COMMENTARY*

Surveillance of Electronic Communications: "Is there anybody out there?"[1]…Yes there is.

The right to private communications with one's lawyer when providing instructions or obtaining legal advice – solicitor client privilege – is a principle of fundamental justice and a civil right of supreme importance in Canadian society.[2] Violations of that privilege by governments or government agencies would be contrary to the rule of law unless one of the very few permitted exceptions applied.

The Edward Snowden revelations force us to question whether solicitor client privilege is a principle we are not adequately safeguarding in the digital age. Among other things the Snowden revelations demonstrate how prevalent government surveillance of electronic communications has become and gives us considerable reason to question the implications of what we now know for the often-sensitive communications between clients and their lawyers.

Lawyers routinely store client information on computers and, in today's world; almost all of these computers are connected to the Internet. Quite possibly, some or all of the information is even stored by lawyers "in the cloud." Given the Snowden revelations regarding the prevalence of government surveillance, how should lawyers approach their professional obligations to protect client confidences? What steps do clients need to take? How worried should we all be? Is there actually a danger? Is the government really going to intercept information gathered by lawyers when communicating with their clients?

The Rule of Law and Lawyer Independence Advisory Committee has been thinking about this issue, and recently had the benefit of a presentation from Michael Geist, the Canada Research Chair in Internet and E-commerce Law and professor of law at the University of Ottawa, during which some of the issues and concerns about widespread government surveillance were raised and discussed. We think it is fair to say that the Committee members were surprised at the extent of such surveillance and the issues it presented to lawyers and their clients. It concluded that it would be advantageous to raise

---

*One of the ways the Law Society of British Columbia is required, by s. 3 of the *Legal Profession Act*, to discharge its mandate is "by preserving and protecting the rights and freedoms of all persons." The Rule of Law and Lawyer Independence Advisory Committee (the "Rule of Law Committee") is charged by the Benchers to monitor issues of importance connected to this mandate. Part of this mandate requires communication to raise awareness of issues with the profession and public and to identify concerns and invite commentary. From time to time, the Committee will be doing just that.

[1] Words and lyrics by Pink Floyd.

[2] *Lavallee, Rackel & Heintz v. Canada (Attorney General)* [2002] 2 S.C.R. 209

these concerns directly, through an article such as this, and to seek feedback from the profession and its clients if possible.

There are many legitimate reasons for governments to collect information. Much of the rationale, in fact, for information gathering dates back as far as World War II and there is no doubt that a country's security depends to a considerable degree on how well-informed it is of risks to that security.

But the Snowden revelations have disclosed how widespread and invasive government surveillance is. The National Security Administration (NSA) in the USA is said to search content of messages to and from the US. It is said to have collected US email records in bulk for periods of years. It is said to have recorded every cell phone call in the Bahamas for certain periods of time.[3] These are no small intrusions.

The Committee understands that Canada is an active participant in the information gathering community. We have been told that then-Defence Minister Peter MacKay is reported to have approved, in 2011 a secret electronic eavesdropping program that scours global telephone records and Internet data trails – including those of Canadians – for patterns of suspicious activities.[4] The Communications Security Establishment of Canada ("CSEC") is reported to have gathered metadata on "untold numbers" of global phone calls and online messages – and that these efforts also "incidentally" intercepted the communications of Canadians.[5] It will be remembered by many that CSEC also used airport WiFi in order to track Canadian travellers.

Canada is also very much involved with the United States, the United Kingdom, Australia, and New Zealand (the "Five Eyes Partners") in information gathering and surveillance of communications. These partners can, and it appears (again, from the Snowden revelations) frequently do, share intercepted communications gathered as part of their security operations.

Whether lawyers or their clients should worry about the security of their communications with clients is not clear. The law itself seems to be definitive that these communications are confidential, and, in many cases, are subject to solicitor–client privilege. But, if all electronic communications can be, or are being, captured, it stands to reason that lawyer-client communications will be included, even if they are not targeted. And, no definitive assurances have been offered by the intelligence community that solicitor-client privilege is being respected in all cases.

---

[3] https://theintercept.com/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/

[4] http://www.theglobeandmail.com/news/politics/data-collection-program-got-green-light-from-mackay-in-2011/article12444909/

[5]http://www.theglobeandmail.com/news/national/how-canadas-shadowy-metadata-gathering-program-went-awry/article12580225/

In fact, we know that the legal community *is* sometimes the actual target of government surveillance, rather than simply a passive target. Earlier this year, the U.K government admitted that it was unlawfully monitoring legally privileged communications.[6] Last year, it was reported that the government of Indonesia retained an American law firm concerning negotiations that it was having with the American government on trade matters. The Australian Signals Directorate conducted surveillance of those trade talks, including the interception of communications between the Indonesian government and its American law firm. The Directorate then offered to share that information with the United States National Security Administration.[7] While admittedly this is an example not involving Canadian organisations or governments, each of the United States and Australia have similar legal principles to those of Canada, yet the apparent ease with which these principles were discarded in this example gives one pause for thought.

