Big Data and privacy: why organizations adopt Big Data

You can only find truth with logic if you have already found truth without it.
– G. K. Chesterton (1905)

Introduction

Governments collect data with three general ends in mind: to deliver, to delve, and finally, to decide. The first of those processes is prosaic and often transactional. To provide citizens with services, benefits and tangible goods, government agencies frequently need information from individuals to determine what precisely is required and if they are eligible.[1] Accounting for programs and spending is important, as are due diligence and effective reporting. And each of those components is founded upon highly reliable, reviewable, structured data about where the data comes from (programmatically) and where it goes (individually).

The second role data plays – allowing governments to delve into and understand issues or scenarios that fall within its jurisdiction (as well as mapping out those which do not) – is equally fundamental.[2] As a result, particularly in the digital era, governments often err on the side of wider collection unless explicitly prohibited, availing themselves of new data sources even prior to having distinct questions they wish to answer or specific problems to solve. In this way, many organizations amass information as a form of insurance, just in case they should be tasked by the government of the day (or of tomorrow) to delve into some as yet uncircumscribed concern.

The third rationale for collection, arguably the ultimate impetus driving accumulation of data by government, is decision-making.[3] All forms and levels of government seek information to be (or at minimum to seem) decisive.[4] How public authorities collect, store, examine, leverage and share data[5] is a matter as current as today's headlines (e.g. what will the new government do about Bill C-51) and as old as government institutions themselves.[6]

The attraction of large-scale data collection by large public organizations then, is decidedly *not* new. Attempts to be universal and enumerative – in other words to go "Big" with data-collection is *not* new. Willingness to store and leverage data collected for all matters of state – *not* new.[7] So what is new about Big Data, and why do public sector organizations show such sustained interest?

Data's First and Second Waves

Politics, administration, justice have lost inaccessibility and secrecy in precisely the degree in which the individual has gained possibility of more complete privacy." – Georg Simmel (1906)

Meg Leta Ambrose, in a recent paper, neatly summarizes the recent prehistory of Big Data, mapping out the 19th c. rise of statistical reform movements across Europe.[8] To quickly recount, in the early 1800s, elites were confronted by a wave of urban crime, disease, poverty, unemployment, mental illness and unrest as industrialization spread and cities grew. Public institutions were caught hopelessly unprepared but social quantification and statistical analysis offered a kind of solution. Bureaus of statistics, scientific census methodology, modern economics and sociology all emerged around this time as tools to generate knowledge and direct reform.

The appeal of minutely surveying the state of the masses back then – the advent of bulk collection in its own right – is echoed in the appeals we hear now.[9] Systematic interrogation of widely collected data on criminality, industrial output, health factors, migration, employment and productivity would permit establishment of standards, enable feedback analysis to better control problem areas, produce more objective discussion and rigorous solutions, generate new knowledge and minimize exclusion (by requiring universal enumeration). Taylorism, actuarial science, cybernetics, traffic analysis, data mining, predictive analytics – each is another layer of technique that can be traced back to that Victorian-era push for data and the belief that it could help determine the best course of government intervention.[10]

No matter the scope of government's ambition for social reform in that era, there were always physical limits and analytical thresholds so long as paper records, segmented files and human minds remained the conduits and containers of information. The introduction of mechanization and automation into the data-processing effort – first mechanical tabulation, then calculation, then computation – set the stage for the first incarnations of techniques we would now associate with Big Data. Once reliable digital storage was developed – eliminating the limitations imposed by reference to paper records – the electronic database soon followed, the notion of metadata analysis, the spreadsheet … preprogrammed formulas allowed for automated calculus, algorithms could be applied and amended in real-time, distributions, trend analysis and pattern recognition produced almost instantly.[11]

Besides the application of such Big Data theory, the last piece to fall into place came as computerization spread from cloistered centres and headquarters to every corner of government. From junior clerk to senior Minister, every individual working in

the public sector is given over to the collection, input, examination, sharing and response to data. From a democratizing perspective, this is arguably a positive development.[12] Yet as a consequence, it is hard to imagine now how many public institutions would function at any level without their information systems, data platforms and electronic devices. For all alternatives to these channels in most quarters are simply gone, for better or worse.[13]

