electronic Card implemented through public-private partnerships between government and the banking sector provided a good illustration of the card cartel theory (Bennett & Lyon, 2008). However, their limited application within big cities and even the failure at the Federal level brings up the importance of the state identification system's mandate and legitimacy. It is not only political opposition or popular movements that exhibit resistance to the electronic identity cards, but also government institutions that resist particular solutions. In the Russian case, public policy reform is not openly debated transparently through democratic institutions but rather talked through by the representatives of the different departments and Ministries depending on their mandates and relationships with the wider political forces.

There is a hypothesis that stronger states with well institutionalized vertical decision-making hierarchies are more likely to implement electronic identity cards. In such states, technological innovation is embraced as part of the digital revolution, and a significant role is dedicated to technocrats. Technocrats make decisions about particular technological solutions based on their assessment of the appropriateness of a particular solution. These decisions do not always result from a wholesome understanding of the legislative and constitutional framework

that defines business processes in the government. In the Russian case, the source of legitimacy for the state identification system was historically closely related to the state sovereignty, and the ability of the Russian state to ensure governance of its immense territory and population movement. The state identification system became a practice of sovereignty and security of the state. Therefore, legitimate authority to modernize the state identification system lies within the mandate of the Ministry of Internal Affairs, which successfully survived the communist revolution, Stalinist passport reforms, and post-Soviet liberalization, and continues to govern identification practices to protect Russian sovereignty. This legacy was not to be challenged and modernized with the electronic identity card through public-private partnerships. Instead, economic liberals and technocrats designed a parallel solution that can pay for itself and will meet the everyday needs of citizens as much as possible. In their view, state identification for the purpose of regulating the movement of Russians (an internal passport) is not important and somewhat archaic.

8.3: Lessons for the Critical Surveillance Studies

One of the surprising discoveries of this case study was the documented awareness of surveillance studies, expressed and internalized by the interpretive community of conservatives and traditionalists. I did not find translated original sources or even references to them, but it was obvious that the Western scholarship developed in response to the Snowden revelations, studies that critically assessed the growing role of technology in society and its ability to establish new ways of surveillance and proliferate social sorting, was influential in Russia.

Moreover, I would hypothesize that surveillance studies were carefully read and interpreted by policy analysts within the Ministry of Internal Affairs, and messages were adopted

and distributed through various channels to be communicated to the public. In their opinion, there is concern with the power of global technology companies to collect and retain information about any internet user in the world. And an even bigger concern is that the biggest companies are American, and they were providing all their intelligence to American law-enforcement and security agencies as revealed by Snowden (Lyon, 2015). This functionality is exactly what the Russian government needed, according to the siloviki, but could not achieve. This is exactly why the siloviki were pushing hard against the Universal Electronic Card, with the American microchip and payment system managed by the Russian banks, who are concerned with their international rankings and alignment with international standards of financial transactions. The problem was with their dependency on globalized high-tech corporations and American technology controlled by American governments. This interpretation of the potential dangers of technology as a lack of control over the information being collected, processed, and shared, sometimes without knowledge of the information owner, was critical for the Russian government to understand and act upon. However, another interpretation of the surveillance research supported by the siloviki is the belief in great opportunities provided by the technology of the electronic identity card to monitor every movement of every citizen through a perfectly designed machinery of surveillance. However, the system must be 100% under the control of the Russian state, meaning funded by the state, produced under the strict control of the state, and guarded against international cybersecurity attacks.

While surveillance studies provide important analysis of the negative and unintended consequences of electronic identity cards for society and human rights, they are also plagued by the foundationalist position, which tends to see the technology as a perfect machine, an absolute evil, the result of capitalism with the unlimited potential not only to collect and process

information about technology users, but to also monetize it through unlimited sharing and uses for secondary purposes. Economic liberals developed their revenue model for the Universal Electronic Card based on the assumption that every single usage of the card would generate profit, leading to massive databases with electronic trails which can be monetized, exchanged, and generate new data uses. But even in their most active years of their operation, SberBank and UEC JSC were still reporting financial losses. Technology is managed and operated by humans within the complex context of the power relationship and pressures, which are influenced by society, culture, and politics. The tool should fit the purpose. The latest technological innovations may seem progressive but not appropriate, neither through a cost-benefit analysis, a policy analysis, or through security and privacy compliance assessments. And these realities are as true in Russia as they are everywhere else.

8.4: The technological innovation of the state identification systems: case study contribution to the theory-building.

This case study was designed as a theory-confirming case study (Lijphart, 1971). I was applying three theoretical frameworks and propositions developed from the research on the electronic identity cards implementation in different jurisdictions and by different disciplines to the single case of the Russian UEC. Such design was instrumental for identification of the interactions between the external, or global ideas and influences, and internal or institutionalized practices and expectations regarding the possibilities for the modernized state identification system. The case is overall confirming the propositions of the global expansion of the eID as an instrument to modernize public administrations, often delivered as public-private partnerships and under the strong influence of the technological industries. However, the hypothesis that a

strong state with the hierarchical structural configuration and institutionalized state identification practices will be more likely implementing a comprehensive national electronic identity card is not confirmed by my study. The failure of the strong, hierarchically organized Russian state to implement an electronic identity card based on the existing and normalized practices of the national passport system, provides sufficient evidence for this case study to become a theory-confirming (Lijphart, 1971), while identifying some gaps in existing propositions as discussed in the lessons above.

However, my study suggests the heuristic identification of new variables and hypothesis through the study of the failure of the UEC project. In the case of the Russian Federation, I reveal the conflicting relationship between the globalized technology and the state itself. Interconnected and subject to global markets and cross-border flows of information and data, the existing smart card technology created challenges to data sovereignty, under which states are struggling to keep data collected from their citizens subject to the laws and regulations and within their territory. This conflict is strong enough due to the contested approaches to data ownership, control and data sovereignty. Eventually, in the Russian case it undermines the policy innovation because it failed to be confirming to the extended government control when the Russian government violated the international order by invading neighboring Ukraine. In response to the international sanctions in the microchips industry and finance, the government attempted to increase its control, including nationalizing design and production of the relevant hardware and software, technological support, security, and technological standards. This national uniqueness of the requirements for a government-based innovation is captured within a concept of the Russian “technological sovereignty” (Medvedev, 2022).

Therefore, this case study also serves as a heuristic case study (Eckstein, 2000). The most important contribution of which is a discovery of new variables, such as traditional view of the Russian state on what it means to govern over its territory and population, including outside of the internationally recognized borders of the Russian Federation, as well as a deep political disagreement with the established global flow of data and role of the technological industries in regulating those flows. The Russian case of the UEC failure reveals that the globalized and interconnected technology can be perceived by the policy makers as external challenges to the state sovereignty and its ability to control information collected from its citizens. Control, as understood by the Russian state, is an ability to reinforce its law, governing legislation, and identification practices over the population, often in paternalistic ways. In terms of the relationship to the theory-building, the heuristic case study allows me to recognize generalizable patterns through observation of the UEC failure, the patterns that were not identified previously and therefore valuable for future studies.

This case study provides persuasive evidence of the conflict between two models: the oligopoly on the means of identification and the state monopoly on the means of identification described in Chapter 7. These models align with the two types of digital identity management solutions: federated digital identity management and centralized digital identity management (Laurent & Bouzefrane, 2015). They are technical solutions for organizations with different types of corporate governance and associated assumptions about trust and control concerning online interactions. The first solution is appropriate for a more interlinked and cooperating governance system with less control and higher trust in third parties (p. 51). The second solution is a centralized digital identity management system (p. 34), fitting stricter security requirements

and designed to minimize high costs of transactions in terms of the risks, therefore more appropriate for a risk-averse organization.

Oligopoly on the means of identification	State monopoly on the means of identification
Universal Electronic Card	Electronic passport
Public-Private initiative	Federal initiative
Convenience	Security
Banking industry	State owned enterprises
E-government, transparency and accountability	Data sovereignty
Technology vs bureaucracy	Sovereignty vs globalization
Monetization of personal information based on consent	Control of personal information of Russians
Federated digital identity management	Centralized digital identity management

Figure 8 Modernizing Russian state identification system: two policy models - two technological solutions

The theoretical proposition would be concerned with the policy communities' perception of the relations between risks and trust and their assumptions about necessarily controls to keep those relations balanced when implementing electronic identity cards. This perception is defined by the institutionalized state identification practices and individual judgement of the appropriate technological solution or administrative treatment under the specific circumstances. Such individual judgement of decision makers is shaped by the organizational culture and societal norms and expectations. While it is true that in democratic and non-democratic states, public officials would have different perception of the relations between risks and trust when it comes to citizens identification and verification of their identity. It is also true that within democratic states, certain ministries and departments develop a more suspicious view on citizens due to their institutionalized practices of interactions with certain social groups. Such proposition would

explain similarities in the use of the electronic identity cards for providing more accountable services to citizens on welfare benefits across different political regimes (Australian welfare Card or Moscow Social Card). The decision about use of technology to manage risks and trust is often governed by the exercise of discretion in administrative decision-making, that in turn is shaped by organizational culture and political influences of the policy communities.

Economic and business policy communities are viewing electronic identity cards as a convenient technological solution that would further facilitate verified interactions between trusted members of the society not associated with the risks. Policy communities supporting such interactions would rely more often on organizations outside of the government to provide trusted identity credentials to verify individuals, together forming a federated digital identity solution. Alternatively, the law-enforcement and social services policy communities would view electronic identity cards as a security enhancement addressing potential risks of the transactions within the context of the risk-averse environment. The perception, of who deserves the trust and who is associated with the risks, seems to be crucial in policy justifications for the implementation of the digital identity management. Such perception reflects institutionalized practices, historical legacies, and political struggles.

The case of the rise and fall of the Russian Universal Electronic Card examines two models of the state identification system, shaped by the complex relations and power struggles between different perceptions of the citizens' identities that can be either trusted or cautiously documented and controlled, depending on the perceived risks for the state and the society. Proponents of each model were engaged in implementation of the identity card based on the practical limitations and appropriateness of technological solution to the environment within which they were operating. Both models were aiming to create the national electronic identity

cards, while the first one was decentralized and outsourced, relying on shared public-private responsibility in terms of technical maintenance, control and data ownership. The second model was overly centralized, unreasonably costly and empowering one law-enforcement agency without significant benefits to the other levels of government.

