CDFAI

CANADIAN DEFENCE & FOREIGN AFFAIRS INSTITUTE

Personal Privacy and Communications Security from the Telegraph to the Internet

by John Ferris

July, 2014

Policy Paper

Personal Privacy and Communications Security from the Telegraph to the Internet

by John Ferris

Professor, History, University of Calgary

July, 2014

CDFAI
CANADIAN DEFENCE & FOREIGN AFFAIRS INSTITUTE

Prepared for the Canadian Defence & Foreign Affairs Institute
1600, 530 – 8th Avenue S.W., Calgary, AB T2P 3S8
www.cdfai.org

ISBN: 978-1-927573-27-3

Executive Summary

This paper puts the modern age of cyber, and the links between private parties and signals intelligence agencies, surveillance and privacy, into historical perspective. It demonstrates the limits to the ability of actors to intercept or read private messages during the telegraph age, and the radical changes in these matters which recently have occurred with the internet. It examines the present circumstances with cyber, including matters such as the role of states, criminals and individuals as actors and targets, and the links between intelligence, privacy, publicity and surveillance on the social market of the internet.

No precedent quite fits the struggle between states and individuals over intelligence, security, surveillance and privacy in the cyber commons. Nowhere is that condition truer than with communications security for private persons.

Before 1800, distance, illiteracy and censorship limited the dissemination of information for states and people. States regularly intercepted letters from subjects carried over their postal services – that capability, written into legislation, was one reason why they maintained those agencies in the first place.[1] Private persons responded to these dangers with forms of cypher and steganography, such as the use of secret ink, which might evade suspicion but offered little security when items were attacked. More significantly, states lacked the resources to read all of the intercepted letters all of the time, and illiteracy capped the number of people using the post. Between 1840-1914, during the rise of mass literacy and modern communications, private messages increased in quantity, but most states reduced these practices of interception at home, compared to the number of messages they used to take, and now could have taken. Tsarist Russia systematically intercepted the correspondence of political dissidents and revolutionaries.[2] Austria-Hungary, France and Germany did so much less frequently than Russia, but perhaps about as much as modern liberal states do. Britain, Canada and the United States rarely intercepted the communications of private parties at home, and then only criminals and the occasional violent revolutionary. Exceptions occurred, however, most spectacularly when encoded telegrams sent by leaders of the Democratic Party during the Presidential election of 1876, which were later acquired under subpoena by committees of Congress from a reluctant company, Western Union, were leaked to a Republican aligned newspaper, The New York Tribune, and then published, to create a political scandal.[3] Britain abandoned the use of general warrants — authorising the opening of every letter between, say, Bradford and Manchester — and turned to special warrants, enabling the interception only of letters to and from specific people and addresses.[4]

These changes in behaviour had functional and ideological roots. In particular, few countries could intercept any traffic outside of their borders, at a time when postal and telegraph services created the first world-wide information commons. Liberal states, above all Britain, were masters of these media. They did not intercept the communications of foreigners because they valued privacy and liberty for themselves and others. Britain did not have a codebreaking agency between 1846-1914 largely because, in peacetime, the government could intercept telegrams (including the enciphered cables of foreign governments) only under special warrant.[5] Necessity drove Britain to censor all internal and international cable and postal communications during the First and Second World Wars, but these practices ended with those conflicts. Even then, it

[1] Stéphane Genêt, Les espions des lumières: Actions secrètes et espionage militaire sous Louis XV, (Paris, Nouveau mondes éditions et Ministère de la Défense, 2013), Chapter 7; Kenneth Ellis, The Post Office in the Eighteenth Century, (Oxford University Press, London 1958), Chapter 6.

[2] Jonathan W. Daley, Autocracy under Siege: Security Police and Opposition in Tsarist Russia, 1866-1905, and The Watchful State: Security Police and Opposition in Russia, 1906-1917, (Northern Illinois University Press, Dekalb,1998 and 2004); Iain Lauchlan,"Security Policing in Late Imperial Russia", in Ian Thatcher (ed), Late Imperial Russia: Problems and Prospects. Essays in Honour of R.B. McLean, (Manchester, Manchester University Press, 2005), pp. 44-63.

