ONTARIO BAR ASSOCIATION
A Branch of the Canadian Bar Association

PUBLIC SECTOR LAWYERS

February 2013 Public Sector Lawyers' Section

Keeping Up is Hard to Do: Current Issues in Electronic Government

John D. Gregory

Like the rest of the world, governments rely on electronic communications more and more, both for internal operations and for dealing with the world outside – the people they govern. Here are a few developments in the legal landscape in which those communications operate. Long-standing obligations of government – authentication and privacy – encounter new challenges, and new phenomena – social media – rewrite the playbook almost week to week. The lawyer's work is never done. Fortunately, it's often rather fun.

1. Authentication

It is often important for government to know who it is dealing with – though not always, and some thought has been given to providing access to some public information without asking the identity of the person with access. It is also often important for people dealing with government to know for sure that they are getting the official information.

These needs have often been dealt with through in-person identification measures accompanied by the provision of communications codes, e.g. log-in information or passwords that allow for access after original enrollment. Thus one can amend one's income tax information or the bank to which refunds are paid, if one can properly authenticate oneself with information very unlikely to be available to anyone but the taxpayer concerned.

'Federated identity' systems

There has been some progress in recent years helping governments authenticate people dealing with it. In particular, work has been done on 'federated identity' systems, which are systems that rely on other systems' evidence of authentication. For example, the Government Digital Service of Cabinet Office in the United Kingdom is working on letting people access government information if they prove who they are by use of third-party authentication. A person might use his or her Facebook credentials to show who they were, or banking credentials. The third party never finds out what the person is asking the government for or sees the information requested. A brief description is here.

This way, the government does not have to create a universal identity data base, or the digital equivalent of a national identity card – something that many states have but that people in countries of the Anglo-Saxon tradition seem to be very unwilling to see created.

Proxy systems

Another, similar method of authenticating people for government purposes is through trusting proxies, other entities that appear to be reliable sources of identification. For example, California allows for online applications for student loans. The applicant must provide identification details from an eligible educational institution and have an account at a participating financial institution. The lending authority calculates that if the university and bank agree on who the person is, so can the state. Further, the money lent is paid first to the university and only the balance is paid to directly to the bank. Thus the chances of 'extra' money being available is small, and it is scarcely worth the effort to figure out how to defraud the system.

Electronic signatures

A traditional way for people to demonstrate who they are, and to associate themselves with a document or other information, is a signature. Electronic signatures have drawn a lot of technical and legal attention from the early days of electronic commerce and electronic government. Since the law does not require a signature to take any particular form, though, it seems likely that electronic signatures have always been valid in law. In any event all Canadian jurisdictions have legislation to validate them, just in case. (The rules are largely but not entirely uniform, and in particular the federal rules are significantly different.)

In September, 2012, the Canadian Centre for Court Technology published its Analysis of Digital and Electronic Signatures in the Canadian Justice Sector, a study of electronic and digital signatures in the justice sector. Much of its analysis could extend to any public sector use of e-signatures. The document reviews legal and technical aspects of e-signatures. It points out correctly that the convenience or ease of use of a signature method usually varies inversely to its security. Secure systems are just not very convenient.

People responsible for designing authentication systems in the public sector therefore need to decide how important security is for them, being careful not to overstate the need, and design signature systems accordingly. This may require more than one signature system in the justice sector – and in the public sector generally. That would accord with what we already have, which is diversity.

The CCCT paper spends some time wondering about the legal validity of e-signatures. In my view that debate is over, if it ever needed to start – except where there is restrictive legislation, as with Part 2 of the PIPEDA, the federal statute. E-signatures are valid in law; the question is what is prudent in practice.

Electronic and online voting

The recent US federal election demonstrated that using voting machines, whether for remote or in-person voting, presents opportunities at least for controversy if not for fraud. The problems have not been solved here either. To save space, here is a commentary on why Internet voting is not the same – basically not as easy – as online banking.

2. Privacy

The public sector has been bound by privacy rules for decades, longer than the private sector for most purposes. The evolution of technology and the evolution of the law have created new issues for these long-standing obligations.

The nature of personal information

Canadian privacy law focuses on the collection, use and disclosure of personal information, or personally identifiable information. It therefore applies more broadly than some U.S. rules that focus on particular kinds of information, like details about a person's driver's licence, social security entitlements or credit cards. It is still important to recognize the increasing scope of data caught in the broad concept of personal information. The power of modern computers to capture, aggregate and analyze apparently random bits of data enables business and government to put a lot of formerly unavailable or meaningless information into a personal profile: browsing habits, including what sites are visited in what order, what searches are asked for and what results are followed up; what advertisements are clicked; what spending is done on different sites.

The spread of smart phones generates constant information about the location of the phone, information needed at any time the owner might want to use the phone to find the nearest transmitter. This information can be used to track people's movements. Social media that invite people to announce their location adds to the data available, as people 'check in' from restaurants, movies, stores and vacation spots.

Whether people online – or just carrying their phones – can be said to consent to the collection of this information is an open question. How much of such a consent can be implied from the necessary operation of the technology, and how much must be express and informed? The European Union has rules about the prior consent needed for web operators to put 'cookies' on people's computers – a basic enabler of personal service, but also a potential spying function. How this will work in practice is still under debate. Likewise the operation of Canada's anti-spam law – not yet in force – has given rise to vigorous discussions based on convenience but also likelihood of consumer understanding of the power of the technology in his or her pocket, purse or laptop.