Bibliography

About, I., Lonergan, G., & Brown, J. (Eds.). (2013). *Identification and registration practices in transnational perspective. people, papers and practices*. Palgrave.

Aburamoto, M. (2010). Who Takes Care of the Residents? United Russia and the Regions Facing the Monetization of L'goty. *Acta Slavica Iaponica*, (28), 101-115.

Abraham, S. (2020). Building trust: Lessons from Canada's approach to digital identity.

Ahn, J., & Bretschneider, S. (2011). Politics of E-Government: E-Government and the Political Control of Bureaucracy. *Public Administration Review*, 71(3), 414–424.

Ahram, A. I., & Goode, J. P. (2016). Researching authoritarianism in the discipline of democracy. *Social Science Quarterly*, *97*(4), 834-849.

Akturk, S. (2010). Passport identification and nation-building in Post-Soviet Russia. *Post-Soviet Affairs*, *26*(4), 314-341.

Alexopoulos, G. (2003). *Stalin's Outcasts: Aliens, Citizens, and the Soviet State.* Cornell University Press.

Laruelle, M. (2016). The Izborsky Club, or the new conservative avant-garde in Russia. The Russian Review, 75(4), 626-644.

Rhodes, R. A. (1997). Understanding governance: Policy networks, governance, reflexivity and accountability. Open University.

Al-Khouri A.M., Bal J. (2007) Digital identities and the promise of the technology trio: PKI, smart cards and biometrics Journal of Computer Science, 3(6), 361-367.

Al-Khouri, A. M. (2011). Re-thinking enrolment in identity card schemes. International Journal of Engineering Science and Technology, 3(2), 912-925.

Allen, R., & Pickup, A. (2017). Two-Factor Authentication. In Birch D. (ed.)., *Digital Identity Management* (pp. 131-138). Routledge.

Ambrosio, T. (2016). *Authoritarian backlash: Russian resistance to democratization in the former Soviet Union*. Routledge.

Amoretti, F., & Musella, F. (2011). Toward the European administrative space: The role of e-government policy. *European Political Science Review, 3*(1), 35-51.

Amoore, L., & De Goede, M. (2005). Governance, risk and dataveillance in the war on terror. *Crime, law and social change*, *43*(2), 149-173.

Anisimov, E. V. (1993). *The reforms of Peter the Great: progress through coercion in Russia*. ME Sharpe.

Ari Schwartz. (2011). Privacy and security: Identity management and privacy: A rare opportunity to get it right. *Association for Computing Machinery. Communications of the ACM, 54*(6), 22.

Armstrong, J. A. (1972). Tsarist and Soviet elite administrators. *Slavic Review*, *31*(1), 1-28.

Axelsson, K., Melin, U., & Lindgren, I. (2013). Public e-services for agency efficiency and citizen benefit—Findings from a stakeholder centered analysis. *Government information quarterly*, *30*(1), 10-22.

Baezner, M., & Robin, P. (2018). Cyber sovereignty and data sovereignty. *CSS Cyberdefence Trend Analysis*, 2. ETH Zurich.

Baiburin, A (2009) K Predystorii sovetskogo pasporta (History of Soviet Passport). *Neprikosnovenny Zapas*, (2), 64. https://magazines.gorky.media/nz/2009/2/k-predystorii-sovetskogo-pasporta-1917-1932.html

Baiburin, A (2017). *Sovetskiy Pasport: istoriya, struktura, praktiki* [Soviet Passport: History, Structure, Practices]. European University, St. Peterburg.

Baiburin, A. (2021). *The Soviet Passport: The History, Nature and Uses of the Internal Passport in the USSR*. John Wiley & Sons.

Ball, K, Haggerty, K and Lyon, D (2012) *Routledge Handbook of Surveillance Studies* London: Routledge.

Barnard-Wills, D. (2016). *Surveillance and identity: Discourse, subjectivity and the state*. Routledge.

Bassin, M. (1999). *Imperial visions: nationalist imagination and geographical expansion in the Russian Far East, 1840–1865* (Vol. 29). Cambridge University Press.

Bauman, Z. & Lyon, D. (2013) *Liquid Surveillance: A Conversation*. Polity

Bauman, Z., & Lyon, D. (2013). *Liquid surveillance: A conversation*. John Wiley & Sons.

Belanger, F. Hiller, J.S. (2006) "A framework for e-government: privacy implications", *Business Process Management Journal*, 12(1), 48 – 60

Bennett, C. J. (2008). *The privacy advocates: Resisting the spread of surveillance*. Cambridge, MA: MIT Press.

Bennett, C. J., & Lyon, D., (Eds.), (2008). *Playing the identity card: Surveillance, security and identification in global perspective*. New York: Routledge.

Bennett, C. J., & Raab, C. D. (2017). *The governance of privacy: Policy instruments in global perspective*. Routledge.

Berbecaru, D., & Lioy, A. (2018, October). On integration of academic attributes in the eIDAS infrastructure to support cross-border services. In *2018 22nd International Conference on System Theory, Control and Computing (ICSTCC)* (pp. 691-696). IEEE.

Bertino, E., & Takahashi, K. (2010). *Identity management: Concepts, technologies, and systems*. Artech House.

Best, K. L., & Pane, J. F. (2018). *Privacy and interoperability challenges could limit the benefits of education technology*. RAND.

Bevir, M., & Rhodes, R. A. (2012). Interpretivism and the analysis of traditions and practices. *Critical policy studies*, *6*(2), 201-208.

Beynon-Davies, P. (2007). Personal identity management and electronic government: The case of the national identity card in the UK. *Journal of Enterprise Information Management, 20*(3), 244-270.

Beynon-Davies, P. (2011). The UK national identity card. Journal of Information Technology Teaching Cases, 1(1), 12-21.

Birch, D. (Ed.) (2017) *Digital Identity Management: technological, business and social implications.* Routledge.

Borodina, A. (2013) Vnedrenie Universalnyh Electronnyh Kart v Rossii [Implementation of Universal Electronic Cards in Russia] *Sovremennaya Nauka: Aktualnye problemy i puti ih resheniya. 6,* (pp. 41-44), Lipetsk

Bourlai, T., Karampelas, P., Patel, V. M., & SpringerLink (Online service). (2020). *Securing social identity in mobile platforms: Technologies for security, privacy and identity management* (1st 2020. ed.). Springer International Publishing.

Bovt, G. (2013). Is the West prodding Moscow into a New Cold War? *Russia behind the Headlines*.

Bradley, J. (1985). *Muzhik and Muscovite: Urbanization in late imperial Russia*. Univ of California Press.

Brainerd, E. (2010). Reassessing the standard of living in the Soviet Union: an analysis using archival and anthropometric data. *The Journal of Economic History*, 83-117.

Brainerd, Elizabeth. "Reassessing the standard of living in the Soviet Union: an analysis using archival and anthropometric data." *The Journal of Economic History* 70, no. 01 (2010): 83-117.

Brehm, J. O., & Gates, S. (1999). Working, shirking, and sabotage: Bureaucratic response to a democratic public. University of Michigan Press.

Brower, D. R. (1990). *The Russian city between tradition and modernity, 1850-1900*. Univ of California Press.

Buckley, C. (1995). The myth of managed migration: migration control and market in the Soviet period. Slavic Review, 54(4), 896-916.

Burds, J. (1998). *Peasant Dreams and Market Politics: Labor Migration and the Russian Village, 1861–1905*. University of Pittsburgh Pre.

Burkhardt, F., (2022, February 17). Passport as Pretext: how Russia's Invasion of Ukraine Could Start. *War on the Rocks. Texas National Security Review* https://warontherocks.com/2022/02/passports-as-pretext-how-russias-war-on-ukraine-could-start/

Burr, W. E., Dodson, D. F., & Polk, W. T. (2004). *Electronic authentication guideline*. US Department of Commerce, Technology Administration, National Institute of Standards and Technology.

Camenisch, J., Leenes, R., & Sommer, D. (2011). *Digital privacy: PRIME – privacy and identity management for Europe*. New York: Springer Berlin Heidelberg.

Campbell, D., & Connor, S. (1986). On the Record: surveillance, computers, and privacy: the inside story. *London: Michael Joseph*.

Campbell, M. (2020). Beyond zero trust: Trust is a vulnerability. *Computer*, *53*(10), 110-113.

Caplan, J., & Torpey, J. (Eds.), (2001). *Documenting individual identity: The development of state practices in the modern world*. Princeton University Press.

Chamayou, G., & Aarons, K. (2013). Fichte's passport – A philosophy of the police. *Theory & Event*, 16(2).

Chernolutskaya, E. (2011) Prinuditelnye migracii na Sovetskom Dalnem Vostoke v 1920-1950 gg. [Forced migration in the Soviet Far East in 2920s-1950s]

Chernyavskaya, T. & Varnavsky, V. (2010) 6. PPPs in the Russian Federation: A Preliminary Assessment In Urio, P. (Ed.), *Public-private partnerships : Success and failure factors for in-transition countries*. ProQuest Ebook Central (pp. 163-199) https://ebookcentral-proquest-com.ezproxy.library.uvic.ca (technology p.190)

Chiodo, A. J., & Owyang, M. T. (2002). A case study of a currency crisis: The Russian default of 1998. *Federal Reserve Bank of St. Louis Review*, *84*(6), 7.

Clarke, R. (1988). Information technology and dataveillance. *Communications of the ACM*, *31*(5), 498-512.

Cobbe, J. (2019). Administrative law and the machines of government: judicial review of automated public-sector decision-making. *Legal Studies*, *39*(4), 636-655.

Cohen, E. D. (2010). *Mass surveillance and state control: The total information awareness project.* New York: Palgrave Macmillan Ltd.

Kolsto, P. (Ed.). (2016). New Russian Nationalism: Imperialism, Ethnicity and Authoritarianism 2000-2015. Edinburgh University Press.

Cordelia, A. (2007). E-government: towards the e-bureaucratic form? *Journal of information technology*, *22*(3), 265-274.

