

ICJ Eminent Jurists Panel on Terrorism, Counter-Terrorism and Human Rights
April 25, 2007 (Ottawa)

Arthur J. Cockfield, Queen's University Faculty of Law
art.cockfield@queensu.ca

Summary of Oral Submissions

My submissions will touch on three areas:

1. an international survey of anti-terrorism laws and privacy concerns in the post-9/11 environment;
2. an assessment of Canadian legislative and enforcement reaction to 9/11 developments; and
3. the need to protect the 'social' value of privacy in an era of rapidly changing surveillance technologies.

1. International Survey on Privacy and Personal Data Flows

From 2004 to 2006, the Queen's Surveillance Project prepared and commissioned an international survey of residents of seven countries to help study the policy impact of cross-border transfers of personal information in an era of enhanced government surveillance. This was the first cross-national study of its kind that surveys attitudes to and experiences with the global flow of personal data, with a special focus on privacy and surveillance in the post-9/11 world. Interviews in Canada, the United States, France, Spain and Hungary were administered over the telephone while interviews were conducted in-person in Spanish within Mexico and Brazil. Background research papers were also prepared by an international multidisciplinary team of researchers led by Prof. David Lyon and Prof. Elia Zuriek of the Queen's Dept. of Sociology.

Summary of a few relevant findings that indicate public support for privacy-intrusive anti-terrorism laws is softening:

- across the globe, a minority of respondents (e.g., Canadians (48%), Americans (39%) and Mexicans (35%)) have reasonably high or very high levels of trust that their governments are striking the right balance between national security and individual privacy rights
- across the globe, a majority of respondents (e.g., Americans (57%) and roughly half of Canadians and Mexicans) believe that laws protecting national security are intrusive upon personal privacy
- Canadians, Americans, Spaniards, and Hungarians tend to be more knowledgeable about technologies (internet, RFID, GPS, biometrics) and their potential to intrude upon privacy when compared to Mexicans and Brazilians
- Minority of respondents agree with idea of security checks for visible minorities (with the exception of Spain and Mexico where a majority agree)

See Ipsos Reid, Summary Report: Global Privacy of Data International Survey (Nov. 2006). The full Summary Report is available at:

http://www.queensu.ca/sociology/Surveillance/?q=research/intl_survey

2. Tentative Evaluation of Canadian Govt. Legal and Enforcement Reaction

In December 2001, the (then) Liberal majority government passed the *Anti-Terrorism Act* which, among other things, changed laws to permit preventive warrantless arrests and judicial investigative hearings as well as warrantless electronic surveillance of international communications. In 2004, I conducted a survey of the empirical research and government internal reports that assess government enforcement efforts with respect to these new laws. In roughly the two years following the 9/11 attacks, the preventative arrests and investigative hearings had not been used, the number of authorizations for interceptions of private communications had not increased, the amount of individuals detained for immigration-related offences had not gone up, and the number of complaints under the *Privacy Act* (which governs federal government collection of personal information) had not appreciably risen.

Nevertheless, there were anecdotal reports that expanded investigatory powers were used to conduct racial and religious profiling of Muslim Canadians. Moreover, the report discussed the potential troubling aspects of new agreements between Canadian and foreign police and intelligence agencies that had not been vetted by the Canadian Parliament (e.g., the Canada-U.S. Smart Borders Agreement of 2001 with Integrated Border Enforcement Teams that share information among law enforcement officials). Ultimately, it was decided that it might be too soon to properly evaluate state practices due to the complex and ongoing legal and technological changes that followed the terrorism bombings.

See Arthur J. Cockfield, *The State of Privacy laws and Privacy-Encroaching Technologies after September 11: A Two-Year Report Card on the Canadian Government*, vol. 1 University of Ottawa Law and Technology Journal pp. 325-344 (2004); Arthur J. Cockfield, *Who Watches the Watchers? A Law and Technology Perspective on Government and Private Sector Surveillance*, vol. 29 Queen's Law Journal p. 364-407 (2003).

3. Protecting the Social Value of Privacy

In pursuit of security, governments around the world are adopting powerful technologies to collect and share detailed personal information, potentially leading to an erosion of privacy. My research strives to address how legal analysis should respond to situations where technology developments challenge privacy interests in the context of state investigations. In particular, judges, lawyers and policy-makers need to take into more explicit account both the individual rights aspect of privacy as well as the social value of privacy, that is, society's interest in preserving privacy apart from a particular individual's interest. This approach demonstrates that legal analysis sometimes overstates the tension between privacy and security as both can be portrayed as social interests.

By inhibiting the social value of privacy, governments place at risk values that are critical to the functioning of our democratic state. More specifically, increased scrutiny by state agents through the use of new surveillance and investigatory technologies can: (a) stifle political dissent as individuals fear reprisal by government actors; (b) inhibit freedom of

expression as individuals fear public scrutiny of their views or behavior; (c) lead to racial or religious profiling (i.e., discrimination) that targets identifiable groups despite no evidence of individual wrong-doing, which could lead to social alienation for members of the targeted group (d) have a disproportionately adverse impact on lower income Canadians who tend to make greater use of public spaces, which are increasingly subjected to state scrutiny; (e) results in political complacency to the extent that ubiquitous surveillance eliminates any subjective expectation of privacy and discourages citizens from questioning more and more state scrutiny; and (f) make it harder to hold state agents accountable for their potentially abusive behavior in part because of the surreptitious nature of the new technologies. In summary, an erosion of the social value of privacy dilutes important shared values within a free and democratic state that, at least in the long run, will make the Canadian public less secure.

See Arthur J. Cockfield, *Protecting the Social Value of Privacy in the Context of State Investigations Using New Technologies*, 40 University of British Columbia Law Review (forthcoming 2007); *Towards a Law and Technology Theory*, vol. 30 Manitoba Law Journal p. 383-415 (2004); Arthur J. Cockfield & Lisa M. Austin, *Introduction: Overview of Technological Challenges to Privacy and Security*, in Lisa Austin, Arthur J. Cockfield, and Patrick A. Molinari, eds., *Technology, Privacy, and Justice* 1 (Montreal: Canadian Institute for the Administration of Justice, 2007).