Shutting the Backdoor: The Perils of National Security and Digital Surveillance Programs

Ronald Deibert | October 2013

Strategic Studies Working Group Papers

CIC
Canadian International Council
Conseil International du Canada

CDFAI
Canadian Defence & Foreign Affairs Institute

ABOUT THE AUTHOR

Ron Deibert, (OOnt, PhD, University of British Columbia) is Professor of Political Science, and Director of the Canada Centre for Global Security Studies and the Citizen Lab at the Munk School of Global Affairs, University of Toronto. The Citizen Lab is an interdisciplinary research and development hothouse working at the intersection of the Internet, global security, and human rights. He is a co-founder and a principal investigator of the OpenNet Initiative and Information Warfare Monitor (2003-2012) projects.

Deibert was one of the founders and (former) VP of global policy and outreach for Psiphon Inc.

Deibert has published numerous articles, chapters, and books on issues related technology, media, and world politics. He was one of the authors of the Tracking Ghostnet report that documented an alleged cyber-espionage network affecting over 1200 computers in 103 countries, and the Shadows in the Cloud report, which analyzed a cloud-based espionage network.

He has been a consultant and advisor to governments, international organizations, and civil society/NGOs on issues relating to cyber security, cyber crime, online free expression, and access to information. He presently serves on the editorial board of the journals International Political Sociology, Security Dialogue, Explorations in Media Ecology, Review of Policy Research, and Astropolitics.

In 2013, he was appointed to the Order of Ontario and awarded the Queen Elizabeth II Diamond Jubilee medal, for being "among the first to recognize and take measures to mitigate growing threats to communications rights, openness and security worldwide."

The opinions expressed in this paper are those of the author and do not necessarily reflect the views of the Canadian International Council, its Senate or its Board of Directors, or the views of the Canadian Defence & Foreign Affairs Institute.

If you would like to download a copy of this report please visit **www.cdfai.org** or **www.opencanada.org**.

If you would like to be added to our mailing list or have questions about our publications please contact: contact@cdfai.org or info@opencanada.org.

ISSN 1925-4903

© 2013 Canadian Defence & Foreign Affairs Institute and Canadian International Council

EXECUTIVE SUMMARY

As governments have sought to monitor digital communications for security purposes, the "backdoor" paradigm has become the predominant approach. Strictly speaking, backdoors refer to special methods of bypassing normal authentication procedures to secretly access computing systems. But here the concept is used in a broader sense to describe a range of policies and practices whereby governments compel, or otherwise get the cooperation of, private sector companies to provide access to data they control. The backdoor paradigm is not only a concern for political reasons, particularly for civil liberties, it is also bad for digital security and foreign policy. Law enforcement and intelligence agencies should instead seek to work within the information-rich world of Big Data that surrounds us with any access to private communications made exceptional and strictly controlled by lawful procedures and oversight mechanisms.

SOMMAIRE

Tandis que les gouvernements ont cherché à exercer une surveillance sur les communications numériques à des fins de sécurité, le paradigme de la « porte arrière » est devenu l'approche prédominante. Strictement parlant, ce terme de porte arrière renvoie à des méthodes particulières de contourner les procédures normales d'authentification pour accéder secrètement aux systèmes informatiques. Mais, ici, le concept est utilisé dans un sens plus large pour décrire un éventail de politiques et de pratiques selon lesquelles les gouvernements forcent ou autrement obtiennent la coopération d'entreprises du secteur privé pour obtenir un accès aux données qu'elles contrôlent. Le paradigme de la porte arrière n'est pas seulement une préoccupation pour des raisons politiques, particulièrement en matière de libertés civiles, mais il est également mauvais pour la sécurité numérique et la politique étrangère. Les organismes d'application de la loi et de renseignements devraient plutôt chercher à travailler à l'intérieur du monde, riche en information, du big data qui nous entoure, avec l'accès aux communications privées faites exceptionnelles et strictement contrôlées par des procédures et des mécanismes de surveillance légaux.