Cordella, A., & Bonina, C. M. (2012). A public value perspective for ICT enabled public sector reforms: A theoretical reflection. *Government Information Quarterly, 29*(4), 512-520. https://doi.org/10.1016/j.giq.2012.03.004

Crasnow, S. (2011). Evidence for use: Causal pluralism and the role of case studies in political science research. *Philosophy of the Social Sciences*, *41*(1), 26-49.

Crasnow, S. (2011). Evidence for use: Causal pluralism and the role of case studies in political science research. *Philosophy of the Social Sciences*, *41*(1), 26-49.

Deakin, M. (2013). 12 Conclusions (on the state of the transition). *Smart Cities: Governing, Modelling and Analysing the Transition*, 217.

De Hert, P. (2008). Identity management of e-ID, privacy and security in Europe. A human rights view. *information security technical report*, *13*(2), 71-75.

Der, U., Jähnichen, S., & Sürmeli, J. (2017). *Self-sovereign identity: opportunities and challenges for the digital revolution*. Cornell University

Deshpande, J. V. (2003). On a national identity card. *Economic and Political Weekly*, 38(4), 277-278.

Domingo, A. I. S., & Enríquez, Á. M. (2018). Digital Identity: the current state of affairs. *BBVA Research*, 1-46.

Dunleavy, P., Margetts, H., Bastow, S., & Tinkler, J. (2006). New public management is dead—long live digital-era governance. *Journal of public administration research and theory*, *16*(3), 467-494.

Dunleavy, P., Margetts, H., Tinkler, J., & Bastow, S. (2006). *Digital era governance: IT corporations, the state, and e-government*. Oxford University Press.

Dutton W., Guerra G.A., Zizzo D. J., Peltu M. (2005). The cyber trust tension in e-government: balancing identity, privacy, security. *Social Information Sciences*, 10(1/2), 13-23

Eckstein, H. (1975) "Case Study and theory in Political Science", in Greenstein, F.I., & Polsby, N.S., Handbook of Political Science, Vol 7: Strategies of Inquiry, 79-137

Eckstein, H. (2000). Case study and theory in political science. Case study method, 119-164.

Elliott, J. (2011). Passport to payment authentication. *Biometric Technology Today*, 2011(6), 5-8.

Engelstein, L. (2011). Slavophile empire: imperial Russia's illiberal path. Cornell University Press.

Ericson, R. V., & Haggerty, K. D. (2006). *The new politics of surveillance and visibility*. Toronto: University of Toronto Press.

Ėtkind, A. (2005). Soviet subjectivity: torture for the sake of salvation? *Kritika: Explorations in Russian and Eurasian History*, *6*(1), 171-186.

Etkind, A. (2011). Internal Colonization: Russia's Imperial Experience (Cambridge, Polity).

European Commission (2017) New Interoperability Framework. Promoting seamless services and data flows for European public administrations. https://ec.europa.eu/isa2/sites/default/files/eif_brochure_final.pdf Retrieved March 10, 2020

European Commission (2018). National approaches to eID in Europe. https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/2021/04/14/Approaches+to+eID+in+EU+countries Retrieved March 8, 2021

European Commission (2018). Shaping Europe's Digital Future https://digital-strategy.ec.europa.eu/en/news/cross-border-digital-identification-eu-countries-major-step-trusted-digital-single-market Retrieved March 8, 2021

European Commission (2021) *Overview of Member States' eID strategies* https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/National+Strategies?preview=/364643428/369688618/eID_Strategies_v4.0.pdf Retrieved March 10, 2021

Fedtke, J. (2006). Identity cards and data protection: Public security interests and individual freedom in times of crisis. *Current Legal Problems*, 59(1), 161-183.

Finkenzeller, K. (2010). *RFID handbook: fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication*. John wiley & sons.

Fioravanti F. & Nardelli E. (2008) “Identity management for e-government services” in Chen H. (eds.), *Digital Government: E-government Research, Case Studies and Implementation,* 331-352

Fischer, F. (2003). *Reframing public policy: Discursive politics and deliberative practices*. Oxford University Press. https://doi.org/10.1093/019924264X.001.0001

Fitzpatrick, S. (1996). Stalin's peasants: Resistance and survival in the Russian village after collectivization. Oxford University Press.

Fitzpatrick, S. (1999). *Everyday Stalinism: ordinary life in extraordinary times: Soviet Russia in the 1930s*. Oxford University Press, USA.

Franklin, S. (2010). Printing and social control in Russia 1: passports. *Russian History*, *37*(3), 208-237.

Froomkin, A. M. (2009). Identity cards and identity romanticism. In Kerr, I., Steeves, V. & Lucock, C. (Eds.), *Lessons from the identity trail: anonymity, privacy, and identity in a networked society. Oxford University Press* (pp. 245-554)

Gandy, O. H. (2003). Data mining and surveillance in the post-9/11 environment. The Intensification of Surveillance. Crime, Terrorism and Warfare in the Information Era, 26-41.

Gandy, O.H. (1993). *The panoptic sort: A political economy of personal information*. Critical Studies in Communication and in the Cultural Industries. Boulder and Oxford: Westview Press.

Garcelon, M. (2001). 5. Colonizing the Subject: The Genealogy and Legacy of the Soviet Internal Passport. In Caplan & Torpey (Eds.), *Documenting individual identity* (pp. 83-100). Princeton University Press. https://doi.org/10.1515/9780691186856-007;10.23943/9780691186856-007

Garson, G. D. (2006) *Public information technology and e-governance: Managing the Virtual State*. Jones & Bartlett Learning

Geertz, C. (Ed.). (1972). *Myth, symbol, and culture*. Norton

Gentes, A. A. (2008). *Exile to Siberia, 1590-1822* (pp. 1-271). Basingstoke: Palgrave Macmillan.

German, T., & Karagiannis, E. (Eds.). (2018). *The Ukrainian Crisis: The Role Of, and Implications For, Sub-state and Non-state Actors*. Routledge.

Gelb, A., & Metz, A. D. (2018). Identification revolution: Can digital ID be harnessed for development? Brookings Institution Press.

Gelb, A., & Clark, J. (2013). Identification for development: The biometrics revolution. Center for Global Development Working Paper, (315).

Giddens, A. (1986). The nation-state and violence. *Capital & Class*, *10*(2), 216-220.

Goede, M. (2019). E-Estonia: The e-government cases of Estonia, Singapore, and Curaçao. *Archives of Business Research*, *7*(2), 216-227

Goldsmith, S., & Eggers, W. D. (2005). *Governing by network: The new shape of the public sector*. Brookings institution press.

Golosov, G. V. (2017). Authoritarian Learning in the Development of Russia's Electoral System. Russian Politics, 2(2), 182-205.

Goode, J. P. (2010). Russia's Gubernatorial Elections: A Postmortem. In *Institutions, Ideas and Leadership in Russian Politics* (pp. 43-66). Palgrave Macmillan, London.

Gore, A. (1993). *Reengineering through information technology: Accompanying report of the national performance review*. Office of the Vice President.

Government of Canada (2022). Digital Academy, *Canada School of Public Service (CSPS)* https://www.csps-efpc.gc.ca/digital-academy/index-eng.aspx Retrieved in June 2022

Government of Canada (2020) Cloud Adoption Strategy, *Treasury Board of Canada Secretariat* https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/government-canada-cloud-adoption-strategy.html Retrieved in July 2020

Graham, S., & Wood. D. (2003) Digitizing surveillance: Categorization, space, inequality. *Critical Social Policy*, 23(2), 227-248.

Gritsenko, D., & Zherebtsov, M. (2021). E-Government in Russia: Plans, Reality, and Future Outlook. In D. Gritsenko et al. (Eds.) *The Palgrave Handbook of Digital Russia Studies* (pp. 33-51). Palgrave Macmillan, Cham.

Groebner V. (2008). Who are you? Identification, deception, and surveillance in early modern Europe. New York

Hadley, C. (2004). Your personal passport. EMBO Reports, 5(2), 124-126.

Haggerty, K. D., & Samatas, M. (2010). *Surveillance and democracy*. New York: Routledge.

Hartley, J. (1999). *A social history of the Russian Empire 1650-1825*. Longman.

Haugen (2005) E-government, cyber-crime and cyber-terrorism: a population at risk. *Electronic Government*, vol. 2/4.

Hedlund, S. (2008). Such a beautiful dream: How Russia did not become a market economy. *The Russian Review*, *67*(2), 187-208.

Hedlund, S. (2011). *Invisible hands, Russian experience, and social science: Approaches to understanding systemic failure*. Cambridge University Press.

Henderson, J. (1996). *The passport society: Controlling movement in Russia and the USSR.* Modern Humanities Research Association.

Henderson, A. (2016). Smart Cards, Smart Identities. In Birch D. (Ed.), *Digital Identity Management* (pp. 29-40). Routledge.

Hendriks, C. M. (2007). Praxis stories: Experiencing interpretive policy research. *Critical Policy Analysis*, *1*(3), 278-300.

Henry, L. A. (2009). Redefining citizenship in Russia: Political and social rights. *Problems of Post-Communism*, *56*(6), 51-65.

Hier, S. P., & Greenberg, J. (2009). *Surveillance: Power, problems, and politics*. Vancouver: UBC Press.

Hier, S. P., & Walby, K. (2014). Policy mutations, compliance myths, and redeployable special event public camera surveillance in Canada. *Sociology*, *48*(1), 150-166.

Hippelainen, L., Oliver, I., & Lal, S. (2017, August). Towards dependably detecting geolocation of cloud servers. In *International Conference on Network and System Security* (pp. 643-656). Springer, Cham.

Hirsch, F. (2005). *Empire of Nations: Ethnographic Knowledge & the Making of the Soviet Union.* Ithaca: Cornell University Press.

Hirsch, F. (2014). *Empire of nations*. Cornell University Press.

Holquist, P. (2001). To count, to extract, and to exterminate: population statistics and population politics in late imperial and soviet Russia. *A State of Nations: Empire and Nation-making in the Age of Lenin and Stalin*, *1*, 111-144.

Hood, C. (2005). The idea of joined-up government: A historical perspective. In Bogdanor, V. (Eds.), *Joined-up government.* (pp. 19-42). Oxford University Press for the British Academy. DOI: 10.5871/bacad/9780197263334.001.0001

Hood, C. C. (1983). The tools of government. London: Macmillan Press.