[3] Ralph E. Weber, (ed). Masked Despatches, Cryptograms and Cryptology in American History, 1775-1900, (Center for Cryptologic History, Fort Meade, Md., third ed., 2013), pp. 143-65.

[4] John Ferris, "Tradition and system: British Intelligence and the Old World Order, 1715-1956", in Greg Kennedy (ed), Imperial Defence, The old world order, 1856-1956, (Routledge, London, 2008), pp. 179-80.

[5] John Ferris, "Whitehall's Black Chamber: British Cryptology and the Government Code and Cypher School, 1919-1929," Intelligence and National Security, Volume 2, Number 1, January 1987, pp. 54-91.

acquired only private data moving across the waves, not that resting in drawers. It did, however, gain a general warrant to intercept the cables of foreign states, sustaining the best codebreaking agency of the age, The Government Code & Cypher School.

Meanwhile, any person concerned with the secrecy of letters could conceal their meaning through book codes, cryptosystems based on a volume known only to the sender and addressee, that were both simple and secure. The vocabularies of the commercial codes used for cable messages were hard for the uninitiated to understand and some also employed effective superencipherment systems.[6] Properly used and without a physical compromise, these codes would stymy any but an experienced cryptanalyst. The latter were few in number. The systems to secure the postal and cable communications of private citizens were so disparate that the greatest of codebreaking agencies could read only a small fraction of them. But these communications were rarely read, although in such cases successful decryption was simple. The safety of private communications lay in the large numbers of people and systems, and the small number of willing and able attackers. Everywhere, however, telephones were tapped with less restraint than letters and telegrams, except in the USSR, where they possessed security services of unprecedented power and precision and were equally ruthless in the interception of all media. Within the United States, under the Olmstead Act, between 1928 and 1967 telephone messages could legally be intercepted anywhere outside ones' own homes.[7] But the British practice was more restrained, through 1914-45, its security services faced fewer restrictions on intercepting telephone messages than telegraphs, and especially letters.[8]

All told, before the digital age, government monitoring of telegraph, telephone and postal communications within liberal states was limited by law, though these practices rose sharply after 1914 and 1945. It rarely extended beyond one country. Totalitarian states pillaged the communications of their subjects, resting or moving, and maintained security services able to index and exploit the information, but could acquire little material away from home. Different means were needed to garner information resting in drawers, and moving by cable, or post or telephone. Rarely could private parties attack others, or states. The limits of technology and the power of governments constrained individuals from intercepting the traffic of other parties. State censorship of information became hard in liberal countries, and easy in totalitarian ones. Even when the bars to collection were raised – in fact, precisely for that reason – private material threatened information overload, far more than did the traffic of foreign states, simply because it was so voluminous, and its importance was so hard to gauge. The problem became data storage and retrieval, as letters had to be copied and telephone calls transcribed manually, and their myriad details indexed and filed.

Regular attacks on private messages, outside of war or within one's own state, emerged through a halting process, linked to the legal and technical characteristics of telephone and wireless traffic, especially from foreign countries. Radio-telephones emerged around 1930, their traffic easily intercepted. Effective modes of security for states did not arrive until 1942-3. Private shields remained weak. From 1960, private messages were transmitted in large volumes by satellite or wireless media and easy for all states (liberal or otherwise) to intercept, unlike cable, line telephone, or post. Many states began to systematically intercept foreign messages of this

[6] Steven Bellovin," Compression, Correction, Confidentiality and Comprehension A Look at Telegraph Codes", 25.4.09, Preliminary Version, http://www.cs.columbia.edu/~CS4HS/talks/codebooks.pdf
[7] Olmstead v. United States-277 (1928), http://supreme.justia.com/cases/federal/us/277/438/case.html
[8] For examples, cf. The National Archives, London, HO 144/20619 and KV 4/445.

sort, especially commercial traffic like telexes, and gradually expanded to include telephone calls. This expansion was enabled by the absence of legal restraints and end of taboos about violating individual privacy, coupled with the rise of radical pragmatism. States mired in decades of hot and cold wars learned the value of communications intelligence, like Ultra in the Second World War. Liberals viewed the traffic of foreign states as fair game, and the privacy of foreign individuals as collateral damage. Totalitarian states became even more cynical than before. These processes were driven by the presence of communications intelligence institutions, huge in size, that wanted to exploit all modes of data collection, even if that drove them to vacuum insignificant data in extraordinary quantities. These modes included the ease — almost the inevitability — for antenna farms to suck in satellite telecommunications, and the ability of computer generated keywords to guide scarce human monitoring toward individual messages.