"If a surveillance capability were quietly added into the core of the Internet and an attempt was made to keep it a secret, in some respects this would be antithetical to the overarching philosophy upon which the Internet was built" Tom Cross, BlackHat 2010

Introduction

The Internet and associated digital media have deeply penetrated all of society. We now live in the world of the "Internet of things," by some estimates there are now 10 billion internet connected devices on the planet networked together via common protocol. This common space is not only a forum for communications, it is a major repository of data about each and every one of us, our daily habits, movements, social relationships, and even private thoughts. For government agencies whose mission is to enforce the law or gather intelligence, cyberspace has become an extraordinary asset and an object of security in its own right. As governments have ramped up digital surveillance programs, they have had to turn to the private sector, which controls not only the familiar services we all use (Google, Facebook, Microsoft), but the vast majority of the physical infrastructure of cyberspace as well—the cell phone base stations, undersea fibre optic cables, Internet Exchange Points, and routers.

One of the ways governments have approached the private sector has been to compel, legally or informally, the development of special modifications to private company's technical systems to enable access to data, what I call the "back door" paradigm. Strictly speaking, backdoors refer to special methods of bypassing normal authentication procedures to secretly access computing systems. But I use the phrase in a broader sense, to refer to the paradigm of state-directed modification of and/or intrusions into communications infrastructure and services for security purposes. Examples of the backdoor paradigm include lawful intercept mechanisms coded directly into software, to "splitters" that surreptitiously fork copies of data streams to alternative destinations, to other, informal, means of data sharing that may go on between private sector and security services. The backdoor paradigm is not new, but the Edward Snowden/NSA revelations have cast a spotlight on them and underscored how deeply entrenched they have become in the post 9/11 era of Big Data surveillance. In what follows I lay out several concerns about the backdoor paradigm, foremost among them being the ways, in the name of security, backdoors actually contribute to greater insecurities down the road. Shutting the backdoor is, therefore, an urgent public policy matter for all liberal democratic countries. Rather than sacrifice cyberspace at the altar of security, law enforcement and intelligence agencies should be encouraged to develop alternative modes of data collection strictly within the framework of the rule of law.

History of Backdoors

Built-in backdoors on communications equipment for law enforcement and intelligence agencies are not new. It is often said that espionage is the second oldest profession, and as long as governments have been engaged in espionage they have looked to assert control through the means of communication. In the early 20th century, for example, telegraphic messages processed by Western Union and other companies, including those of foreign diplomatic communications, were copied and secretly given to US authorities, much the same as Verizon has reportedly done so today. Codenamed "Shamrock," the program required the companies to, on a daily basis, hand over to the NSA copies of all of the cables sent to, from, or through the US.[1] During the Cold War, a variety of signals intelligence collection mechanisms, from specially equipped naval vessels to huge land-based antennas, intercepted stray radar and radio transmissions, even those that bounced off the surface of the moon.

1 See James Bamford, *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency,* (New York: Random House, 2001), p. 133.

The rise of the Internet and digital technology presented a new challenge to signals intelligence, but also a special opportunity. Digital media flowing through fibre optic cables do not unintentionally leak data into the atmosphere in the same way, making signals interception a more difficult task. At the same time, huge and exponentially growing volumes of digital data, processed and archived through the Internet's physical points of control (e.g., switches, gateways, exchange points), presented irresistible targets for data mining and analysis, leading the government to seek access through cooperation with the companies that own and operate the infrastructure. Then, as now, the government sought to ensure access to data by deliberately weakening one type of security in the name of another. Occasionally, these efforts trickled into the public domain. During the 1990s, there was a cantankerous "cryptodebate" over US government proposals to control the export of strong encryption to foreign jurisdictions to weaken the security of adversaries and make them more open to US surveillance. Criticism at that time questioned the wisdom of such controls, arguing that restricting cryptography would end up hurting the US itself. As Bruce Schneier explains

> [t]he government deliberately weakened U.S. cryptography products because it didn't want foreign groups to have access to secure systems. Two things resulted: fewer Internet products with cryptography, to the insecurity of everybody, and a vibrant foreign security industry based on the unofficial slogan 'Don't buy the U.S. stuff—it's lousy.'