Hood, C. C., & Margetts, H. Z. (2007). The tools of government in the digital age. Palgrave Macmillan.

Horrocks, I. (2009) 'Experts' and E-government. *Information, Communication and Society*, 110-127.

Humphry, D., & Ward, M., (1974). *Passports and politics*. Harmondsworth: Penguin.

Husz, O. (2018). Bank identity: banks, ID cards, and the emergence of a financial identification society in Sweden. *Enterprise & Society*, *19*(2), 391-429.

Huysmans, X. (2008). Privacy-friendly identity management in e-Government. (pp. 245-258). Boston, MA: Springer US.

Intelligence, A. M. (2017). The Global National eID Industry Report: 2017 Edition. https://www.acuitymi.com/product-page/the-global-national-eid-industry-report Retrieved October, 2019

Jain A.K., Nandakumar K., Nagar A. (2008) Biometric template security *EURASIP Journal on Advances in Signal Processing*, Special Issue on Advanced Signal Processing and Pattern Recognition Methods for Biometrics, 1(13)

Janowski, T. (2015). Digital government evolution: From transformation to contextualization. *Government Information Quarterly*, 32(3), 221-236

Janssen, M., & Estevez, E. (2013). Lean government and platform-based governance—Doing more with less. *Government Information Quarterly*, *30*, S1-S8.

Johnston, S. F. (2018). Alvin Weinberg and the promotion of the technological fix. *Technology and culture*, *59*(3), 620-651.

Kalinina, A. (2021) *Vydadut li zagran passport esli est dolgi?* [Would they issue an international passport if I have a debt?]. Legal expert analysis. https://visasam.ru/samotur/passport/zagranpasport-dolgi.html Retrieved April 20, 2021

Kazantsev, S. Yu, and I. E. Frolov. "Developing the Russian info communication complex: Conditions and potential." *Studies on Russian Economic Development* 17, no. 4 (2006): 395-406.

Kessler, G. (2001). The passport system and state control over population flows in the Soviet Union, 1932-1940. *Cahiers du monde russe. Russie-Empire russe-Union soviétique et États indépendants*, *42*(42/2-4), 477-504.

Kessler, G. (2001). The passport system and state control over population flows in the Soviet Union, 1932-1940. *Cahiers du monde russe. Russie-Empire russe-Union soviétique et États indépendants*, *42*(42/2-4), 477-504.

Kirichenko, Y. N. (2014). Historic and Legal Review on Passport Reform of 1974 and its Role in Strengthening of the USSR Public Order. *Былые годы. Российский исторический журнал*, (34), 707-713.

Konstantinov, A. (2006). Korumpirovannaya Rossiya [Corrupted Russia]. OLMA-Press, Moscow

Kotkin, S., & American Council of Learned Societies. (1997). Magnetic mountain: Stalinism as a civilization. University of California Press

Kotsonis, Y. (1999). *Making peasants backward: Agricultural cooperatives and the Agrarian question in Russia, 1861–1914*. Springer.

Kotsonis, Y. (2014). *States of obligation: Taxes and citizenship in the Russian empire and early Soviet Republic*. University of Toronto Press.

Korenev, A. (1999). Administrativnaya Deiatelnost′ Organov Vnutrennikh Del. Chast′ Osobennaia.[Administration Activities of the Departments of Internal Affairs. Special Requirements]. Moscow

Krueger, S. (2009). Passports in the twenty-first century. *Global Jurist*, 9(1), 1-16.

Kubicek, H., & Hagen, M. (2000). One stop government in Europe: An overview. *Hagen, M., Kubicek, H.(Eds. 2000). One Stop Government in Europe. Results from*, *11*, 1-36.

Kulchytsky S.V. & Vronska, T.V. (1999) Soviet Passport System. Ukrainian Historical Journal, 3, 1-15

Lamersdorf, W., Tschammer, V., & Amarger, S. (Eds.). (2004). *Building the e-service society: e-commerce, e-business, and e-government* (Vol. 146). Springer Science & Business Media.

Lapidus, G. W. (1978). *Women in Soviet society*. University of California Press.

Lapidus, G. W. (1992). *From democratization to disintegration: the impact of perestroika on the national question*. Berkeley-Stanford Program in Soviet and Post-Soviet Studies.

Lapidus, G. W. (Eds.). (1992). *The" Nationality" Question in the Soviet Union* (Vol. 11). Taylor & Francis.

Laruelle, M. (2016). Russia as an anti-liberal European civilisation. In Kolsto P. & Blakkisrud H. (Eds.), *The new Russian nationalism: Imperialism, ethnicity and authoritarianism 2000-2015*, 275-297.

Laurent, M., & Bouzefrane, S. (2015). *Digital identity management*. Elsevier.

Lawson, G. (1998). *NetState: Creating electronic government* (Vol. 18). Demos.

Lee, H. J. (2018). The Tension between Cultural Codes in South Korean Civil Society: The Case of the Electronic National Identification Card. *Cultural Sociology*, *12*(1), 96-115.

Leitold, H. (2010, August). Challenges of eID interoperability: The STORK project. In *IFIP PrimeLife International Summer School on Privacy and Identity Management for Life* (pp. 144-150). Springer, Berlin, Heidelberg.

Leitold, H., & Zwattendorfer, B. (2011). STORK: architecture, implementation and pilots. In *ISSE 2010 Securing Electronic Business Processes*. 131-142). Vieweg+ Teubner.

Leman-Langlois, S. (2012;) (Ed.), *Technocrime, policing, and surveillance*. Routledge. https://doi.org/10.4324/9780203105245

Leman-Langlois, S. (Eds.), (2018). Technologies of surveillance. *The handbook of social control*, 347-360.

Lentner, G. M., & Parycek, P. (2016). Electronic identity (eID) and electronic signature (eSig) for eGovernment services–a comparative legal study. *Transforming Government: People, Process and Policy*.

Li, Y., & Wagenaar, H. (2019). Revisiting deliberative policy analysis. Policy Studies. (Vol. 40, pp. 427-436).

Light, M. (2010). Policing migration in Soviet and post-Soviet Moscow. *Post-Soviet Affairs*, *26*(4), 275-313.

Lijphart, A. (1971). Comparative politics and the comparative method. American political science review, 65(3), 682-693.

Lips, S., Bharosa, N., & Draheim, D. (2020). eIDAS Implementation Challenges: The Case of Estonia and the Netherlands. In *International Conference on Electronic Governance and Open Society: Challenges in Eurasia* (pp. 75-89). Springer, Cham.

Lips, A. M. B., Taylor, J. A., & Organ, J. (2009). Identity management, administrative sorting and citizenship in new modes of government. *Information, Communication & Society*, *12*(5), 715-734.

Lloyd, M. (2003). *The passport*. Phoenix Mill et al.: Sutton Publishing.

Lohr, E. (2006). The ideal citizen and real subject in late imperial Russia. *Kritika: Explorations in Russian and Eurasian History*, *7*(2), 173-194.

Lohr, E. (2012). *Russian Citizenship: From Empire to Soviet Union*. Harvard University Press.

Lonergan, G. (2013). Registration as Privilege: The Moscow Residence Permit as a Mark of Privilege in the Russian Empire, 1881–1905. In About, I., Brown, J. & Lonergan, G. (Eds.),

Identification and Registration Practices in Transnational Perspective (pp. 31-43). Palgrave Macmillan, London.

Lynch, A. C. (2005). *How Russia is not ruled: Reflections on Russian political development*. Cambridge University Press.

Lyon, D. (2007). Surveillance, security and social sorting: Emerging research priorities. *International Criminal Justice Review*, 17(3), 161-170.

Lyon, D. (2008). Biometrics, identification and surveillance. *Bioethics*, 22(9), 499-508

Lyon, D. (2010) "Liquid Surveillance: The Contribution of Zygmunt Bauman to Surveillance Studies1." International Political Sociology 4(4) 325-338.

Lyon, D., (1994). *The electronic eye: The rise of surveillance society*. Minneapolis: University of Minneapolis Press.

Lyon, D., (2006). *Theorizing surveillance: The panopticon and beyond*. Cullompton, Devon, UK: Willan Publishing.

Lyon, D., (2007). *Surveillance studies: An overview*. Malden, MA: Polity.

Lyon, D., (2009). *Identifying citizens: ID cards as surveillance*. Malden, MA: Polity.

Lyon, D., (2015). Surveillance after Snowden. Polity

Lytras, M. D., & Visvizi, A. (2018). Who uses smart city services and what to make of it: Toward interdisciplinary smart cities research. *Sustainability*, *10*(6), 1998. https://doi.org/10.3390/su10061998

Maerz, S. F. (2016). The electronic face of authoritarianism: E-government as a tool for gaining legitimacy in competitive and non-competitive regimes. *Government Information Quarterly*, *33*(4), 727-735.

Magnusson, W. (2013). *Politics of urbanism: Seeing like a city*. Routledge.

Maltseva, E. (2012). *Welfare reforms in post-Soviet states: a comparison of social benefits reform in Russia and Kazakhstan* (Doctoral dissertation, University of Toronto).

Manby, B. (2021). The Sustainable Development Goals and 'legal identity for all':'First, do no harm'. *World Development*, *139*, 105343.

Mani, S. (2002). *Government, innovation, and technology policy: An international comparative analysis*. Northampton, MA: Edward Elgar Pub.

Margetts, H., & Dunleavy, P. (2013). The second wave of digital-era governance: a quasi-paradigm for government on the Web. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *371*(1987), 20120382.

Martens, T. (2010). Electronic identity management in Estonia between market and state governance. *Identity in the Information Society, 3*(1), 213-233.

Mason, S. (2004). Is there a need for identity cards? *Computer Fraud & Security*, 2004(9), 8-14.

Mayes, K. (2017). An introduction to smart cards. In *Smart Cards, Tokens, Security and Applications* (pp. 1-29). Springer, Cham.

Merriam, S. B. (1998). *Qualitative Research and Case Study Applications in Education. Revised and Expanded from" Case Study Research in Education."*. Jossey-Bass Publishers, 350 Sansome St, San Francisco, CA 94104.

Melin, U. (2016). *Identity, identification and eID in a public e-service context*. Emerald.

