# Privacy, elections and political parties: Emerging issues

Colin J. Bennett

June 2013

# Privacy, elections and political parties: Emerging issues

As political parties in the US and Europe use ever more sophisticated targeting techniques, **Colin J. Bennett** asks what is the appropriate balance between privacy and the values of democratic education and participation.

The 2012 presidential election in the United States raised to public attention the general question of how political parties and candidates process and analyze personal data on individual voters. An incomplete summary of these techniques includes: extensive "voter management" databases; widespread use of personal data purchased from data brokerage firms; extensive use of robo-calling and robo-texting; smartphone apps that allow door-to-door canvassers instant access to voter histories; extensive uses of social media that allows for peer pressure or "targeted sharing"; and integrated campaign "toolkits" for website development, social media strategies, and political messaging.[1] These techniques permitted the "micro-targeting" of online and offline messages to more precisely defined categories of voters, especially in marginal states and districts.[2]

The range and sophistication of techniques in the US are staggering, and obviously facilitated by the absence of any general data protection law that applies to such data, as well as to a First Amendment that provides robust protections for freedom of communication and association. And of course, these techniques are facilitated by a permissive campaign financing system that generally places no restrictions on how much money individual candidates may spend on their election campaigns, or how much they may raise from individuals, groups or corporations.

We might find micro-targeting practices a little "creepy" – but the arguments on the other side of the debate are important and worthy of serious consideration. After all, political parties do have a democratic responsibility to educate voters about their positions and policies, and to mobilize voters. In an era of declining voter turnout, and membership in political parties in most Western democracies, perhaps micro-targeting should be embraced as a more effective and efficient way for parties to target their messages to those who are interested in hearing them. These issues raise a set of fascinating questions about the appropriate balance between privacy and the values of democratic education and participation.[3]

To what extent are the "micro-targeting" techniques entering the election campaigns of other democratic countries? And what are the implications for privacy laws and for the data protection authorities (DPAs)? Very little has been written about these issues in the privacy literature. And with few exceptions, DPAs have been reluctant to provide guidance to parties and candidates, and less still to regulate their activities. Furthermore, there are huge differences in electoral laws, financing provisions, voting systems and political cultures between the United States and parliamentary systems.

On the other hand, there is evidence that parties in other countries are drawing lessons from the American experience, and that similar techniques are gradually entering the politics of other countries. Back in 2005, the DPAs were sufficiently concerned about the use of new technologies to "establish direct and personalized contacts with vast categories of data subjects," about "invasive profiling" and about the unlawful collection of "sensitive data related to real or supposed moral and political convictions and activities" to issue a joint Resolution at their international conference in Montreux, Switzerland.[4] So how have voter surveillance issues arisen in countries outside the US?

## Canada: Complaints to DPA result in research

I begin with Canada. Neither the Canadian Privacy Act of 1982, nor the Protection of Personal Information and Electronic Documents Act (PIPEDA) of 2000 cover political parties because they are neither government agencies nor commercial entities; like some other non-profit entities, they fall between the cracks of the Canadian privacy regime. Nevertheless, the Canadian Privacy Commissioner has received a number of complaints about invasion of privacy by candidates and politicians going back several years. Partly in response, the office commissioned me to conduct a study on the subject, which concluded that the federal parties process an increasing amount of data on supporters, non-supporters, volunteers, candidates and employees.[5]

The issue has also achieved a prominence in the media as a result of a scandal involving the practice of "robo-calling" at the 2011 federal election. Voters in key marginal constituencies received automatic calls from an individual purporting to represent Elections Canada, and informing them (falsely) that their place of voting had changed. The "robo-call" scandal hit the front pages, and prompted investigations from the Royal Canadian Mounted Police and from Elections Canada.[6] The most interesting aspect of this affair is that only non-Conservative supporters were targeted, meaning that the individual must have had access to the voter management database operated by the Conservatives – the Conservative Information Management System (CIMs). The Chief Electoral Officer recommended that it was about time for the basic privacy principles within PIPEDA to be applied to political parties.[7]

### Australia: No guidance so far

Like Canada, the privacy laws of Australia also leave political parties unregulated. And like Canada, there have been a series of stories in the media about inappropriate communications with voters, about the non-consensual capture of personal data by parties and candidates, and about data breaches. In 2008, the Australian Law Reform Commission (ALRC) recommended that: "In the interests of promoting public confidence in the political process, those who exercise or seek power in government should adhere to the principles and practices that are required of the wider community. Unless there is a sound policy reason to the contrary, political parties and agencies and organisations engaging in political acts and practices should be required to handle personal information in accordance with the requirements of the Privacy Act." Before amending the law, however, the ALRC recommended "the Office of the Privacy Commissioner should develop and publish guidance to registered political parties and others to assist them in understanding and fulfilling their obligations under the Act."[8] To date, no such guidance has been issued.