The US Communications Assistance for Law Enforcement Act (CALEA), passed in 1994 and still in effect, requires telecommunications carriers to install technical capabilities for lawful surveillance into all equipment manufactured or sold in the US. Although the law applies to telecommunications carriers, US government officials have appealed to expand the law to cover VOIP and other broadband digital services. During the "Clipper Chip" debate of the 1990s, the US government attempted to mandate the production of special chips into telecommunications equipment that would allow the NSA to eavesdrop on voice traffic using a surrendered encryption key. While critics of the Clipper Chip managed to scuttle the proposal, the same basic backdoor philosophy has continued to drive government surveillance efforts up to and including the present time. 9/11 gave added impetus to these approaches, with a perceived "failure to connect the dots" driving ambitious plans and a thriving new market to gather as much information from as many discrete information sources as possible and then mine and analyze it.[2]

The Snowden Revelations and the Backdoor Paradigm

Edward Snowden's detailed leaks have opened a chasm into the otherwise secretive world of intelligence practices, revealing widespread monitoring of both US and international communications by the US NSA and some of its allied agencies, like the UK's GCHQ. Among other revelations, the leaked documents have provided details on elaborate programs involving the cooperation of some of the Internet's largest companies, like Google, Microsoft, Facebook, and Yahoo! as well as major tier 1 telecommunications companies, like Verizon and Global Crossing. Although the exact details are in dispute, the program codenamed PRISM appears to have involved a hiving off of customer data onto special servers to give law enforcement and intelligence agencies direct access.[3] In the case of leaks involving Verizon, the company supplied the NSA with metadata on all domestic and international telephone call records.[4] Metadata might best be described as everything but the content of the communications, meaning the endpoints of the transmission, the length and time of the call, and so on. Other leaks have shown how foreign owned telecommunication companies seeking to operate in the United States are approached by US legal officials, called "Team Telecom," who may request similar data sharing arrangements, such as compliance with CALEA or archiving of data on US soil for national security investigations.[5]

2 A good historical resource for all of the above is Shane Harris, *The Watchers: The Rise of America's Surveillance State,* (New York: Penguin, 2010).
3 http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data; also see "How Prism Works" http://ashkansoltani.org/2013/06/14/prism-solving-for-x.
4 http://www.guardian.co.uk/world/2013/jun/06/nsa-phone-records-verizon-court-order.
5 http://www.guardian.co.uk/world/2013/jul/12/telstra-deal-america-government-spying and http://articles.washingtonpost.com/2013-07-06/business/40406049_1_u-s-access-global-crossing-surveillance-requests.

In the case of leaks concerning Microsoft, the company reportedly helped solve encryption cracking issues surrounding email, cloud, and VOIP services, including providing access to videoconference streams over Skype without users' knowledge.[6]

Other leaked documents have shed light on top secret programs, codenamed "Bullrun," whose objectives are to weaken encryption standards worldwide, including by encouraging companies to insert deliberate vulnrabilities into their encryption algorithms known only to the NSA. Given Canada's own signals intelligence agency, the Communications Security Establishment of Canada (CSEC) has a long-standing special relationship with the NSA, it should come as no surprise that we would develop similar programs. According to recent Globe and Mail reports, "for nearly two decades, Ottawa officials have told telecommunications companies that one of the conditions of obtaining a licence to use wireless spectrum is to provide government with the capability to bug the devices that use the spectrum."[7] Documents obtained by The Globe also reveal that as part of these requirements, Ottawa has demanded companies scramble encryption so that it can be accessed by Canada's law enforcement agencies.

The leaks have touched off vigorous public policy and security debates in the US and abroad. Their scope and scale as highlighted in the leaked documents (which themselves are probably only a partial peek), call into question recent law enforcement lobbying efforts, claiming that the FBI was at risk of "going dark" because of new communication technologies.[8] In light of Snowden's revelations about wholesale surveillance programs, as well as the abundance of information in the public domain users willingly give out about themselves, their friends, interests, political preferences, etc, the assertions seem ludicrous. The controversy has also raised questions about the degree and effectiveness of oversight and public accountability for backdoor arrangements. While it is true that three branches of US government approved the programs associated with the Snowden leaks, the deliberations of the court that oversees them, the FISC, are themselves secret.[9] Moreover, it appears that many elected officials were either ignorant, or deliberately misled by government officials, about the true scope and scale of the programs in question.[10] The leaks have also raised questions about oversight of similar programs operating outside the United States, such as the UK's GCHQ or Canada's CSE, both of which have arguably far less independent scrutiny of their activities.[11] While European countries are subject to more stringent privacy protections, some of their signals intelligence programs have even less rigorous oversight than what appears to be the case in the UK and Canada, and certainly less than in the United States. Backdoors into massive and detailed databases of private information, as appears to have been constructed in the US and allied countries, calls for an urgent debate about proper checks and balances around national security in the world of Big Data.