In the analog age, however, work against private traffic was constrained not merely by the perennial problems of limits to computing and analytical power, but by difficulties with data storage and retrieval. Telephone messages captured on tape could only be assessed after the physical motion of reels and through the craftwork of human analysts. The monitoring of satellite communications during the cold war intercepted some data in motion (missing the greater masses carried by the post, and cables) but none of that at rest: most of the take was foreign, and little from one's citizens.

From 1990, however, the internet became the core of communications, as did the telephone – much would have changed had messages moved only over telegraph cables controlled by, and accessible to, just a few companies and states. Paper mail, which constrained the capture of communications and interception because of the labour required, gave way to electronic mail, dispatched by telephone lines, and carried voice and print messages. Data at rest and in motion became unified and digitized, simple to acquire, store, retrieve, analyse – and to intercept. It all could be attacked by the same cryptanalytical means. Communications, carried online and through wireless telephones by signals that crossed national boundaries promiscuously, linked to any data stored on computers connected to the internet, became open to interception by all comers at once, not merely to states with sole control over cables or postal services. This material could be copied as easily as electrons, although retrieval and analysis remained frustrating.

These changes in communication and information also enabled the emergence of the largest and most complex human commons ever known, a social market. This market centred on the unparalleled ability of people to communicate, and for messages to be intercepted. It was marked by the self-interest, cooperation, warfare, intelligence gathering, deception, and security characteristics of the individuals, states, and pirates that abound on every commons. In order to maximise their gains from this social market, people sought to simplify the processing of information. They paid for that end with privacy, thus easing piracy. Privacy and surveillance are problematic concepts as attitudes toward them vary by culture and time. There may have been no more privacy or less surveillance in villages, than there is in the global village. Bourgeois forms of privacy and respectability, intended to contain surveillance, limited one's opportunities on the signals market. Given the mass of other people one could best find individuals, attract their attention or pursue comparative and mutual advantage by combining openness with the constant transmission of, and search for, broad and narrow signals. People commodified others, and themselves. Voting with their digits, they assigned privacy a low price, if sometimes pretending its value was higher. Their modes of communication transformed the relations between their reputations, and themselves. New needs to communicate outweighed old modes of privacy, producing a society based on signals and surveillance, both as subject and object.

These social and technological developments created unprecedented abilities to intercept and transmit signals. They transformed privacy and surveillance, intelligence and security, and old distinctions between states and individuals, and their competitions. The greatest change was not the ability of states to attack each other, or their own people, though these capabilities did rise. It was the ability of states to monitor foreign civilians, and above all of private parties to read anyone's mail or memoranda, private or governmental, home or abroad. As ever, states lacked the resources to read all of the traffic they could intercept, but they no longer were the only power on these seas. Individuals were more open to attack from pirates, and foreign governments, than on any other commons. Against this, for perhaps the first time in history, anyone could acquire cryptography proof against the best of codebreakers. Few did so. Most were exposed to attack from millions. Pirates had unprecedented power, precision and range. States attacked the communications of foreign individuals and corporations far more than ever before in peacetime, and faced greater challenges in defending their citizens.

Changes in the characteristics of communication spilling across national borders affected the practices of liberal states to intercept any traffic of their citizens, home or abroad, or foreign messages passing through their space. In the analog age, lawyers and siginters could differentiate between traffic transmitted at home and abroad, and illegal and lawful interception. In the digital age, however, domestic traffic moved abroad, and foreign messages through your home. Foreign targets might best be attacked by intercepting communications passing through your home, despite legal quibbles. Domestic traffic would be acquired through interception abroad. Bulk collection of any internet traffic must include one's citizens, in the first instance. To do otherwise would be to abandon communications intelligence, which one's rivals would not. Yet any analysis of such material, whether intercepted at home or abroad, must touch the envelopes, the metadata, of their citizens' mail, without warrant. These procedures were legal, but not politic: they felt icky. Surveillance, which might be necessary in war depending on the threat, was intolerable in normal life when stricter procedures were imperative.