### EU: Restrictions on sensitive data

So, what of the application of privacy law in Europe to political parties? Under the 1995 European Union Data Protection Directive, and under the new draft Regulation, political parties are clearly covered by data protection rules. There are a number of relevant provisions. I will cite the new wording in the new draft Regulation, as the rules are essentially the same.[9]

First data on political opinions is unequivocally defined as a "sensitive" form of personal data, which is generally prohibited unless: "processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other non-profit seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed outside that body without the consent of the data subjects" (Article 9(d)). Recital 36 reinforces this exemption in the case of political parties: "Whereas where, in the course of electoral activities, the operation of the democratic system requires in certain Member States that political parties compile data on people's political opinion, the processing of such data may be permitted for reasons of important public interest, provided that appropriate safeguards are established."

A plain reading of the law would indicate, therefore, that parties may only process political data on members, former members of on persons "who have regular contact." But what does this mean? Someone who attends meetings? Some who has friended the party on Facebook? And what of political communication that might be in the public domain – signs in windows, letters in newspapers, blog postings and so on? We convey explicitly and implicitly our political affiliations and preferences in an increasing number of contexts, and in a range of manners.

Does European law outlaw the kind of "voter management databases" common in North America? It is reported that the main political parties in the UK have operated such databases for several years, using similar proprietary software to their counterparts in the United States, and essentially augmenting the basic address information from the electoral roll with additional personal data on voters.[10] The Conservative Party has used the "Voter Vault" software named MERLIN (Managing Elector Relations through Local Information Networks).[11] The Labour Party now operates a system called Contact Creator.[12]

The Information Commissioner's Office has not ruled on the legality of such databases, but it did issue some guidance on the general question of political communication in 2005, as a result of a series of complaints about inappropriate telemarketing and particularly by individuals who objected to receiving calls from canvassers from parties they would never support.[13]

The French Commission Nationale de L'Informatique et Libertés (CNIL) provided similar guidance on political campaigning in 2012.[14] The CNIL also issued a more general set of decisions on the application of the data protection law to the range of party activities, including the construction of databases. Of particular interest in France was the recent innovation of a primary election for the presidential candidates for the French socialist party. "Open" primary elections pose particular problems for the application of data protection law to political parties. Voters from the general public may participate in the "internal" affairs of the party by selecting its candidate for the general election. Are such voters "regular contacts"? The CNIL struggled with this question and tried to balance the data protection law with the legitimate rights of association that parties claim.[15] Similar issues arose for the Italian Garante after primary elections for the center left coalition, Common Good, in 2012.[16]

Isolated examples of the inappropriate capture, use and disclosure of personal data by political parties and their candidates surface from time to time in other European countries. An initial survey suggests the following questions have required resolution:

1 Questions of intrusion – inappropriate communication by phone, e-mail, or text to people who have not given their consent, and who may be listed in respective "do-not-call" lists
2 The non-consensual capture of personal data by elected officials who come into contact with constituents in their capacities as electoral officials and communicate data on electors to their party headquarters
3 The logging of support or non-support by canvassers who may communicate data on political preferences in the course of election campaigning at the door, or over the telephone
4 The capture of data on political preferences through Facebook, Twitter and other social networking services
5 The capture of personal data through the inappropriate logging of cookies when the party website is visited.[17]
6 The use of membership lists for other organizations (churches, unions, clubs, schools etc.) used by candidates for political canvassing

7 Data breaches, especially when address information from the respective electoral roll is shared with party organizations at election time.

I predict that these, and other privacy issues, will become more prominent in the years ahead. The pressures for political parties to find more efficient methods to reach voters with their messages will increase as a result of social networking and other technologies, the influence of political consultants, the break down of traditional bases of support and the inherent competitiveness between parties within any political system. This brief survey suggests that the lessons from the United States have not been lost on their counterparts in many European countries, despite obvious and fundamental differences in data protection law, election rules, and political cultures.

