What's New Again?
Security Measures Must Be Real – Not Illusory

A Commentary by Ann Cavoukian, Ph.D.

Ann Cavoukian, Ph.D.
Information and Privacy
Commissioner of Ontario

In September 2001 – immediately after the devastating events of 9/11 – I was asked by the CBC to comment on the likely impact on privacy that the heightened government emphasis on assuring public security may result in. My remarks were published on my website.[1]

I described a future world of dramatically increased state powers to collect, use and disclose growing volumes of detailed personal data, from more and more sources, using increasingly technological and automated means, in an effort to identify and catch terrorists, and to secure our physical spaces against future attacks. I predicted a world of enhanced state powers to deploy controversial new technologies of identification and to expand surveillance activities to an unprecedented scope and scale.

These efforts, I predicted, would have profound consequences for human rights and civil liberties, especially privacy.

I warned that the security gains of such activities needed to be real and not illusory, and that whatever the measures taken by the state, they had to be effective, or else the price of the perception of enhanced security – in terms of individual freedoms and civil liberties – would be too high to pay.

I warned against overly broad or illegitimate purposes, and the need to ensure that new intelligence technologies were deployed in a manner consistent with those objectives, and not beyond. I warned about "drowning in a vast sea of electronic data collected" and against over-reliance on technology as a silver bullet, insisting upon greater emphasis being placed upon the human element of intelligence gathering – eyes on the ground.

I called for informed public debate on the existence and extent of covert and privacy-invasive intelligence gathering measures.

I pressed to preserve the responsibility of law enforcement officials to protect the confidentiality of personal information collected against excessive sharing, secondary uses, misuse or loss. In this climate of public fear and patriotic duty, I also reminded businesses of their responsibility to protect the personal information of their customers and to safeguard their hard-earned trust against unnecessary erosion.

Since then, I have continued to monitor developments in state powers of surveillance under the guise of ensuring national security -- and their impacts upon individual privacy. In early 2003, I authored an extensive report documenting the various national security initiatives undertaken and their impacts upon information privacy rights.[2] In it, I offered recommendations for restoring a sense of balance.

In the intervening years, I have taken public positions on a wide range of public security-related issues such as the creation, deployment and use of identification cards and systems, surveillance and "lawful access" and other information-gathering proposals and technology-related initiatives. I have consistently advocated for innovative positive-sum, "win-win" solutions that minimize privacy invasion to an absolute minimum while promoting successful operational objectives and outcomes.

I was reminded of all of this by a recent paper by Professor Fred Cate and Newton Minow on government data mining.[3] The paper surveys the extent to which U.S. government data-mining activities are taking place in order

to combat terrorism, and how utterly ineffective they have been in achieving their objectives. It goes on to describe the profoundly troubling impacts upon privacy of the large-scale collection, use and dissemination of detailed personal information of millions of individuals by U.S. intelligence and law enforcement agencies. It is an excellent paper that is well worth reading.

Problems arise from misidentifying individuals in data-matching systems, and from the faulty algorithms that seek to match personal data, profile individuals, predict their behaviour, and trigger automated decisions that affect their freedoms. Significant problems also arise from the large-scale harvesting of personal data and decisional support from private-sector sources by the state. The worst part is that these privacy-invasive activities not only show little promise of being demonstrably effective, but they fail to apprehend the real suspects.

Professor Cate's conclusions are worth quoting in full: "Government data mining can pose a variety of risks to individuals and institutions alike. Those risks include the infringement of legally protected privacy rights; undermining national security by targeting innocent individuals, failing to identify real suspects, or otherwise misfocusing scarce resources; creating liability for businesses and others that provide, or fail to provide, the government with requested data, or otherwise fail to comply with often detailed and burdensome laws; and interfering with transnational data flows or subject U.S. companies to liability under foreign national laws.

> "These and other risks are exacerbated by the escalating pace of technological change … [T]echnological innovation is leading to less expensive storage capacity for digital data, cheaper and more advanced tracking technologies, steady advances in computer processing power, and increased standardization in data formats. Taken together, these developments mean that more personally identifiable data will be created and stored, they will be easier to access, and it will be increasingly possible to aggregate and match them quickly and affordably. The privacy and other risks associated with government data mining will increase as information technologies develop."

Words well spoken. These are indeed the challenges that we collectively face, more urgently than ever, and which we must face together in an engaged and constructive manner. In Professor Cate's words, we now live in a world of "ubiquitous data availability," requiring new solutions. We propose that we change the paradigm from zero-sum to positive-sum. See our papers on transformative technologies[4] and radical pragmatism.[5]

Ann Cavoukian, Ph.D.

---

[1] *Public safety is paramount - but balanced against privacy*: www.ipc.on.ca/index.asp?navid=46&fid1=255

[2] *National Security in a Post-9/11 World: The Rise of Surveillance … the Demise of Privacy?*: www.ipc.on.ca/images/Resources/up-nat_sec.pdf

[3] Cate, Fred H. and Minow, Newton, *Government Data Mining* (July 08, 2008). MCGRAW-HILL HANDBOOK OF HOMELAND SECURITY, 2008. SSRN: http://ssrn.com/abstract=1156989

[4] *Transformative Technologies Deliver Both Security and Privacy: Think Positive-Sum not Zero-Sum,*: www.ipc.on.ca/images/Resources/trans-tech-handout_098824173750.pdf

[5] Privacy & Radical Pragmatism: Change the Paradigm: http://www.ipc.on.ca/index.asp?navid=67&fid1=89

See also:

- National Research Council, Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals: *Data-based Counterterrorism Programs Should be Evaluated for Effectiveness, Privacy*, (October 7, 2008) at: www.nationalacademies.org/morenews/20081007.html

- Solove, Daniel J., Data Mining and the Security-Liberty Debate. GWU Law School Public Law Research Paper No. 278. SSRN: http://ssrn.com/abstract=990030