Data in seclusion, systems that forget

> *If we use, to achieve our purposes, a mechanical agency with whose operation we cannot efficiently interfere once we have started it, because the action is so fast and irrevocable that we have not the data to intervene before the action is complete, then we have better be quite sure that the purpose put into the machine is the purpose which we really desire and not a colorful imitation of it. – Norbert Wiener (1960)*

Having strayed from the original query – what is the appeal of Big Data for government – we should here return from another vantage. Classic theory of bureaucracy – via Weber, Simmel and others – give us some fairly clear points on why public authorities collect, protect, and in some essential ways, hoard information.[14] The obvious benefit is that data gives the officials within these organizations power: power over their own direction, influence over their future expansion, and leverage over institutional competitors.[15]

All these factors resound today as clearly as when Weber listed them almost a century ago.[16] In that vein, the pitch of Big Data to any information-intensive, self-protective, publicly-funded body is evident: we can help you do more with all the information you already have and do better what you already do. But there are less obvious realties inside government organizations that deserve discussion in connection with the appeal of digitization, data analytics and information-leverage.

One fact not readily discussed is many government agencies can be poor custodians of institutional knowledge or corporate memory.[17] And because of this, either through design or distraction, despite the vast sums of information they collect and store (or perhaps because of that methodology), public officials can often be seen in the media, before the legislature, or even in court quite unaware of what data exactly their organizations collect, for what precise purpose, or what practical guidance can be derived from such records.[18]

That is until some crisis or inquiry leads them to unearth the evidence they had all along but ignored, overlooked, misfiled, didn't translate properly, failed to share … and so it goes. Recent history is rife with these cases. And so just as Big Data

promises more purpose-driven foresight to bureaucrats, it also promises a kind of infinite recollection. Call it the "never again, never forget" claim.[19]

Finally, as a side benefit to Big Data, we should not leave out verification. The last bugbear of many bureaucratic structures and processes is not inconsistency, but anonymity. All modern government service, activity and programming is premised first on identifying, vetting and logging a client. From the most prosaic interaction to the most intrusive, however, there is always the potential for friction, pushback, or credential fatigue. The annoyance factor always looms, and when that dynamic creeps too high, government structures can suddenly find themselves stumbling politically.

Witness the cyclical backlash at various times against systems managing social welfare payments or claimant targets[20], airport and border screening practices[21], scrutiny of passport and visa applications.[22] Here again Big Data offers government some relief, primarily by promising to render aspects of identity validation invisible, to automate aspects of due diligence, to allow citizens the veneer of practical obscurity. For any operation tied to a public satisfaction metric, which is most services these days, rendering some of these mechanics more discrete can only be considered a selling feature for government.

If data's the answer, remind us of the question?

Big Brother no longer blares out of loudspeakers. Today Big Brother barely beeps. – Ursula Franklin (1993)

To be fair, there are truly some stubborn and pernicious public policy issues where Big Data techniques show real promise; these societal risks are pressing ones and new technologies could affect real improvement. Public health authorities point to better control of infectious disease[23], energy utilities to gains in conservation[24], environmental scientists demonstrate more accurate climate models, urban planners show new insight into traffic and transit patterns.[25] These are each highly complex systems, as variables within them are persistently intertwined, so that a better range of sensors and sources can aide analysis. This is Big Data's promise.

Given the massive spectrum of human intervention merged with natural phenomena, using large datasets fed by remote sensors or networked information streams, there are whole array of contexts where sophisticate analysis could be applied quite free of controversy. Species conservation, infrastructure monitoring and protection[26], meteorological work, supply-chain management, transportation networks[27], agriculture, and waste management – each is an obvious, perennial concern of government where citizens have high expectations and real benefits could follow from improvements in data collection and analysis.

Yet these regulatory areas of intervention, at least in Canada, do not seem to have attracted major investment to date. Where Big Data has been targeted instead by government is at people and their behaviours.[28] Granted Statistics Canada, Revenue Canada, and other agencies have been sophisticated data gathers for decades (for the very reasons noted at the outset), but Big Data techniques arise from a new set of largely *automated* tools and *predictive* techniques that set them apart.