Metcalf, K. N. (2019). How to build e-governance in a digital society: the case of Estonia. *Revista Catalana de Dret Public*, 1-12.

Michael, R. A. D. U. (2008). Russian Imperialism–It's Back. *Revista de Ştiinţe Politice. Revue des Sciences Politiques*, (18+ 19), 11-12.

Milberry, K., Parsons, C., (2013). *The BC services card: A national ID card by stealth? Privacy risks, opportunities and alternatives.* Vancouver, BC: BC Civil Liberties Association.

Miller, H. T. 1. (2012). *Governing narratives: Symbolic politics and policy change*. University of Alabama Press.

Milward, H. B., & Snyder, L. O. (1996). Electronic government: Linking citizens to public organizations through technology. *Journal of Public Administration Research and Theory*, *6*(2), 261-276.

Mistry, J. & Jalal, A. (2012). An empirical analysis of the relationship between e-government and corruption. *The international journal of digital accounting research*, 12, 145-176.

Modi, K., Shimon (2011) *Biometrics in identity management: concepts and applications.* Artech House

Moe, R. C. (1994). The" reinventing government" exercise: Misinterpreting the problem, misjudging the consequences. *Public administration review*, *54*(2), 111-122.

Monahan, T. (2008). Marketing the beast: Left Behind and the apocalypse industry. *Media, Culture & Society*, *30*(6), 813-830.

Molokotos-Liederman, L. (2003). Identity crisis: Greece, orthodoxy, and the European Union. *Journal of Contemporary Religion*, *18*(3), 291-315.

Molokotos-Liederman, L. (2007). The Greek ID card controversy: A case study of religion and national identity in a changing European Union. *Journal of Contemporary Religion*, *22*(2), 187-203.

Moon, D. (2002). Peasant Migration, the Abolition of Serfdom and the Internal Passport System in the Russian Empire, c. 1800-1914'. In *Free and Coerced Migration* (pp. 324-57). Stanford University Press.

Moon, D. (2014). *The Abolition of Serfdom in Russia: 1762-1907*. Routledge.

Murakami Wood, D., & Webster, C. W. R. (2009). Living in surveillance societies: The normalisation of surveillance in Europe and the threat of Britain's bad example. *Journal of Contemporary European Research*, *5*(2), 259.

Ndou, V. (2004). E-Government for Developing Countries: Opportunities and Challenges. *The Electronic Journal of Information Systems in Developing Countries*, *18*(0), 1-24

Nelson, R. M. (2015). *US sanctions on Russia: Economic implications*. Washington, DC: Congressional Research Service.

Neumann, L., & as SSEDIC, A. N. E. C. T. (2012). Cyber Identity is NOT Human Identity–A System Weaknesses Analysis of Current eID Technologies. *European Journal of ePractice*, 79-89.

Novakouski, M., & Lewis, G. A. (2012). *Interoperability in the e-Government Context*. Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst.

O'Byrne, D. J. (2001). On passports and border controls. *Annals of Tourism Research*, 28(2), 399-416.

Oduro-Marfo, S. (2021). Surveillance for development? Debating citizen identification systems in Ghana (Doctoral dissertation).

OECD (2020), "The OECD Digital Government Policy Framework: Six dimensions of a Digital Government", *OECD Public Governance Policy Papers*, No. 02, OECD Publishing, Paris, https://doi.org/10.1787/f64fed2a-en.

Official website of the Moscow City Council, Karta Moskvicha [Moscow Social Card] https://www.mos.ru/karta-moskvicha/ Retrieved January 20, 2021

Ojha A., Palvia S., Gupta M.P. (2008) "A model for impact of e-government on corruption: Exploring theoretical foundations". In Bhattacharya J. (eds.) *Critical thinking in e-governance,* 160-170

Oleinik, A.N. (2010). “Russkaia vlast: konstruirovanie idealnogo tipa.” [Russian State: Constructing an Ideal Type]. *Politicheskaia kontseptologiia,* no. 1.

Otjacques B., Hitzelberger P., Feltz F. (2007) Interoperability of E-government Information Systems: Issues of Identification and Data Sharing. *Journal of Management Information Systems* 23(4), 29-51

Ott, A., Hanson, F., & Krenjova, J. (2018). Introducing integrated e-government in Australia. *Fonte: https://www. acs. org. au/content/dam/acs/acs-publications/E-Gov% 20Report. pdf*.

Packard, V. (1964). The Naked Society'McKay. *New York*.

Palihapitiya, H. (2006). *National identity cards, biometrics and the consumer: Displacing the personal from the person.* Ottawa, Ont: Public Interest Advocacy Centre.

Pang, M. S., Lee, G., & DeLone, W. H. (2014). IT resources, organizational capabilities, and value creation in public-sector organizations: a public-value management perspective. *Journal of Information Technology*, *29*(3), 187-205.

Park, N., & Lee, D. (2018). Electronic identity information hiding methods using a secret sharing scheme in multimedia-centric internet of things environment. *Personal and Ubiquitous Computing*, *22*(1), 3-10.

Paris, R. (2022, March 3) Putin has been redefining “sovereignty” in dangerous ways. *The Washington Post.* https://www.washingtonpost.com/politics/2022/03/03/putin-sovereignty-ukraine-part-of-russia/

Pathak, R. D., Belwal, R., Naz, R., Smith, R. F., & Al-Zoubi, K. (2010). Citizens’ Perceptions of Corruption and E-Governance in Jordan, Ethiopia, and Fiji—the Need for a Marketing Approach.

Pelletier, M. P., Trépanier, M., & Morency, C. (2011). Smart card data use in public transit: A literature review. *Transportation Research Part C: Emerging Technologies*, *19*(4), 557-568.

Piccolino, G. (2016). Infrastructural state capacity for democratization? Voter registration and identification in Côte d'Ivoire and Ghana compared. *Democratization*, *23*(3), 498-519.

Pohlebkin, V. (1992) Passport. Istorichesky ocherk. [Passport. Historical Review] http://xn--90aefkbacm4aisie.xn--p1ai/content/pasport Retrieved March 20, 2021

Poller, A., Waldmann, U., Vowe, S., & Turpe, S. (2012). Electronic identity cards for user authentication – promise and practice. *IEEE Security & Privacy Magazine*, 8(1), 46-54.

Popov, V. (1996). Pasportnaya sistema sovetskogo krepostnichestva [Passport System of the Soviet Serfdom]. *Novyi mir*, (6).

Popova, Alena “Why Russians pay the most for the municipal services in the world?” [in Russian]. Echo Moscow Published August 30, 2014. Last accessed on April, 2015. Available at http://echo.msk.ru/blog/apopova/1390426-echo/

Porcedda, M. G. (2018). Regulation of Data Breaches in the European Union: Private Companies in the Driver’s Seat of Cybersecurity?. In *Security Privatization* (pp. 275-299). Springer, Cham.

Rankl, W., & Effing, W. (2004). *Smart card handbook*. John Wiley & Sons.

Rankl, Wolfgang, and Wolfgang Effing. *Smart card handbook*. John Wiley & Sons, 2010.

Reddick, C. G., & SpringerLink Ebook Collection. (2010). *Comparative e-government*. New York: Springer New York.

Reeves, M. (2015). Living from the Nerves: Deportability, Indeterminacy, and the 'Feel of Law' in Migrant Moscow. *Social Analysis*, *59*(4), 119-136.

Reina-Rozo, J. D., & Medina-Cardona, L. F. (2021). Science, technology and Solidarity: The emergence of a free culture for the future. *International Journal of Engineering, Social Justice, and Peace*, *8*(1), 86-104.

Ribeiro, C., Leitold, H., Esposito, S., & Mitzam, D. (2018). STORK: a real, heterogeneous, large-scale eID management system. *International Journal of Information Security*, *17*(5), 569-585.

Rogovin, L. (1913) *Ustav o Pasportah.* [Statute about Passports]. Zakonovedenie. Sankt-Peterburg.

Roe, E. (1994). *Narrative policy analysis: Theory and practice*. Duke University Press.

Ro'i, Y. (Ed.). (1995). Jews and Jewish life in Russia and the Soviet Union (Vol. 2). Psychology Press

Rosenthal, B. (2010). New myth, new world: From Nietzsche to Stalinism. Penn State Press.

Rowney, D., & Huskey, E. (Eds.). (2009). Russian bureaucracy and the state: officialdom from Alexander III to Vladimir Putin. Springer.

Roy, J. (2020). Digital Government and Democratic Trust: From Online Service to Outward Engagement. In Small, T. & Jansen, H., (Eds.), *Digital Politics in Canada: Promises and Realities*, (pp.46-64). University of Toronto Press.

Rozov, N. S. (2012). The Specific Nature of" Russian State Power". *Russian politics and law*, 50(1), 36-53.

Ruggles, R., Pemberton Jr, J. D. J., & Miller, A. R. (1968). Computers, Data Banks, and Individual Privacy. *Minn. L. Rev*, *53*, 211.

Runnel, P., Pruulmann-Vengerfeldt, P., & Reinsalu, K. (2009). The Estonian tiger leap from post-communism to the information society: From policy to practice. Journal of Baltic Studies, 40(1), 29-51.

Rumyantsev, A. (2017). Russia: Information Security Doctrine, Stricter Regulations Against "Fake News" and Blocking LinkedIn. *Computer Law Review International*, *18*(1), 28-32.

Ryavec, K. W. (2005). Russian bureaucracy: Power and pathology. Rowman & Littlefield.

Saeed, S., Ramayah, T., & Mahmood, Z. (2018). *User Centric E-Government*. Springer

Sakwa, R. (2010). The crisis of Russian Democracy: the Dual State, Factionalism and the Medvedev Succession. Cambridge University Press.

Salenko, A (2012). *EUDO Citizenship Observatory. Country report: Russia.* European University Institute. https://cadmus.eui.eu/bitstream/handle/1814/60230/RSCAS_EUDO_CIT_2012_1.pdf Retrieved December 20, 2020

Sanborn, J. A. (2014). Russian imperialism, 1914–2014: annexationist, adventurist, or anxious? *Revolutionary Russia*, *27*(2), 92-108.

Sasse, G. (2007). *The Crimea question: identity, transition, and conflict*. Harvard University Press.