What can be done?

Given the prevalence of government surveillance techniques, and lawyers' obligations to protect solicitor-client privilege, what can be done? One likely cannot ensure that electronic communication is secure or that it is not being monitored by government surveillance. Every time data is moved – by email, by messaging, even if data is moved from one secure system to another secure system – it may be monitored or intercepted.

Obviously, the safest way to prevent government surveillance of lawyers' client matters is to not use computers. While that is obviously not very practical in today's world, lawyers should be discussing these issues with their clients. Perhaps the time is coming – or has come – where lawyers should consider whether it would be prudent to obtain client consent to certain storage methods.

The Canadian Bar Association has outlined some guidelines.[8] Generally, these guidelines look to ensure that passwords are secured, encryption is used where appropriate, that cloud computing resources do not interfere with client confidentiality, and that steps have been taken against inadvertent disclosure of data and the like. The Law Society of Upper Canada and the American Bar Association also have issued statements, guidelines, or rules on the subject. The CBA guidelines reference the commentary to Rule 1.1 in the American Bar Association's *Model Rules of Professional Conduct*, which was amended in 2012 to clarify that lawyer competence requires lawyers to keep abreast of benefits *and risks* associated with the use of relevant technologies.

---

[6] http://www.theguardian.com/uk-news/2015/feb/18/uk-admits-unlawfully-monitoring-legally-privileged-communications

[7] http://www.nytimes.com/2014/02/16/us/eavesdropping-ensnared-american-law-firm.html?_r=0

[8] *Legal Ethics in a Digital World* Report of the 2014-15 CBA Ethics and Professional Responsibility Committee (Part 1)

The Law Society has also issued guidelines on the use of cloud computing systems,[9] which require lawyers to be vigilant that the confidentiality of communications can be protected. These are not easy tasks in light of the Snowden revelations.

Following procedures such as these might, in the face of widespread surveillance, reduce the risks that such surveillance will capture communications that the government has no legal right to access. Discussing matters with clients may also help educate the public generally about the consequences that unlimited government surveillance may have on the rights and freedoms that individuals are supposed to enjoy in this country.

But beyond the ethical obligations that lawyers always have to be vigilante in preserving the confidentiality of client communications, the Committee is cognizant of underlying principles and the fundamental values of the confidentiality of such communications. Surveillance efforts – especially those undertaken by the state or its agencies - must recognize these principles and build in protections to reduce and ideally eliminate the risk of interceptions of lawyer-client communications. Legislators need to take them into account when preparing legislation that permits surveillance. How can these principles be advanced and enforced?

A Decision from Holland

By monitoring developments on this issue, the Committee learned that the question of surveillance by the Dutch government concerning interception of communications between clients and lawyers was before the Dutch courts. In a decision released recently,[10] the Dutch government was ordered to cease all interception of communications between lawyers and their clients when conducting state surveillance techniques. As noted in a news release by the Council of Bars and Law Societies of Europe[11] (which obtained intervenor standing in the case) the court ruled "that surveillance of lawyers by intelligence agencies constitutes an infringement of fundamental rights and [ordered] the State to stop all surveillance of lawyers' communications."

The Committee believes that this decision lends some useful legal weight to the position that governments must not, when conducting surveillance, interfere with fundamental values, including core legal values and fundamental principles of justice such as solicitor-client privilege.

[9] Report of the Cloud Computing Working Group, January 27, 2012
[10] http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2015:7436
[11] Press release, Council of Bars and Law Societies of Europe, July 2, 2015 *CCBE wins case against the Dutch State on surveillance of lawyers.*

Conclusion

Fundamental values and core principles like solicitor-client privilege can be under attack – either intentionally or unintentionally –by organizations with highly sophisticated technical capabilities and financial means to access information. These include state bodies having secret investigatory powers. This presents dangers to rights and freedoms of clients of lawyers in Canada and adversely affects the rule of law. The Committee urges that lawyers be cognizant of these risks, and believes that they should consider discussing the risks with their clients. Ideally, the Committee would prefer that all state institutions take steps to protect and enhance confidentiality of lawyer-client communications when modern technology is used.

This is an issue that the Committee will continue to assess and very likely bring before the Benchers for discussion in an effort to identify some principles for the protection of solicitor-client confidentiality and privilege in light of wide-spread surveillance efforts particularly when undertaken by the state. Possibly these would extend to advocating for a cessation of surveillance of known communications between clients and their legal counsel and to build in legislative requirements and protections to such ends.

Committee members would welcome your views on this issue.[12]

[12] Committee members include David Crossin, Q.C. (Chair); Leon Getz Q.C. (Vice-Chair); Craig Ferris, Q.C.; Gregory Petrisor; Jan Lindsay Q.C.; and Jon Festinger, Q.C.