These new analytics applications are so powerful because they draw in a myriad of sources and data streams. They can incorporate feedback, errors and unpredictable observations almost instantly. And they can produce sophisticated models to extrapolate anomalies that may require intervention. Whether it has been to map suspicious financial transactions, detect intrusion attempts of government systems, or assess security risks of people coming to or leaving the country, it would be inaccurate to say Canada has somehow overlooked use of Big Data in government. Rather, one could note it has been adopted quite discretely, with little fanfare, with quite intentional circumspection.[29]

Dilemmas from data

> *A world of informational transparency will necessarily be one of deliriously multiple viewpoints, shot through with misinformation, disinformation, conspiracy theories and a quotidian degree of madness. We may be able to see what's going on more quickly, but that doesn't mean we'll agree about it any more readily. – William Gibson (2003)*

Besides the securitization of data use, another obvious reality that confronts organizations is that the amalgamation of ever-larger datasets, connected to ever-broader networks and systems, has in point of fact created new risks both for state interests and privacy.[30] As organizations compile and combine more elaborate and exhaustive repositories of personal information, open up network access to these files for internal government applications and analysis, and make these data-sets "mission critical" it should be objectively apparent (just by dint of their size) that they will become probable targets of snooping, theft, hacking and/or surveillance.[31] For even the most technically-advanced and well-funded organizations in the world like multi-national tech conglomerates or globalized intelligence agencies seem unable to foil persistent attackers or detect terabytes of data being pulled off their networks.[32]

Yet even now, Big Data analytics is recursively suggested as the solution to the very security problem its models helped create by leveraging over-collection. Agencies amass new security data in the hope of better protecting the vast registers of information they already store. More active monitoring becomes the solution as government data losses deplete institutional reputation and community trust. Where

exactly this vortex of circular logic will deliver us as citizens, or our countries and institutions, remains to be seen.[33] But nowhere in the data-points or trend-lines can one detect either more meaningful security of the person or essential privacy.

Finally, there is the question of seeking the views of citizens themselves. To be clear, there is no positive right to exert when it comes to many functions of government. One cannot opt-out of passport requirements, tax returns, social insurance registries or census instruments. Still, that single factor does not relieve public sector bodies of other obligations. Assuming viable legal authorities even exist, any accountable organization should demonstrate transparency *before* the capture, use, sharing and storage of public information is redeployed through Big Data approaches. They should have sought, heard and weighed input by those affected, whether one refers to social licence, consent of the community, elected mandate or simply citizen input.[34]

Conclusion

Taking the wider social view, citizens of many developed states have historically shown a resilient attachment to guarding aspects of their private lives, even in the face of government or commercial practice. People – free ones in any case – will always need and hopefully demand some measure of respect for their thoughts, individuality and personhood. They will demand from governing authorities some essential recognition of their rights. They'll even exert agency of their own to protect themselves and their data.[35]

But citizens should not feel so exposed to scrutiny that they feel the need to cloak themselves from the state; on the issue of public trust, many would argue that government institutions and commercial organizations both need to act more responsibly. When it comes to technological data-gathering, one concern is that basic rights have become – in an age of invisible networks and ubiquitous sensors – very expensive to exert, or that privacy requires in effect self-isolation and active disconnection to maintain.[36]

Returning to the promise of data, to conclude, clearly potential exists for better analysis and benefits to society. As noted above, in many complex areas of public policy, deeper understanding of phenomena is crucial. But this forensic, data-driven capacity cannot be deployed without serious consideration – especially where the objects of study are people and their futures are being shaped and nudged by the insights gleaned. The deeper ripple effects - upon individuals, their freedoms and the tenor of their communities and societies - as information accumulates and mirrors back at us, also deserve a hard, critical look.

Side-note: privacy as an ethical and legal threshold

Many experts and commentators have argued recently that the use of Big Data approaches – especially in the security and intelligence context – requires strict legal controls.[37] Not constraints by administrative policies, not internal bureaucratic mechanisms, not senior management sign-off, not retrospective evaluations. None of those methods have demonstrated that agencies can police themselves or constrain the threat of misuse.[38] As in statute governing use of electronic surveillance by police in Canada, what many argue is required instead are concrete barriers, plain prohibitions, and serious penalties.[39] Whatever one thinks of the severity of these "hard limits", they clearly show it possible to treat the inappropriate use and sharing of sensitive information with serious legal consequences.[40] So why have Big Data practices receive no such attention?[41]