Savoldelli, A., Codagnone, C., & Misuraca, G. (2012, October). Explaining the e-government paradox: An analysis of two decades of evidence from scientific literature and practice on barriers to egovernment. In *Proceedings of the 6th International Conference on Theory and Practice of Electronic Governance* (pp. 287-296).

Saxby, S. (2006). Government feels the pressure on identity cards. *Computer Law and Security Review: The International Journal of Technology and Practice, 22*(2), 103-104.

Schedler, K., & Scharf, M. C. (2001). Exploring the interrelations between electronic government and the new public management. In *Towards the E-Society* (pp. 775-788). Springer, Boston, MA.

Schenk, C. (2018). 5. Local Politics of Immigration in Moscow. In *Why Control Immigration?: Strategic Uses of Migration Management in Russia* (pp. 125-150). University of Toronto Press.

Schmidt, E., & Cohen, J. (2014). *The new digital age: Transforming nations, businesses, and our lives*. Vintage.

Scholl H.J., Klischewski R. (2007) E-government integration and Interoperability: Framing the Research Agenda. *International Journal of Public Administration*, 30, 889-920

Schrader, A. M. (2000). Branding the Exile as 'Other': Corporal Punishment and the Construction of Boundaries in mid-Nineteenth Century Russia. In *Russian Modernity* (pp. 19-40). Palgrave Macmillan, London.

Schrader, A. M. (2002). *Languages of the lash: Corporal punishment and identity in imperial Russia*. Northern Illinois University Press.

Schuppan, T. (2009). Reassessing outsourcing in ICT-enabled public management: Examples from the UK. *Public Management Review*, *11*(6), 811-831.

Schwartz-Ziv, M., & Volkova, E. (2021). Is Blockholder Diversity Detrimental? Available at *Social Science Research Network* 3621939.

Seltsikas, P., & O'keefe, R. M. (2010). Expectations and outcomes in electronic identity management: the role of trust and public value. *European Journal of Information Systems*, *19*(1), 93-103.

Semukhina, O. B., & Reynolds, K. M. (2013). Understanding the modern Russian police.

Shearer, D. (2004). Elements near and alien: passportization, policing, and identity in the Stalinist state, 1932–1952. *The Journal of Modern History*, *76*(4), 835-881.

Shearer, D. R. (2009). *Policing Stalin's socialism: Repression and social order in the soviet union, 1924-1953*. Yale University Press.

Shearer, D. R., 1952, & Khaustov, V. N. (2015). *Stalin and the Lubianka: A documentary history of the political police and security organs in the Soviet Union*, 1922-1953. Yale University Press.

Shevtsova, L. F. (2007). *Russia: lost in transition: the Yeltsin and Putin legacies*. Carnegie Endowment.

Shipan, C. R., & Volden, C. (2008). The mechanisms of policy diffusion. *American journal of political science*, *52*(4), 840-857.

Singla, S. K. (2011) Combating corruption through e-governance in public service delivery system. *Journal of Global Research in Computer Science* 7 (2), 96-100.

Sister, Vladimir "Informational Technology Serving Cities", [in Russian]. Information Society 1 (2003): pp. 22-24 [in Russian]

Sloan, R., & Warner, R. (2017). *Unauthorized access: The crisis in online privacy and security* (p. 401). Taylor & Francis.

Solove, D. J. (2008). Understanding privacy.

Solove, D. J. (2012). Introduction: Privacy self-management and the consent dilemma. *Harv. L. Rev.*, *126*, 1880.

Soldatov, A. (2016). All-Encompassing Paranoia: How the Attitude Toward Security Has Changed in Russia. *Russian Politics & Law*, *54*(4), 395-403.

Stanziani, A. (2010). Revisiting Russian serfdom: bonded peasants and market dynamics, 1600s-1800s. *International Labor and Working-Class History*, 12-27.

Stamp, M. (2011). *Information security: principles and practice*. John Wiley & Sons.

Steel, Emily "Visa's Blueprint for Targeted Advertising" Wall Street Journal, Published October 24, 2011. Last accessed on April, 2015. Available at: http://blogs.wsj.com/digits/2011/10/24/visas-blueprint-for-targeted-advertising/

Steinwedel, C. (2001). Making Social Groups, One Person at a Time: The Identification of Individuals by Estate, Religious Confession, and Ethnicity in Late Imperial Russia. In J. Caplan & J. Torpey (Eds.), *Documenting individual identity: The development of state practices in the modern world*. (pp. 67-82). Princeton University Press.

Stites, R. (1978). *The women's liberation movement in Russia: feminism, nihilism, and bolshevism, 1860-1930* (Vol. 59). Princeton University Press.

Stites, R. (2008). *Serfdom, society, and the arts in Imperial Russia*. Yale University Press.

Stoica, M., & Ghilic-Micu, B. (2016). E-Voting Solutions for Digital Democracy in Knowledge Society. *Informatica Economica*, *20*(3), 55-65.

Stuart, R. C., & Morton, H. W. (Eds.). (1984). *The Contemporary Soviet City*. ME Sharpe.

Study Tours to Poland, 2008

Sturm, T., & Albrecht, T. (2020). Constituent Covid-19 apocalypses: contagious conspiracism, 5G, and viral vaccinations. *Anthropology & Medicine*, 1-18.

Suhardi, S., Sofia, A., & Andriyanto, A. (2015). Evaluating e-Government and Good Governance Correlation. *ITB Journal Publisher, LPPM ITB*, *9*(3), 236-262

Sullivan, R. J. (2008). Can smart cards reduce payments fraud and identity theft? *Economic Review, 93*(3), 35-62.

Sullivan, C. (2018). Digital identity–From emergent legal concept to new reality. *Computer Law & Security Review*, *34*(4), 723-731.

Sundstrom, L. M., & Henry, L. A. (2016). Russian civil society: Tensions and trajectories. In Russian civil society: a critical assessment (pp. 313-330). Routledge.

Svod zakonov Rossiyskoy Imperii. Tom 14. Ustav o pasportah (1903). [Laws of Russian Empire. Tome 14. Statute about Passports] http://rus-sky.com/history/library/vol.14/vol.14.1.htm Retrieved January 15, 2021

Tambouris, E., & Wimmer, M. (2005). Online One-Stop Government: A Single Point of Access to Public Services. In Huang, W., Siau, K., & Wei, K. K. (Eds.), *Electronic Government Strategies and Implementation* (pp. 115-144). IGI Global. http://doi:10.4018/978-1-59140-348-7.ch006

THALES (2021). National ID cards: 2016 – 2021: facts and trends. Industry market report

Thomas, E., & Zhang, A. (2020). *ID2020, Bill Gates and the Mark of the Beast: how Covid-19 catalyses existing online conspiracy movements*. Australian Strategic Policy Institute.

Thompson, S. (2008). Separating sheep from the goats: The United Kingdom's National Registration programme and social sorting in the pre-electronic era. In Bennett, C. & Lyon, D. (Eds.), *Playing the identity card. Surveillance, security and identification in global perspective*. New York: Routledge

Tistarelli, M., Li, S. Z., & Chellappa, R. (2009). *Handbook of remote biometrics: For surveillance and security*. New York: Springer. doi: 10.1007/978-1-84882-385-3.

Torpey, J. (1997). Revolutions and freedom of movement: an analysis of passport controls in the French, Russian, and Chinese revolutions. *Theory and Society*, *26*(6), 837-868.

Torpey, J. (1998). Coming and going: On the state monopolization of the legitimate "means of movement". *Sociological theory*, *16*(3), 239-259.

Torpey, J. (2000). *The invention of the passport: Surveillance, citizenship, and the state*. New York: Cambridge University Press.

Twizeyimana, J. D., & Andersson, A. (2019). The public value of E-Government–A literature review. *Government information quarterly*, *36*(2), 167-178.

Umland, A. (2012). Russia's new" special path" after the Orange Revolution: radical anti-westernism and paratotalitarian neo-authoritarianism in 2005-8. *Russian Politics & Law*, *50*(6), 19-40.

United Nations E-Government Survey (2003-2020), *E-Government Knowledge Database.* https://publicadministration.un.org/egovkb/en-us/ Retrieved March 20, 2021

Vaile, D. (2014). The Cloud and data sovereignty after Snowden. *Journal of Telecommunications and the Digital Economy*, *2*(1), 31-1.

van Dijck, J., & Jacobs, B. (2020). Electronic identity services as sociotechnical and political-economic constructs. *New media & society*, *22*(5), 896-914.

Van Eecke, P. (2009). Electronic Identity Cards: The e-government accelerating factor in Europe. *Scitech Lawyer, 6*(2), 4.

Wagenaar, H. (2011). *Meaning in action: Interpretation and dialogue in policy analysis*. ME Sharpe.

Warner, M., & Stone, M. (1970). The Data Bank Society: Organisations. *Computers and Social Freedom'George Allen and Unwin*.

Weber, M. (2009). *The theory of social and economic organization*. Simon and Schuster.

Webster, C.W.R. (2012) "Public Administration as Surveillance" in Ball, K, Haggerty, K and Lyon, D (eds.) *Routledge Handbook of Surveillance Studies* London: Routledge.

West, D. M. (2004). E-government and the transformation of service delivery and citizen attitudes. *Public administration review*, *64*(1), 15-27.

Westin, A. F., & Baker, M. A. (1973). Databanks in a free society. *Acm Sigcas Computers and Society*, *4*(1), 25-29.

Westin, A. F. (2013). Civil liberties issues in public databanks. In *Information technology in a democracy* (pp. 301-310). Harvard University Press.

Whitmore, A. (2012). A statistical analysis of the construction of the United Nations E-Government Development Index. *Government Information Quarterly*, *29*(1), 68-75.

Wills D. (2008) "The United Kingdom identity card scheme: Shifting motivations, statics technologies" in Bennett, C. J., & Lyon, D., (2008). *Playing the identity card: Surveillance, security and identification in global perspective*. New York: Routledge, 163-179.

Wilson, D. (2008). 11 The politics of Australia's "Access Card". In Bennett, C. J., & Lyon, D., (Eds.), *Playing the Identity Card: Surveillance, security and identification in global perspective*. (pp. 180-197). Routledge.

Windley, P. J. (2005). *Digital Identity: Unmasking identity management architecture (IMA)*. " O'Reilly Media, Inc.".