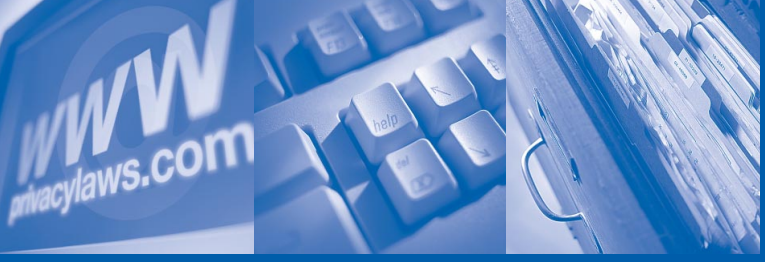
**AUTHOR**

Colin J. Bennett, Department of Political Science, University of Victoria, BC. Canada.
www.colinbennett.ca

Professor Colin Bennett will give the introductory thematic address at Bridging Privacy Cultures, *Privacy Laws & Business's* 26th Annual International Conference, at Queens' College, Cambridge 1-3 July.

**REFERENCES**

1 The best contemporary overview of these practices is: Sasha Issenberg, *The Victory Lab: The Secret Science of Winning Campaigns* (Crown Publishing, 2012).
2 Charles DuHigg, "Campaigns Mine Personal Lives to Get out the Vote," *New York Times*, October 13, 2012.
3 Colin J. Bennett, "What Political Parties Know about You," *Policy Options* (February 2013) at: www.irpp.org/po/archive/feb13/bennett.pdf?utm_source=Thinking+Ahead+February&utm_campaign=Thinking+Ahead+July+EN&utm_medium=email
4 International Conference of Data Protection and Privacy Commissioners, Resolution on the Use of Personal Data for Political Communication, Montreux, Switzerland, 16 September 2005.
5 Colin J. Bennett and Robin M. Bayley, Canadian Federal Political Parties and Personal Privacy Protection: A Comparative Analysis (Report to the Office of the Privacy Commissioner of Canada, March 2012) at: http://www.priv.gc.ca/information/research-recherche/2012/pp_201203_e.asp
6 Elections Canada, Preventing Deceptive Communications with Electors Chief Electoral Officer of Canada, 2013 at: http://www.elections.ca/res/rep/off/comm/comm_e.pdf
7 *Ibid*, p. 32
8 Australia Law Reform Commission, For Your Information: Australian Privacy Law and Practice, para. 41 at: www.austlii.edu.au/au/other/alrc/publications/reports/108/41.html#Heading25
9 European Union (EU). Proposal for a Regulation of the European Union and the Council on the Protection of Individuals with respect to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Published January 25, 2012. http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf
10 Amberhawk Training Ltd. "Could the Conservative Party's Electoral Database breach the Data Protection Act?" at: http://amberhawk.typepad.com/amberhawk/2013/03/could-the-conservative-partys-electoral-database-breach-the-data-protection-act.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+HawkTalk+%28Hawk+Talk%29
11 James Crabtree, "David Cameron's Battle to Connect" *Wired Magazine*, March 24, 2010 at: http://www.wired.co.uk/magazine/archive/2010/04/features/david-camerons-battle-to-connect
12 www.cfl.labour.co.uk/images/uploads/166988/9b6fc688-c195-be24-2db3-b7f130f35c08.pdf
13 UK Information Commissioners Office, Guidance for political parties for campaigning or promotional purposes (UK: ICO, 2005)
14 Commission Nationale de l'Informatique et Libertes (CNIL), Communication Politique: Obligations Legale et Bonnes Pratiques (Paris: CNIL, January 2012)
15 Commission Nationale de l"Informatique et Libertes (CNIL), Deliberation no. 2012-020 du Janvier 2012 portant recommendation relative à la mise en oeuvre par les partis ou groupements à caractère politique, eélus ou candidats à des fonctions électives de fichiers dans le cadre de leurs activités politiques.
16 Garante per la protezione dei dati personali, Elezioni primarie 2012 e trattamento di dati personali – 31 October 2012.
17 This became an issue in the Netherlands when some parties were found to be in breach of the Dutch law on cookies.




26 YEARS
1987-2013

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

# Art. 29 WP insists on narrow scope for purpose limitation

Purpose must be unambiguous and clearly explained. Relying on a new legal ground for processing is simply not enough to meet the compatibility test. By **Monika Kuschewsky**.

In early April, the Article 29 Working Party[1] published an important Opinion on purpose limitation,[2] one of the data quality principles contained in Article 6 (1) of the EU Data Protection Directive (the Directive).[3] The Article 29 Working Party regards this principle as "an essential condition to processing personal data" and "a prerequisite for applying other data quality requirements",[4] such as adequacy, relevance, proportionality and accuracy. The Article 29 Working Party even goes so far as to suggest that the "erosion of the purpose limitation principle would consequently result in the erosion of all related data protection principles".