That privacy somehow ceased to be an important social value or legal right (call it the "privacy is dead" argument) seems imprecise; taking Canada alone, in the period noted above, official numerous Commissions of Inquiry investigated and documented invasions and abuses by federal authorities.[42] That the question somehow dissipated from view as a political priority or matter of law is similarly inaccurate; through the 1980s and 1990s, legislatures and courts deliberated over an unending string of cases, breaches and controversies tied up with surveillance and privacy.[43] From the 1970s onward, it is worth noting, information-processing services and computer equipment sales to public sector organizations rose dramatically in nearly every jurisdiction and level of government across the developed world.[44]

At the same time, in the private sector, personal information itself was transformed.[45] Where already in the public domain, but not digitized, it became a commodity for resale. Where private and individualized, it became a key data-point in marketing and customer relations. In either case, taking that view of information-as-asset tended to set privacy rights against a whole set of other market assumptions and cast personal information as an "economic sink", hurdle to "innovation", barrier to trade, and so forth.[46]

Still placing barriers between data sets, setting limitations on their use, fixing ground rules for sharing, and ensuring individuals have some measure of access – all figured into legal provisions passed in the 1970s and 1980s, precisely to constrain plans to centralize and cross-reference personal data using computers.[47] Glossing over the constitutional status of privacy protection - to say nothing of its foundation as a human right, personal ethic or its social value – tends to lead policy-makers to a reductive, asset-based view of information that remains prevalent to this day.[48]

Endnotes and sources

[1] This sounds simplistic, to the point of inconsequential, but when considers that such outlays represent almost 63% of the entire federal annual budget – a sum approaching $280 BN a year – the complexity and importance of rigor becomes evident. See Receiver General of Canada, *Consolidated Statement of Operations and Accumulated Deficit for the Year Ended March 31, 2015* - http://www.tpsgc-pwgsc.gc.ca/recgen/cpc-pac/2015/vol1/s2/efc-cfs-eng.html#b1

[2] Complex social, economic and environmental issues crop daily, often at quite a distant remove from centralized government decision-makers. Even with excellent records and long-term historical data, authorities of broad federal states or dispersed territories can easily overlook issues on the horizon, especially when they are preoccupied with more localized crises. For numerous examples from the experience of the British Empire, see James R. Beniger, *The Control Revolution: technological and economic origins of the information society* (1986), Peter J. Hugill, *Global Communications since 1844: geopolitics and technology* (1999) and Hugh Barty-King, *Girdle Round the Earth: the Story of Cable and Wireless* (1980)

[3] Historically, a great many states have come and gone that provided effectively no services or material benefits to their citizens (nor even really cared to know much about them); despotism is, at day's end, still a form of government. Similarly, many forms of government have existed and ruled which retained no written record, or worse actively destroyed what historical data was available; for post-revolutionary purging was also a fairly common theme in the 19th and 20th centuries. See Federico Baez, *Universal History of the Destruction of Books* (2008) or Lucien Polastron, *Books on fire: destruction of libraries throughout history* (2007) or Rebecca Knuth, *Burning Books and Levelling Libraries* (2006)

[4] That constant call upon all governments, to respond and react to direct petitions, has set the tones of its advisors throughout the ages, who will tend to borrow from Thomas Hobbes, Sun Tzu, Machiavelli or Foucault interchangeably on the "power of knowledge".

[5] Whether it is branded knowledge transfer, intelligence-fusion, information-sharing or records disposition is a specialist sub-species of the question, principally information studies. See Thomas Gleick, *The Information: A History, a Theory, a Flood* (2011) or Mark Stefik, *The internet Edge: social, legal and technological challenges for a networked world* (1999)

[6] Ian McLeod, "Liberals planning swift overhaul of controversial Anti-terrorism Act, Bill C-51", National Post (October 22, 2015) – URL: http://news.nationalpost.com/news/canada/canadian-politics/liberals-planning-swift-overhaul-of-controversial-anti-terrorism-act-or-bill-c-51 ; AAAS, *Ancient History, Modern Destruction: Assessing the Status of Syria's Tentative World Heritage Sites Using High-Resolution Satellite Imagery* – URL: http://www.aaas.org/page/ancient-history-modern-destruction-assessing-status-syria-s-tentative-world-heritage-sites-7#Ebla

[7] Roman census-taking, the Doomsday Book, the archival excess of East Germany were all such precursors.