Quite apart from these concerns about privacy and potential abuse of unchecked power is an additional concern around the security implications of backdoors. Building backdoors into devices and infrastructure may be useful to law enforcement and intelligence agencies, but it also provides a built-in vulnerability for those who would otherwise seek to exploit them and in doing so actually contributes to insecurity for the whole of society that depends on that infrastructure. In 2013, a team of twenty computer security researchers issued a report published by the US-based Center for Democracy and Technology, arguing that "mandating wiretap capabilities in endpoints poses serious security risks," and that building "intercept functionality into … products is unwise and will be ineffective, with the result being serious consequences for the economic well-being and national security

6 http://www.guardian.co.uk/world/2013/jul/11/microsoft-nsa-collaboration-user-data.

7 Colin Freeze and Rita Trichur, "Wireless firms agree to give Ottawa ability to monitor calls, phone data," The Globe and Mail (September 16, 2013).

8 See the testimony of Robert S. Mueller, Director, FBI before the Committee on the Judiciary, US Senate, June 19, 2013 http://www.judiciary.senate.gov/pdf/6-19-13MuellerTestimony.pdf and Hearing on: "Going Dark: Lawful Electronic Surveillance in the Face of New Technologies" http://judiciary.house.gov/hearings/hear_02172011.html.

9 See Mark Rumold and David Sobel, "Government Says Secret Court Opinion on Law Underlying PRISM Program Needs to Stay Secret," EFF (June 7, 2013) https://www.eff.org/deeplinks/2013/06/government-says-secret-court-opinion-law-underlying-prism-program-needs-stay.

10 Greg Miller, "Misinformation on classified NSA programs includes statements by senior US officials," *Washington Post,* June 30, 2013) http://www.washingtonpost.com/world/national-security/misinformation-on-classified-nsa-programs-includes-statements-by-senior-us-officials/2013/06/30/7b5103a2-e028-11e2-b2d4-ea6d8f477a01_print.html.

11 http://www.independent.co.uk/news/uk/home-news/gchq-spying-programme-spy-watchdog-is-understaffed-and-totally-ineffective-8708231.html and http://www.thestar.com/news/world/2013/06/10/us_online_surveillance_canadian_cyber_expert_weighs_in.html.

of the United States."[12] As noted security expert Bruce Schneier points out with respect to the FBI's claims, but in terms that could be generalized to other security services:

> The FBI believes it can have it both ways: that it can open systems to its eavesdropping, but keep them secure from anyone else's eavesdropping. That's just not possible. It's impossible to build a communications system that allows the FBI surreptitious access but doesn't allow similar access by others. When it comes to security, we have two options: We can build our systems to be as secure as possible from eavesdropping, or we can deliberately weaken their security. We have to choose one or the other.[13]

MIT's Susan Landau contributes an additional argument to these security concerns, which she labels the "time factor."[14] The US law, the Communications Assistance for Law Enforcement Act (CALEA), mandated that telecommunications equipment be built with law enforcement access capabilities, and also applied retrospectively to older technologies. But it never factored in that the back doors could become vulnerable over time as attack capabilities progressed, and knowledge of the back doors spread. These types of concerns were amply demonstrated in a 2010 Black Hat presentation by IBM researcher Tom Cross of security vulnerabilities connected to lawful intercepts in Cisco routing products (which were based on standards set by the European Telecommunications Standards Institute)[15] in which he showed how the lawful intercept could be exploited to enter the systems and eavesdrop on communications without leaving a trace.[16]