The likelihood of private parties being monitored and their messages being read, and the number of potential attackers, reached levels beyond that even in totalitarian states – and would do so even in the most libertarian system imaginable, or if the NSA were abolished. Any serious attacker, private or public, could read the traffic of most civilians, and many states. Private attackers could be bad boyfriends, criminals, mercenaries, states, freelance or corporate data miners, idealists, or enemies of 1984. Private people might be surveyed, surveyor, victim, voyeur, pirate, or exhibitionist. Their safety lay only in numbers, anonymity, or allies, where their governments served both as problem and solution.

Internet libertarians, viewing government intelligence and secrecy as evil, purported to defend freedom from the slavery caused by the pursuit of security. These comments had some force, but more melodrama. They ignore the problems of competition on the commons, and the agency and ambitions of individuals. The metaphors used to describe this situation, 1984 or the Panopticon, were one dimensional. They looked only at peoples being attacked by their own state – not those assaulted by foreign governments, or by pirates, at home or abroad. The latter problems will remain, even if the former finds a solution. Nor was the question simply the gaze of the state. People used this Panopticon for their own purposes – to attract attention and display what they wanted to show, rather than to tremble before the unblinking eye. In western countries, few people will be assaulted by their own states: more will be attacked by foreign governments, and above all, private parties. On the internet, hell is other people. Fewer people will fear Big Brother than want his help against pirates, or foreign governments.

The key issue in the relationship between secrecy, privacy and intelligence is where are the borders? They shift constantly, and not just in only one way. Liberal democracies questioned how to balance liberty and privacy versus security, while keeping the former supreme, in overlapping competitions between states and peoples, on a new information commons. This question was not entirely new, and nor were the answers. The harder question was, how does a liberal democratic state respond when its society choses to embody surveillance, or to embrace the politics of exhibitionism?

About the Author

John Ferris is a Professor of History at The University of Calgary, where he also is a Fellow at The Centre for Military and Strategic Studies. He received an MA (1980) and a PhD (1986) in War Studies, from King's College, The University of London, United Kingdom. He has published four books and one hundred academic articles or chapters in books, on diplomatic, intelligence and military history, as well as contemporary strategy and intelligence. His books have been published in Australia, Canada, France, Japan, Singapore, Turkey, The United States and the United Kingdom: they also have been translated into French, Hebrew and Japanese. He comments in national and international media, on Canadian and American foreign and military policy, the wars in Iraq and Afghanistan, intelligence, and nuclear weapons.

Canadian Defence & Foreign Affairs Institute

CDFAI is the only think tank focused on Canada's international engagement in all its forms - diplomacy, the military, aid and trade security. Established in 2001, CDFAI's vision is for Canada to have a respected, influential voice in the international arena based on a comprehensive foreign policy, which expresses our national interests, political and social values, military capabilities, economic strength and willingness to be engaged with action that is timely and credible.

CDFAI was created to address the ongoing discrepancy between what Canadians need to know about Canadian international activities and what they do know. Historically, Canadians tend to think of foreign policy – if they think of it at all – as a matter of trade and markets. They are unaware of the importance of Canada engaging diplomatically, militarily, and with international aid in the ongoing struggle to maintain a world that is friendly to the free flow of goods, services, people and ideas across borders and the spread of human rights. They are largely unaware of the connection between a prosperous and free Canada and a world of globalization and liberal internationalism.

In all its activities CDFAI is a charitable, nonpartisan organization, supported financially by the contributions of foundations, corporations and individuals. Conclusions or opinions expressed in CDFAI publications and programs are those of the authors and speakers and do not necessarily reflect the views of the Institute staff, fellows, directors, advisors, or any individuals or organizations that provide financial support to CDFAI.