[8] Meg Leta Ambrose, "Lessons from the Avalanche of Numbers: Big Data in Historical Perspective" from *I/S: A Journal of Law and Policy for the Information Society* (February 2016) – URL: http://moritzlaw.osu.edu/students/groups/is/files/2016/02/6-Ambrose.pdf

[9] For example, *Big Data at Shared Services Canada* (June 2015) – URL: http://ssc-spc.gc.ca/pages/itir-triti/pdf/afac-big-data-at-ssc-eng.pdf; see also ICTC, *Big Data and the Intelligence Economy* (2015) – URL: http://www.ictc-ctic.ca/wp-content/uploads/2015/12/BIG-DATA-2015.pdf

[10] Gordon Corera, *Intercept: the Secret History of Computers and Spies* (2015)

[11] Albert Borgmann, *Holding on to reality: the nature of information at the turn of the millennium* (1999) and Peter Hall, *The Carrier Wave: New Information Technology and the Geography of Information* (1988)

[12] Gabriella Coleman, *Hacker, Hoaxer, Whistleblower, Spy* (2014)

[13] Katherine Marshall, "Working With Computers" Perspectives on Labour and Income (May 2001) – URL: http://www.statcan.gc.ca/pub/75-001-x/00501/5724-eng.html

[14] Peter Gill, *Policing politics: security intelligence and the liberal democratic state* (1994)

[15] See Georg Simmel, "The Sociology of Secrecy" (1906) from *Government Secrecy* (2009); see also discussion more broadly on government use of data in David Lyon, *The Electronic Eye* (1994), 41-46.

[16] More information also attaches to agencies the public power of expertise and indispensability; see Max Weber, "Bureaucracy" from *Essays in Sociology* (2009), p. 196 – 244, or *Max Weber and the theory of modern politics* (1974)
[17] To borrow a trope from pop psychology, we might say many public authorities have "self-identities" that seem "poorly integrated." In effect, government bodies very often forget as quickly as they collect. This obviously stymies effective administration, in so much as constant watching becomes a replacement for more effective memory. Ultimately, one or the other is an imperative of modern government. See Christopher Dandeker, *Surveillance, power and modernity* (1990)
[18] Michael Isikoff, "NSA program stopped no terror attacks, says White House" *NBC News* (December 20, 2013) –URL: http://www.nbcnews.com/news/other/nsa-program-stopped-no-terror-attacks-says-white-house-panel-f2D11783588
[19] This has serious appeal in the corridors of government, for if there is one sin in public service existence which is truly grave and inexcusable, it is the repetitive human tendency to forget. Granted, at root, the entire point of a bureaucratic system of records is ensure continuity of operation and preserve memory; see Hessel Tolzmann, *The Memory of Mankind: the story of libraries since the dawn of history* (2001)
[20] "Welfare computer woes cost Ontario millions in overtime", *Toronto Star* (December 29, 2014) – URL: http://www.thestar.com/news/queenspark/2014/12/19/welfare_computer_woes_cost_ontario_millions_in_overtime.html
[21] CBC, "Does racial profiling exist at the Canada-U.S. border?" (November 20, 2014) – URL: http://www.cbc.ca/news/canada/toronto/does-racial-profiling-exist-at-the-canada-u-s-border-1.2843758
[22] CBC, "Biometric data collection change in budget bill raises privacy concerns" (June 3, 2015) – URL: http://www.cbc.ca/news/politics/biometric-data-collection-change-in-budget-bill-raises-privacy-concerns-1.3095488
[23] Dion M, Abdel-Malik P, Mawudeku A, "Big Data and the Global Public Health Intelligence Network" C*anada Communicable Disease Report* (September 2015) – URL:: http://www.phac-aspc.gc.ca/publicat/ccdr-rmtc/15vol41/dr-rm41-09/assets/pdf/15vol41_09-eng.pdf
[24] Micheal Fitzgerald, "Big Data cutes buildings energy use" *Wall Street Journal* (Sept. 28, 2014) – URL: http://www.wsj.com/articles/big-data-cuts-buildings-energy-use-1411937794
[25] Steve French, Camille Barchers and Wenwen Zhang, "Moving beyond Operations: Leveraging Big Data for Urban Planning Decisions" (MIT, 2015) – URL: http://web.mit.edu/cron/project/CUPUM2015/proceedings/Content/pss/194_french_h.pdf
[26] Ted G. Lewis, *Critical Infrastructure Protection in Homeland Security: defending a networked nation* (2015)
[27] *Big Data's Implications for Transportation Operations: An Exploration* (December 2014) – URL: http://ntl.bts.gov/lib/55000/55000/55002/Big_Data_Implications_FHWA-JPO-14-157.pdf
[28] Transparent Lives : Surveillance in Canada (April 2014) – URL: http://www.aupress.ca/index.php/books/120237 ; see also http://www.surveillanceincanada.org/
[29] See Mark Andrejevic, *Infor-glut: how too much information is changing the way we think and know* (2013), also Jim Bronskill, "Canadian security agencies urged to embrace big data crunching despite privacy concerns" Toronto Star (November 2015) – URL : http://www.thestar.com/news/canada/2015/11/12/federal-security-agencies-need-to-embrace-big-data-crunching-or-risk-failing-to-foresee-threats-warns-internal-report.html
[30] Risks of intrusion, risks of theft, risks of loss, risks of abuse, risks of unintended use and consequences – one can cite here a litany of cases from the data protection context alone – Google Street View and their amassing of wireless network data, the succession of hacks into Sony's PlayStation Network, the data losses of HRM in the UK or the breach of the US Office of Personnel Management (OPM). On this last incident, see the report of the Congressional Research Service, "Cyber Intrusion into U.S. Office of Personnel Management " (July 2015) – URL: https://www.fas.org/sgp/crs/natsec/R44111.pdf and "OPM – the worst hack of all time," *Computerworld* (June 29, 2015) – URL: http://www.computerworld.com/article/2941754/data-security/opm-the-worst-hack-of-all-time.html
[31] See Simon Chesterman, *One Nation Under Surveillance: a new social contract to defend freedom without sacrificing liberty* (2010)