The Opinion is relevant to all

*Continued on p.3*

# Do-Not-Track – US answer to privacy on the Internet

Protecting privacy should be as simple as asking "Do you wish websites to track you?" when upgrading or installing a browser – **Laura Linkomies** explains why this is not the case.

Do-Not-Track is being designed to let users block online "tracking" at the browser level, and specifically to address the issue of invisible third-party tracking. Users should, with Do-Not-Track technology, be able to opt out of tracking by websites they do not visit, including analytics services and advertising. The W3C (World Wide Web Consortium) had taken on a task to develop such technologically neutral Do-Not-Track standard, but had so far made slow progress. However, in its 6-8 May meeting, the Working Group adopted a consensus document, stating that there was sufficient progress

*Continued on p.5*

Issue 123 **June 2013**

**NEWS**

**2 - Comment**
The many faces of privacy

8 - DPAs monitor privacy policies

25 - Privacy issues and missing persons

28 - EU DPAs: BCRs for processors

32 - EU DPAs: Consent for Big Data

33 - Russia amends its DP laws • Spanish DPA issues guidance on cookies and cloud computing

34 - Singapore's Personal DP Act in force July 2014 • US Safe Harbor applies to cloud computing? • US COPPA amendments in force 1 July

35 - Apple's privacy policy breaches German DP law • Germany: Facebook data under Irish DP law • Ireland steps up its audit programme

**ANALYSIS**

**10 - Global data privacy laws 2013: 99 countries and counting**

**14 - Table of 99 countries with DP laws**

**20 - Table of 21 official DP Bills**

**24 - EU DP law harmonisation needed in employment field**

**26 - Privacy, elections, political parties**

**29 - Risks and benefits of CoE Convention 108 'modernisation'**

**LEGISLATION & REGULATION**

**9 - Dutch cookie law offers some relief**

**MANAGEMENT**

**8 - DPAs' 35th International Conference, Warsaw, Poland**

**22 - Mozilla's privacy policy via icons**

**33 - European DP: Coming of Age**

**35 - *PL&B's* 26th Annual International Conference, Cambridge, 1-3 July**

INTERNATIONAL report

ISSUE NO 123 **JUNE 2013**

**PUBLISHER**
**Stewart H Dresner**
stewart.dresner@privacylaws.com

**EDITOR**
**Laura Linkomies**
laura.linkomies@privacylaws.com

**ASIA-PACIFIC EDITOR**
**Professor Graham Greenleaf**
graham@austlii.edu.au

**REPORT SUBSCRIPTIONS**
**Glenn Daif-Burns**
glenn.daif-burns@privacylaws.com

**CONTRIBUTORS**

**Monika Kuschewsky**
Covington & Burling LLP, Belgium

**Gerrit-Jan Zwenne**
Bird & Bird, The Netherlands

**Berend van der Eijk**
Bird & Bird, The Netherlands

**Colin J Bennett**
University of Victoria, British Columbia, Canada

**Dugie Standeford**
*PL&B* Correspondent

**Monika Zalnieriute**
*PL&B* Correspondent

**PUBLISHED BY**
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
**Tel: +44 (0)20 8868 9200**
**Fax: +44 (0)20 8868 5215**
**Email: info@privacylaws.com**
**Website: www.privacylaws.com**

**Subscriptions:** The *Privacy Laws & Business* United Kingdom Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.

Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686

ISSN 2046-844X



# comment

## The many faces of privacy

In this issue, we bring you an updated table (p.14) of and commentary about 99 global privacy laws and 21 bills (p.10). The majority of countries will have enacted laws by 2014, predicts our Asia-Pacific Editor, Professor Graham Greenleaf, and almost all of the economically significant countries on the globe already have one.

The US "Do-Not-Track" proposal (p.1), prompted by congressional and consumer pressure, is making slow progress. The Federal Trade Commission proposed a legislative framework including a proposal for a Do-Not-Track mechanism in 2010 and now, in 2013, the Congress is saying that a solution has to be found soon or legislation will follow. Privacy icons are being developed (p.22) which provide a novel approach to offering users a simplified privacy indicator.

As the European Parliament's summer recess nears, it looks like the co-decision partners, the European Commission, the European Parliament and the EU's Council of Ministers are running out of time for creating a new EU DP framework (p.25). A leaked European Council Working Party on Information Exchange and Data Protection (DAPIX) document suggests that the rules may become less stringent for companies. One of the important issues in the revision is purpose limitation (p. 1).