Wimmer, M., & Traunmuller, R. (2000, September). Trends in electronic government: managing distributed knowledge. In *Proceedings 11th International Workshop on Database and Expert Systems Applications* (pp. 340-345). IEEE.

World Bank (2021) Project on Identification for Development https://id4d.worldbank.org/

Wright, D., & Raab, C. (2014). Privacy principles, risks and harms. *International Review of Law, Computers & Technology*, *28*(3), 277-298.

Yanow, D. (2000). *Conducting interpretive policy analysis*. SAGE Publications, Inc. https://www-doi-org.ezproxy.library.uvic.ca/10.4135/9781412983747

Yanow, D. (2007). Interpretation in policy analysis: On methods and practice. *Critical policy analysis*, *1*(1), 110-122.

Yanow, D. (2015). Making sense of policy practices: Interpretation and meaning. In *Handbook of critical policy studies*. Edward Elgar Publishing.

Yekelchyk, Serhy. "The Crimean Exception: Modern Politics as Hostage of the Imperial Past." *The Soviet and Post-Soviet Review* 46.3 (2019): 304-323.

Yeow, P. H. P., Hong Loo, W., & Choy Chong, S. (2007). Accepting multipurpose "Smart" identity cards in a developing country. *Journal of Urban Technology, 14*(1), 23-50.

Yiu, C. (2012) The Big Data Opportunity: Making government faster, smarter and more personal. Policy Exchange report, London

Zakaria, F. (2007). *The Future of Freedom: Illiberal Democracy at Home and Abroad (Revised Edition)*. WW Norton & company.

Zherebtsov, M. (2016, June). The Troubled Path of e-Government in Russia: When Advanced Technologies Don't Work Properly. In *European Conference on Digital Government* (p. 247). Academic Conferences International Limited.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power* (First ed.). Public Affairs.

Zureik, E. (2010). *Surveillance, privacy, and the globalization of personal information: International comparisons*. Montreal: McGill-Queen's University Press.

Appendix A: List of primary sources

All titles of the primary sources in Russian are transliterated and translated for the purpose of analysis. Some of the sources were archived by the publisher and may not be available via internet. Their electronic copies in PDF are stored by the principal researcher.

1. Russian government legislation, policies, regulations, programs

Government of the Russian Federation (2002, January 28). Federalnaya tselevaia programa "Electronnaya Rossiia", [Federal Target Program "Electronic Russia 2002-2010] Retrieved June 30, 2014 from https://www.prlib.ru/en/node/432947

Government of the Russian Federation (2006, July 27), Federalnyi zakon "O personalnyh dannyh 152-FZ" [Federal Law on Personal Data nr. 152-FZ] Retrieved August 30, 2020 from https://rg.ru/documents/2006/07/29/personaljnye-dannye-dok.html

Government of the Russian Federation (2006, July 27) Federalnyi zakon "Ob informatsyi, informatsyonnyh tehnologiiah i o zashite informatsyi 149-FZ" [Federal Law "On information, information technologies and protection of information" nr. 149-FZ]

Government of the Russian Federation (2015, July 13) Federalnyi zakon "O vnesenii izmenenii v zakon Ob informatsyi, informatsyonnyh tehnologiiah i o zashite informatsyi 264-FZ" [Federal Law "On amendments in the law On information, information technologies and protection of information" nr. 264 -FZ]

Government of the Russian Federation (2004, August 22). Federalnyi zakon 122-FZ "Monetizatsiia lgot" [Federal Law nr. 122-FZ Monetization of social benefits]. Archived as a PDF copy on June 30, 2014

Government of the Russian Federation (2010, July 14). Federalnyi zakon 210-FZ, Ob organizatsii predostavleniia gosudarstvennyh i munitsypalnyh uslug [Federal Law nr. 210-FZ, The Organization and Provision of State and Municipal Services] archived as a PDF copy on June 30, 2014

Government of the Russian Federation (2017, July 28), Ukaz 1632, Programa tsyfrovaia ekonomika Rossiiskoi Federatsyi [Decree nr. 1632, Digital Economy of the Russian Federation Program], Retrieved August 15, 2017 from http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf

Ministry of Digital Development, Communications of the Russian Federation (2010, October 20) Gosudarstvennaia Programma "Informacyonnoie Obshestvo 2011-2020", [Government Program "Information Society 2011-2020"] https://digital.gov.ru/ru/activity/programs/1/#section-description

Moscow Government (1998, December 15) Regulation nr. 962 ПП Sozdaniie v Moskve Sistemy Beznalichnyh Raschetov za Tovary I Uslugi s Ispolzovaniem “Karty Moskvicha, [Creating cashless system in Moscow based on the Moscow Social Card”], archived as a PDF copy

Moscow Government (2002, February 5) Directive nr. 585-РП, Organizatsyia Moskovskogo Sotsyalnogo Registra, [The organization of Moscow Social Registry based on Moscow Social Card] archived as a PDF copy

Moscow Government (2014, December 16) Bylaw nr. 780-ПП, “The organization of the production, application and service of the Moscow Social Card”, [O vnedrenii Sotsyalnoi Karty dla Zhytelei Mosckvy], archived as PDF copy

Moscow Government (2014, November 18) Bylaw nr. 668- ПП “About production, distribution and servicing of social cards in Moscow” [O vnedrenii Sotsyalnoi Karty dla Zhytelei Moskvy], archived as a PDF copy

Moscow Mayor (2020, October 6) Decree nr. 97-УМ, About Updating Legal Acts of Moscow [O Vnesenii Izmeneii v Pravovyh Aktah Moskvy], https://www.mos.ru/upload/documents/docs/97-YM-fjlna.pdf

Russian President (2011, February 28) Komissiya po modernizacyi i technologicheskomu razvitii Rossii [Commission for Modernization and technological development of Russian economy] http://kremlin.ru/catalog/keywords/66/events/10453/audios

Security Council of the Russian Federation. (2016, December 12). Doktrina Informacyonnoi Bezopasnosti, [Doctrine of Information Security] https://rg.ru/documents/2016/12/06/doktrina-infobezobasnost-site-dok.html

2. Key stakeholders’ briefings/statements/speeches/presentations

Akimov, M. (2019, July 17) Soveshchanie pravitelstva RF “O vnedrenii elektronnogo udostovereniia lichnosti grazhdanina RF” [Government of the Russian Federation briefing on implementation of the national identification document for citizens of the Russian Federation] http://government.ru/news/37379/

Aliot’s CEO, Igor Vasil’yev (2013, March 19) Aliot – Unikalnost v Kazdoi Karte [Aliot – Uniqness in every card, An interview with the Aliot’s CEO], Journal Plus Nr. 3 (190) 2013. https://plusworld.ru/journal/section_1168/section_153900/art153879/

Gayev, D& Marchenko, A., (2003) Socialnaya Karta Moskvicha [Moscow Social Card], Information Society 1: pp. 77-78

President of the Russian Federation (2011) Zasedanie Komissii po modernizacii i tehnologicheskomu razvitii eknomiki Rossii. [Commission for Modernization and technological development of Russian economy]. Video is available on the official website

of the Russian President, http://kremlin.ru/events/president/news/10453 Retrieved on February 10, 2020

Medvedev, D. (2013, August 30) Plastikovaia Karta dla Rossiskih Grazhdan [Plastic card for Russian citizens] http://www.kommersant.ru/doc/2266546 Retrieved January 10, 2021

Medvedev, D. (2022, June 21) Komissia Soveta Bezopasnosti Rossiiskoi Federatsii po voprosam obespecheniia tehnologicheskogo suvereniteta gosudarstva. [Commission of the Security Council of the Russian Federation on the issues of the technological sovereignty of the state] http://www.scrf.gov.ru/news/allnews/3272/ Retrieved July 1, 2022

Popov (2015, June 2015) Bilingovye centry UEC zarabotayut v bolee chem 30 regionah [UEC centers will start operation in more than 30 regions] https://www.cnews.ru/articles/billingovye_tsentry_uek_zarabotayut

Russian Orthodox Church Statement (February 4, 2013) Pozicya Tserkvi v svyazi s razvitiyem tehnologiiy ucheta i obrabotki personalnyh dannyh [Russian Orthodox Church position on technological development of collection and processing of personal information], http://www.patriarchia.ru/db/text/2775107.html

3. Corporate websites, Corporate materials, industry publications, reports

CNews Russian internet portal (2015) UEC Technologii [Technological Innovations of UEC] https://uec.cnews.ru/ An archived website of the UECcard.ru

Department of Labor and Social Protection of Moscow Population (2020, June 15) Produkty, Veshi, Technika: Kak Stolichnyie semeinyie tsentry pomagayut moskvicham [Products, clothes, technology: how municipal service centers help Moscow residents] https://dszn.ru/press-center/news/3830

JSC UEC (2010) Godovoi Otchet [Annual report] Moscow 2011, archived as a PDF copy

JSC UEC (2011) Godovoi Otchet [Annual report] Moscow 2012, archived as a PDF copy

JSC UEC (2012) Oficyalny sait Universalnaya Electronnaya Karta [Official website of the Universal Electronic Card], discontinued and archived at https://web.archive.org/web/20130116094050/http://www.uecard.ru/

Kommunisticheskaia Partiia Rossiiskoi Federatsyi (KPRF) (2015, March 30) Elektronnoe obshestvo – ugroza perevoda Rossii pod vneshnee upravlenie [Communist Party of the Russian Fedration, Electronic society – a threat of the external control of the Russian society]. https://kprf.ru/dep/gosduma/activities/141186.html

Marchenko, A. (2005) Proekt “Sotsyalnaia Karta Moskvicha” [Project “Moscow Social Card”] Informational Society, 2, pp. 22-26.