[32] See Glenn Greenwald, *No Place to Hide* (2014) and Zack Whittaker, "2015's biggest hacks, breaches" *ZDnet* (January 2016) – URL: http://www.zdnet.com/pictures/biggest-hacks-security-data-breaches-2015/

[33] Past experiences with precisely this dynamic loop of surveillance and institutional mistrust would indicate the direction of governmental relations and political distemper would not be healthy for public debate. See Penney, Jon, Chilling Effects: Online Surveillance and Wikipedia Use (2016) *Berkeley Technology Law Journal*, 2016. Available at SSRN: http://ssrn.com/abstract=2769645 or Christopher H Pyle, "Political data banks and civil liberties" in *Surveillance and Espionage in a Free Society* (1972)

[34] Whether that is via public consultation, or Parliamentary debate, many organizations view such processes as daunting in that they can yield limited consensus and uneven quality of feedback. Nor are particular outcomes to be assured or a judgment of inclusiveness necessarily always reached. But even then, the risk of serious government IT projects running afoul on both privacy violations and undemocratic processes would seem to be pitfall most elected officials would care to avoid. Examples detailed by Liberty, "The Case Against ID Cards" – URL: https://www.liberty-human-rights.org.uk/human-rights/privacy/id-cards/case-against-id-cards; Oxfam, *Community Consent Index 2015* – URL: https://www.oxfam.org/sites/www.oxfam.org/files/file_attachments/bp207-community-consent-index-230715-en.pdf; BSR, *Engaging with Free, Prior and Informed Consent* (September 2012) – URL: http://www.bsr.org/reports/BSR_Engaging_With_FPIC.pdf; for counter-argument to hearing community views, see Jeffery Simpson, "Define consultation and social licence" *Globe and Mail* (October 22, 2014) – URL: http://www.theglobeandmail.com/opinion/define-consultation-and-social-licence/article21199386/

[35] Bruce Schneier, *Data and Goliath: the hidden battles to collect your data and control your world* (2015)

[36] Hardened, encrypted smartphones are by no means cheap, nor is living offline practical, for most citizens. The legal and technical knowledge required is equally formidable. No matter one's personal inclination toward proxies, encryption, scrambling or anonymization, the idea that all this and more will be required in the future to protect individual privacy of the next generation seems regressive.