France's DPA (the CNIL) is arguing the case for cementing privacy rights in France's Constitution and has asked the government to act. The CNIL has been critical about the EU draft Regulation's proposal for a Data Protection Board, as it would diminish the powers of national DPAs and multinationals could often find themselves regulated by the Data Protection Board. The European Data Protection Supervisor, when issuing his Annual Report on 29 May, said that 'according to the proposal DPAs in the relevant Member States will continue to be responsible for all cases, however, when there is an EU dimension, they will have to seek advice from the Data Protection Board. The current text of the proposal means that DPAs will follow this approach but it is a serious point of discussion in the Council and the European Parliament whether or not it will be an obligation.'

A free-trade agreement between the US and the European Union proposed recently by US President, Barack Obama, will pose more challenges for data protection. At the same time, the Council of Europe Convention 108, which is now expanding its scope to other regions, is being revised (p.29).

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

## Contribute to PL&B reports

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura.linkomies@privacylaws.com.

# Your Subscription **includes**

**1. Six Reports a year**
The *Privacy Laws & Business (PL&B) International* Report, published since 1987, provides you with a comprehensive information service on data protection and privacy issues. We bring you the latest privacy news from more than 100 countries – new laws, bills, amendments, codes and how they work in practice.

**2. Helpline Enquiry Service**
Subscribers may telephone, fax or email us with their questions such as: contact details of Data Protection Authorities, the current status of legislation and amendments, and sources for specific issues and texts.

**3. Email updates**
We will keep you informed of the latest developments.

**4. Index**
A cumulative Country, Subject and Company index is available at www.privacylaws.com/Publications/report_index/. Subject headings include Binding Corporate Rules, data breaches, data security, encryption, enforcement, sensitive data, subject access and transborder data flows.

**Electronic Option**
The Report is available, for an additional enterprise licence fee, in PDF format for uploading onto your Intranet or network. This format enables you to see the Report on any computer on your network as it appears in the paper version. It allows you to print out pages at any location.

*Privacy Laws & Business has clients in more than 50 countries, including 25 of the Global Top 50, 24 of Europe's Top 50, 25 of the UK's Top 50 in the* Financial Times *lists; and 10 of the Global Top 20 in the* Fortune *list.*

*Privacy Laws & Business also publishes the* United Kingdom Report, *a publication which ranges beyond the Data Protection Act to include the Freedom of Information Act and related aspects of other laws.*

# Subscription Form

## *Subscription Packages*

(VAT will be added for subscriptions within the UK)

**Single User Access**

❑ *PL&B International* Report Subscription **£500**

❑ *UK/International* Reports Combined Subscription **£800**

**Subscription Discounts**

Discounts for 2-4 users or 5-25 users

Number of years: 2 (10% discount) or 3 (15% )

**Go to www.privacylaws.com/subscribe**

Special academic rate – 50% discount on above prices – contact the *PL&B* office

**Subscription Includes:**

Six new issues of each report, on-line access to back issues, special reports, and event documentation.

**Data Protection Notice:** *Privacy Laws & Business* will not pass on your details to third parties. We would like to occasionally send you information on data protection law services. Please indicate if you *do not* wish to contacted by: ❑ Post ❑ email ❑ Telephone

Name:

Position:

Organisation:

Address:

Postcode: Country:

Tel:

Email:

Signature:

Date:

## *Payment Options*

Accounts Address (if different):

Postcode:

VAT Number:

❑ Purchase Order

❑ Cheque payable to: *Privacy Laws & Business*

❑ Bank transfer direct to our account:
*Privacy Laws & Business*, Barclays Bank PLC,
355 Station Road, Harrow, Middlesex, HA1 2AN, UK.
Bank sort code: 20-37-16 Account No.: 20240664
IBAN: GB92 BARC 2037 1620 2406 64 SWIFTBIC: BARCGB22
*Please send a copy of the transfer order with this form.*

❑ American Express ❑ MasterCard ❑ Visa

Card Name:

Credit Card Number:

Expiry Date:

Signature: Date:

*Please return completed form to:*
Subscriptions Dept, Privacy Laws & Business,
2nd Floor, Monument House, 215 Marsh Road,
Pinner, Middlesex HA5 5NE, UK
Tel +44 20 8868 9200 Fax: +44 20 8868 5215
e-mail: glenn@privacylaws.com 06/06

**www.privacylaws.com**

## *Guarantee*

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.