There have been several real-life demonstrations of these types of vulnerabilities that should give us pause. Recent political scandals in Greece and Italy, in which prominent officials and business people had their phones secretly tapped with the information used for purposes of blackmail and slander, were enabled by poorly designed lawful access back doors on cell phone infrastructures.[17] A project to search the internet for access to critical infrastructure, called the Shodan search engine, has vividly demonstrated the number of easily accessible systems, some critical, that can be accessed from the wider Internet.[18] Some of the access points have emerged because of vulnerabilities in the code, but in other cases back doors have been built in and then forgotten about, or poorly maintained, by the engineers. In one case, the Canadian company Rugged.com, whose industrial grade software is used to control everything from power utilities to military plants and traffic control systems, had a back door that was hard coded with a single username ("factory"), and a password that was automatically generated depending on the MAC address of the device, which itself could easily be searched for using Shodan.[19] In 2008 Citizen Lab researchers discovered that the Chinese version of the popular VOIP product, Skype (called TOM-Skype) had been coded with a special surveillance system in place such that whenever certain keywords were typed into the chat client, data would be sent to a server in mainland China (presumably to share with China's security services).[20] Upon further investigation, it was discovered that the server onto which the chat messages were stored was not password protected, allowing for the download of millions of personal chats, many of which included credit card numbers, business transactions, and other private information.[21]

12 https://www.cdt.org/files/pdfs/CALEAII-techreport.pdf.

13 "The Problems with CALEA-II," Schneier on Security, June 4, 2013, http://www.schneier.com/blog/archives/2013/06/the_problems_wi_3.html.

14 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2028152.

15 Tom Cross, "Exploiting Lawful Intercept to Wiretap the Internet," BlackHat DC 2010, http://www.blackhat.com/presentations/bh-dc-10/Cross_Tom/BlackHat-DC-2010-Cross-Attacking-LawfulI-Intercept-wp.pdf. Notably the presentation was based on the fact that Cisco is one of the few companies to openly publish its lawful intercept architecture for peer review. Without that transparency, Cross' analysis could not be done.

16 http://judiciary.house.gov/hearings/printers/112th/112-59_64581.PDF, p.23.

17 See Vassilis Prevelakis and Diomidis Spinellis, "The Athens Affair," IEE Spectrum (June 29, 2007), found here: http://spectrum.ieee.org/telecom/security/the-athens-affair.

18 http://arstechnica.com/security/2012/10/backdoor-in-computer-controls-opens-critical-infrastructure-to-hackers.

19 http://lists.grok.org.uk/pipermail/full-disclosure/2012-April/086652.html.

20 Information Warfare Monitor and ONI Asia, "Breaching trust: An analysis of surveillance and security practices on China's TOM-Skype platform," 2008 and Jedidiah Crandall et al, "Chat program censorship and surveillance in China: Tracking TOM-Skype and Sina UC," First Monday, June 2013, http://firstmonday.org/ojs/index.php/fm/article/view/4628/3727.

21 The China-based espionage attacks aimed at Google and other companies, and revealed in January 2010 as Operation Aurora, may have been directed towards accessing Google's database of court-ordered surveillance targets, and possibly even the forked databases that enable access for the FBI to Google data, known as the "PRISM" program. Not enough is known about the attacks or the PRISM program to say for certain. See http://articles.washingtonpost.com/2013-05-20/world/39385755_1_chinese-hackers-court-orders-fbi.

By definition, back doors engineered for lawful interception are engineered vulnerabilities by a different name. In these and likely numerous other undiscovered cases, those vulnerabilities offer a direct point of access for exploitation. Building insecurities into the communications infrastructure that surrounds us may be a shortcut for law enforcement and intelligence, but is it one worth making relative to the vulnerabilities that are created for all of society?