[37] For example Ian Leigh, *In from the Cold: national security and parliamentary democracy (1994),* Susan Landau, *Surveillance or security: the risks posed by new wiretapping technologies* (2010), David K. Shipler, *Rights of the People: how our search for safety invades our liberties* (2011), Daniel Solove, *Nothing to Hide: the false trade-off between privacy and security* (2011)

[38] Basically, experience shows that arguments of expedience, exigence or efficiency always win out over privacy or legal restraint. See Laura Donohue, *The Future of Foreign Intelligence: Privacy and Surveillance in a Digital A*ge (2016)

[39] That such measures are possible is easily demonstrated, for we have had them in place through Parliamentary enactment (since 1939) for the protection of government information, and have updated the federal statute for official secrets half-a-dozen times since. Unauthorized disclosure of classified information can result in prison sentences up to 14 years; breach of trust alone is punishable by two years in prison. Similarly, under our telecommunications law and *Criminal Code* companies can face sharp, escalating fines for non-compliance with investigative orders (up to $250,000). For counter-argument see Richard A. Posner, "On being overinvested in law as a weapon against terrorism" from *In the Balance: the administration of justice and national security in democracies* (2008)

[40] Stanley A. Cohen, "Freedom of Information and the Official Secrets Act" *McGill Law Journal* (vol. 25, 1979), 99-110 – URL: http://lawjournal.mcgill.ca/userfiles/other/7099188-cohen.pdf

[41] Put another way: Why are practices amounting to bulk collection permitted? What spurred Canadian and US lawmakers to so rigorously protect the private communications of postal mail and voice calls in the 1970s, only to weaken protections a generation later as electronic mail emerged? Why was there clear political consensus at one point for very strong laws (wiretapping prohibitions), less so a generation later (federal privacy statues), and almost zero interest in the question over the past decade?

[42] With our *Canadian Charter of Rights and Freedoms* being enacted as a consequence; see Commission of Inquiry Concerning Certain Activities of the RCMP, *Freedom and Security under the Law* (1981), also Stanley A. Cohen*, Invasion of privacy: police and electronic surveillance in Canada* (1983)

[43] One might then conclude the data practices of large organizations have not attracted in-depth regulation because it is too technical (i.e. difficult to legislate), too abstract (i.e. uninteresting to examine) or too lucrative (i.e. might curtail the public purse). This last possibility, tied to the economics of

information, is in the end the most convincing. See Shawn M. Powers and Michael Jablonski, *The Real Cyber War: the political economy of internet freedom* (2015)

[44] Parliament (UK) Public Administration Committee - Government and IT- "A Recipe For Rip-Offs": Time For A New Approach – URL: http://www.publications.parliament.uk/pa/cm201012/cmselect/cmpubadm/715/71502.htm; OECD, Information Technology Outlook 2010 - Recent Developments and Outlook – URL: http://www.keepeek.com/Digital-Asset-Management/oecd/science-and-technology/oecd-information-technology-outlook-2010/recent-developments-and-outlook_it_outlook-2010-3-en#page29 and *Rethinking e-Government Services: User-Centred Approaches* (2009) – URL: http://dx.doi.org/10.1787/9789264059412-en

[45] Hamilton Bean, *No more secrets: open source information and the reshaping of US intelligence* (2011)

[46] For example, World Economic Forum, *Rethinking Personal Data* (2012) - http://www3.weforum.org/docs/WEF_IT_RethinkingPersonalData_Report_2012.pdf

[47] That led to the first generation of privacy law in North America. Given computational power in our current era, and what is to come, one would think legislators would be scrambling to revisit and reinforce those limits, not carve out more exceptions to their application or set up new loopholes for government investigators. See Rahul Sagar, *Secrets and leaks: the dilemma of state secrecy* (2013), and see Gary T. Mark, "Coming to terms and avoiding information techno-fallacies" from *Privacy in the Modern Age: the search for solutions* (2015)

[48] Nowhere is this more notable than among many scientists, business people, elected officials and bureaucrats, as documented well by both Cesar Hidalgo, *Why Information Grows: evolution of order from atoms to economies* (2015) or Andrew Keen, *Digital Vertigo* (2012)