Moscow Government Official Website (2014) Sotsyalnaia Karta Moskvicha [Moscow Social Card] https://www.mos.ru/karta-moskvicha/

Moscow Government Official Website (2014) Sozdana karta magazinov, v kotoryh predostavlyayutsia skidki po socyalnoy karte moskvicha [Map of stores with discounts for Moscow Social Card] https://data.mos.ru/News/Browse/39

Moscow Government Official Website (2014, March) Moskovski Sotsyalnyi Registr. "Novaia Karta Moskvicha" [The Moscow Social Register, "New Moscow Social Card"] http://www.soccard.ru/news/5404/

Moscow Government Official Website (2014, March) Novaia Karta Moskvicha [New Moscow Social Card] http://www.soccard.ru/news/5404/

Moscow Government Official Website (2017) Karta Moskvicha dla Sotrudnika MVD [Social card for MVD and police officers], archived as a PDF copy

Moscow Government Official Website (2020) Kak poluchit skidku po karte moskvicha v aptekah i magazinah. [Discounted services for MSC card holders] https://www.mos.ru/news/item/74273073/

Organizational Policy (2014, June) [The Moscow Social Registry Data Processing and Security Policy]. http://www.soccard.ru/articles/5455/

Rosan Finance (2003, November 18) Moscow Social Visa https://cardflash.com/news/2003/11/moscow-social-visa/

UEC JSC (2013, November) Godovoi Otchet. "Status i budusheie Universalnoi Elektronnoi Karty dla grazhdan Rossii" [Annual Report "Status and prospects of the Universal Electronic Card for Russian Citizens"] http://www.cnews.ru/reviews/ppt/forum_2013/plenum/10.Popov_Aleksey.pdf

Zaikin, A. (2013, October 29), Kontseptsyia Razvitia Electronnogo Bisnesa Banka Moskvy [Marketing presentation for the Board of Managers "The Bank of Moscow – directions of development of electronic business] https://prezi.com/-6e2t7l4t8ut/presentation/

4. Media interviews/journalists reports

Amos, H. (2011, July 4) "The Bank of Moscow gets a record bailout", The Moscow Times, http://www.themoscowtimes.com/business/article/bank-of-moscow-gets-record-bailout/439955.html

Ashychmin, A. & Agapov, I. (2011) Moskvichi pereplachivayut za metro, [Moskovites overpaying for the metro fares], Marker, archived as a PDF copy

Buranov, I. (2020) Ostorozno, socyalnyye karty zakryvayutsia.[Careful, Moscow Social Cards are closing down], *Kommersant* https://www.kommersant.ru/doc/4528323

Dement'yeva & Shestopal (2015, August 13) UEC ostalas bez glavy: Aleksey Popov pokidayet post i proekt, Kommersant https://www.kommersant.ru/doc/2787215

Dorokhov, R. (2003, December 23) Moskva po kartochkam Vlasti stolitsy vydaiut naseleniyu "sotsyalnyie karty" https://www.comnews.ru/content/23450

Filippov, S. (2012) "Emerging Russian multinational companies: Managerial and corporate challenges." *European Journal of International Management* 6, no. 3, pp. 323-341

Global Mass Transit Report (2011, April), "Social Cards in Russia: progress from regional to national", http://www.globalmasstransit.net/archive.php?id=6137

Il'yin D. (2014) "All Moscow in the mobile phone. The Moscow Department of Informational Technology has prepared a number of innovations." Published April 2014. Last accessed on May 2015, http://moscowtorgi.ru/news/informatcionny_gorod/865/

Interfax (2021, November 8) Sotsyalnuyu kartu v Moskve razblokiruyut v techenii 5 rabochih dnei posle privivki [Moscow Social Card is re-activated five days after vaccination] https://www.interfax.ru/moscow/801762

Ishkov, S. (2013, November) "There is an E-certificate instead of "Ration." Archived as a PDF copy.

Karpov, M. (2015, April 1) V Gosdume obsudili opasnost elektronnogo rabstva i lomku psihiki cherez computer [The State Duma discussed the danger of electronic slavery and a mental breakdown due to computers] https://lenta.ru/articles/2015/04/01/electrogulag/

Kork, A. (2020, October 10) Sotnyam moskvichey zablokirovali sotsyalnye karty,[Hundreds of Moscow Social Cards were blocked], Pravmir.ru https://www.pravmir.ru/dostup-zapreshhen/

Koshkina, Y. & Dziadko, T. (2014, December 20) Karta Grefa Bita: Pochemu ne poluchilsia proiekt s UEK http://www.rbc.ru/finances/10/12/2014/5486fad3cbb20fd6319a9f50

Krainova N., (2011) Luzhkov's Ouster Explained https://www.themoscowtimes.com/2011/10/26/luzhkovs-ouster-explained-a10430

Krasnikov (2013, February, 19) Universalnoy elektronnoy karte prikazali zyt ne bolee 5 let https://www.mk.ru/social/2013/02/19/814853-universalnoy-elektronnoy-karte-prikazali-zhit-ne-bolee-5-let.html

Krupin, A. (2013, October 23) Krupnym planom: universalnaya eletronnaya karta [A close look to the universal electronic card] https://3dnews.ru/770439

Larina E. & Ovchinsky V. (2013, December 5). Tsyfrovaia voina kak realnost [Digital War as a Reality]. Izborsk Club Retrieved June 30, 2014 from https://izborsk-club.ru/2321

Lenta.ru (2012) Gayev, Dmitri – Byvshyi Nachalnik GUP Moskovskoie Metro, [Dimitry Gayev – an ex-Head of the Moscow Metro] http://lenta.ru/lib/14162405/#20

Meduza (2022, June 13) Kak proshel den rossii v moskve reportaz meduzy https://meduza.io/feature/2022/06/13/hochetsya-chtoby-bylo-kak-pri-sssr

Ovchinsky V. (2017) "Slovo i Tsyfra". *Izborskii Klub. Russkie Strategii.* Tsyfrovaia Ekonomika i Virtualnaia Realnost. ["The word and "a digit". *Izborsk Club. Russian Strategies* n. 8 (54), 2017 Digital Economy and Virtual Reality]. Retrieved July 25, 2018 from https://izborsk-club.ru/magazine_files/2017_08.pdf

Sergina, Y. (2014, January 24) "There is no enough of Moscow Social Cards for all Moscow Residents." [in Russian]. Vedomosti nr. 3514 http://www.vedomosti.ru/newspaper/articles/2014/01/24/moskvicham-ne-hvataet-socialnyh-kart

The Moscow Times. (2019, April 19) Mir Card Payment System Looks Beyond Russia https://www.themoscowtimes.com/2019/04/19/mir-card-payment-system-looks-beyond-russia-a65311

Turovsky, D. (2015, March) "This is how Russian Internet censorship works. A journey into the belly of the beast that is the Kremlin's media watchdog" https://meduza.io/en/feature/2015/08/13/this-is-how-russian-internet-censorship-works

Voeikov, D. (2012, March 15) UEC vystoiala pod davleniem religioznyh aktivistov [UEC withstood pressure from religious activists] https://www.itweek.ru/business/article/detail.php?ID=137654

Yeremina & Tret'yak (2018, July 12) Sberbank perezapustit "Universalnuyu Elektronnuyu Kartu" https://www.vedomosti.ru/finance/articles/2018/07/12/775272-sberbank-universalnuyu-elektronnuyu-kartu

5. Websites, social media and other electronic content created by public

The Moscow Times. (2019, April 19) Mir Card Payment System Looks Beyond Russia https://www.themoscowtimes.com/2019/04/19/mir-card-payment-system-looks-beyond-russia-a65311

Banki.ru (2019, November 9) Otkrytie scheta bez moyego soglasiya https://www.banki.ru/services/responses/bank/response/10317771/

Cheboksary Religious Protest against UEC (2012, November 27) Religiozny miting protiv UEC: "My ne hotim byt electronnymi rabami", ["We don't want to be digital slaves"] https://moygorod.online/society/society_5598.html

Koordinacyinniy komitet protiv vnedreniya universalnoy elektronoy karty [Coordination Committee Against Universal Electronic Card] http://protivkart.com/

Lukatsky, A. (2010, August 19) Kak SberBank podvinul FSB v chasti kriptografii [How SberBank pushed over Federal Security Service (FSB) in regards of cryptography] https://lukatsky.blogspot.com/2010/08/blog-post_19.html

Lukatsky, A. (2011, March 1) Universalnaia Elektronnaia Karta pobedila FSB [Universal Electronic Card won over Federal Security Service (FSB)]

Marketing Youtube channel PressaUecard (2011) https://www.youtube.com/user/PressaUecard

Moscow protest against UEC (2011, August 23) Coordination Union Protiv Kart https://www.youtube.com/watch?v=p_3hjH7Z0M0

Orlov, D. (2012) O Pismah Galiny Tsarevoi prizyvaiushih borotsia s vnedreniem universalnoi elektronnoi karty. [Letters from Galina Tsareva calling for resistance to the Universal Electronic Card]. https://missia.me/o-pismah-galiny-tsarevoj-prizyvayushhih-borotsya-s-vnedreniem-universalnoj-elektronnoj-karty-svyashhennik-dmitrij-orlov/

Tsareva, G. (2013, April 2) Kruglyi stol po voprosu yuvinalnyh technologii i tsyfrovogo pokolenia. [Round Table on Juvenile justice technologies and digital generation] https://www.youtube.com/watch?v=UOi_KggLH0g

Tsareva, G. (2015) Era tehnotronnoi diktatury. [The era of technocratic dictatorship] https://www.youtube.com/watch?v=8YZq7OARAE0

Tsareva, G. (2018) Elektronnii Kapkan [Electronic Trap]. Retrieved July 30, 2019 from https://protivkart.org/main/12024-elektronnyy-kapkan-kniga-galiny-carevoy.html

Vasileva, J. & Medvedev V. (2017). Tendentsii razvitiia zakonodatelstva v sfere zashity personalnyh dannyh. Vestnik Rossiiskogo Universiteta [Tendencies in the development of the data protection regulation]. 2 (28), pp. 103-107.

Yakovleva, O. (2013), "Elektronnyie uslugi" ili privatizatsiia gosudarstva" ["Electronic services" or privatization of government]. Moscow, archived as a PDF copy

Yakovleva, O. (2014, January 8) Sroki polucheniia UEC i otkaza ot UEK. Obrashenie ob otkaze ot UEC. [Timeline of receiving and opting out from UEC. Application to opt-out from UEC], Archived as a PDF copy

Yakovleva, O. (2013, January) Elektronnoe Naselenie na Prodazu. [Digital Populataion for Sale]. *Rodina Pravoslavnaya* https://rodinaprav.info/index_php/novosti/100-elektronnoe-naselenie-na-prodazhu/