Not only are back doors a concern for civil liberties and infrastructure security, they set a bad precedent for, and help legitimize, the very same practices abroad. The Tom-Skype example may look amateur in comparison to programs like the NSA's PRISM, but it is a local variation on a common theme. No doubt one implication of Snowden's revelations will be the spurring on of numerous national efforts to regain control of information infrastructures through national competitors to Google, Verizon, and other companies implicated, not to mention the development of national signals intelligence programs that attempt to duplicate the US model.[22] Already prior to the revelations, numerous companies faced complex and, at times, frustrating national "lawful access" requests from newly emerging markets. Many countries of the global South lack even basic safeguards and accountability mechanisms around the operations of security services, and their demands on the private sector could contribute to serious human rights violations and other forms of repression. For example, India, the United Arab Emirates, Saudi Arabia, and other countries have all demanded that Canada's Blackberry put in place lawful interception and monitoring capabilities, compliance with which could begin to affect the nature of the Blackberry product itself. Although the company rarely discloses anything about these agreements, a spokesperson for the company admitted that it had developed a monitoring system for its consumer devices for the government of India and will even train technicians in interception back in Canada.[23] (In India, the government requires all telecommunication companies to make available data to security agencies without a warrant or other basic safeguards). What was once a signature feature of the Blackberry product (uncrackable encryption), has been compromised in the name of opening up new markets.

Alternatives to BackDoors

If the backdoor paradigm is questionable on civil liberties, economics, security, and foreign policy grounds, what are the alternatives? As long as we live in a dangerous world with real threats, intelligence agencies are going to be an important element of liberal democratic government. Likewise, without agencies to enforce the law, the very basis for the exercise of human rights, including privacy, would quickly diminish.

Elsewhere, I have argued that civil society needs to develop a cyber security strategy, and part of that strategy must involve a response to the back door paradigm on security grounds. Rather than building in insecurities by design, a better strategy would emphasize the opposite: encouraging the widespread use of state of the art encryption systems, as well as adoption of standards such as "https by default" and "two factor authentication." Another component of such a strategy would be to emphasize the security benefits of open source software, which provide greater assurances that companies have not built in special back door privileges by design, that customers get what they sign off on in their terms of service. In line with this approach would be regulations around deletion of stored data and proposals like the "right to be forgotten," which, although typically seen in a rights-based framework, have security implications insofar as they restrict the copies of stored data that might be exploited for nefarious purposes.

As for legitimate lawful access requests, the group of experts involved in the CDT study argue that "law enforcement's use of passive interception and targeted vulnerability exploitation tools creates fewer security risks for nontargets and critical infrastructure than do design mandates for wiretap interfaces."[24] In a world of "Big Data" in which so much of our information is routinely given away as part of our daily life, law enforcement

22 See Ron Deibert, "Why NSA Spying Scares the World," CNN Opinion, (June 12, 2013) http://www.cnn.com/2013/06/12/opinion/deibert-nsa-surveillance.
23 http://timesofindia.indiatimes.com/tech/tech-news/telecom/Government-BlackBerry-dispute-ends/articleshow/20998679.cms.
24 "Going Bright: Wiretapping without Weakening Communications Infrastructure," p.63.

and intelligence agencies need to find ways to work within this universe as it exists, rather than drill holes in it from the inside-out in ways that undermine confidence and create additional risks for all of society. Those lawful access provisions that are still required should be infrequent and strictly controlled with rigorous oversight and public accountability provisions. Direct tapping of entire services wholesale should be eliminated. Not only will this protect civil liberties and prevent the concentration of power in unchecked hands, it will ensure that we are not doing more to undermine our own security in an overzealous surveillance quest.

Conclusion

The communications environment we have created around us is complex and expanding, and the security issues surrounding it are serious and important. The backdoor paradigm is symptomatic of a larger trend that privileges intelligence and security agencies, builds borders around cyberspace, and undermines checks and balances around concentrations of power. The backdoor paradigm is not only bad for civil liberties, it is bad for security, and sets dangerous precedents for the legitimization of practices abroad we ostensibly oppose. Law enforcement and intelligence agencies are necessary and important to liberal democracy, but there is more than one way for them to go about their missions. In the world of Big Data, in which so much personal information is readily abundant, new methods of "connecting the dots" must be explored other than those that drill holes into our communications infrastructure. Government surveillance practices need radical re-thinking, beginning first and foremost with a reinforcement of basic checks and balances that have, for too long, been sidestepped in the name of security.

STRATEGIC STUDIES WORKING GROUP

The Strategic Studies Working Group (SSWG)is a partnership between the Canadian International Council (CIC) and the Canadian Defence and Foreign Affairs Institute (CDFAI). The CIC absorbed the former Canadian Institute of Strategic Studies (CISS) upon the CIC's formation in 2008, and the CISS's original focus is now executed by the SSWG.