Ontario's Information and Privacy Commissioner has for some years advocated 'privacy by design' – build in the privacy protection when one is building the technology itself, rather than trying to figure out afterwards how to protect privacy. The phrase is very widely adopted. It is not completely clear, however, whether governments for themselves or as

regulators have come to terms with how broadly it must be implemented or with the threats to privacy as technology develops.

The expectation of privacy

Many discussions of the legal right to privacy make that right depend on the person's expectation of privacy. If one does not expect one's personal information to be private, one has no right to object to its collection, use or disclosure – at least for the purposes that one expects it to be used for. Such a principle can become a self-fulfilling prophecy, and a downward spiral: the less one expects, the less one is protected, and the more one knows the capacity of the technology to violate one's privacy, the less the law will do to help.

Courts have tried to find a reasonable balance in this dynamic, and have talked about information essential to one's core of personality as being particularly protected, as distinct from information about unimportant activities. The Supreme Court of Canada has played a major role in the discussion, approving of dealing with readings of power meters to the home (Gomboc), readings from heat sensors flown over homes by aircraft (Tessling), and seizure of garbage by reaching over the property line (Patrick), but disapproving of the use of drug-sniffing dogs in bus stations (Kang-Brown), as well as adjudicating on other more or less sensitive situations.

The most recent decision was Cole, where an employee was held to have an expectation of privacy in personal information in a computer supplied by his employer for work purposes. Some personal use was permitted. So employer supervision or access rights are not unlimited, despite ownership. It may be noted, however, that incriminating information discovered by the employer's IT department was allowed to be disclosed to the employer; the police at that point should have sought a warrant – but in this case the evidence was held admissible anyway. So a right in principle may or may not be maintainable in practice.

Another area that has been litigated in the US between employers and employees is the claim of privilege, when an employee uses a workplace email system to communicate with a lawyer about an employment issue. Does the employer's ownership or right to monitor employee communications trump solicitor-client privilege? The better answer seems to be that privilege prevails, but the cases are not consistent. There are Canadian cases too.

Not all private messages are protected, though. Non-privileged personal communications that violate employment policies may lead to discipline. Employers do not have all the cards, but employees should not count on protection in every case.

Law enforcement

Everything one does online leaves traces somewhere. Individual computers that connect to the Internet are identified by a unique Internet Protocol (IP) address. Question: can the police follow those traces? Can they find out who made them? These issues continue to be litigated, and legislated.

On the legislation front, the Cybercrime Convention to which Canada is a party requires member states to require Internet intermediaries (e.g. Internet service providers) to retain traffic information for fixed periods, such as six months or two years. The government of Canada has introduced several 'lawful access' bills to require maintenance of such records (generally without compensation) and access by law enforcement officials to it, without a warrant. The most recent version of such legislation was Bill C-30, which became controversial when the Minister of Public Safety claimed that any opponent of the bill was in favour of child pornography.

Even without the legislation, police have largely succeeded in court cases where they have asked ISPs for the name and address of the individual subscriber associated with an IP address. Some ISPs sometimes ask for a warrant, but many simply hand over the information. Bill C-30 would require them to do so. Law enforcement officials claim that the information is no more private than a name, address and phone number available in a telephone directory. Privacy advocates say that the ubiquity of the IP address allows someone to trace the activity of a particular computer all over the Internet, and knowing the identity of the subscriber essentially puts all that tracking ability into the hands of the police – something that would need a warrant offline.

The most recent case in the Ontario Court of Appeal allowed the police to collect and use this information on the ground that there was no reasonable expectation of privacy in it. (To some extent child pornography is the 'universal solvent' of legal rights; few barriers survive the search for it. See also the discussion of *Cole* above.)

Mobile phones are a rich source of data for law enforcement. Not only do they allow police to trace where the owner has been (and the phone companies tend to hand over that information without compulsion of law), but they can provide a record of all calls made. The courts have tended to hold that police who seize a phone may search it – even though smart phones are the equivalent of a fairly strong computer – and in one recent US case, have allowed the police to make a call to a number shown on the phone, set up a drug deal, then arrest the person who answered the call and provided the drugs. An Ontario court took the opposite view and Canadian telecom companiessay they do not give out this information without a warrant.

Email security has been in the public eye since the Director of the CIA found his private emails in the press – after being located by the FBI. This raises intersting privacy issues as well, including the willingness of intermediaries to turn over the information on request by police investigators.

The obligations of governments to respect privacy and the desire of law enforcement bodies for information that would otherwise be private are not readily reconciled. The law must be considered to be in evolution on both these fronts.

3. Social media

Social media are the hot topic in the regular media, and often on the stock market, these days. (I defend my use of the plural on grounds both of etymology and of diversity of the

media in question.) Social media are characterized by interactivity – many-to-many communications – and by reliance on user-generated content. They appear to offer a 'public intimacy' that can lead to informality and indeed careless use that in turn can lead to legal problems.

Employment issues

One of the areas where social media create legal issues is in employment law, and governments are employers too. What are the duties of an employee in using social media? Criticisms of one's employer on Facebook, for example, have been found to justify dismissal, and comments about fellow employees have been held able to justify sanctions against the employer for allowing a poisoned work environment. Employees can put employers at risk as well by untoward publication of confidential information or simply disrespect to clients, customers or the public.

An employee starting a Twitter account to communicate for the government should be bound by contract to give it up at the end of his or her employment, though Twitter allows only personal accounts. Public servants frequently have 'professional' sites at LinkedIn that presumably travel with them as they leave public service – but is that clear to all concerned? Private parallels have led to litigation in the US.

Limits to interactivity

Ontario Deputy Ministers have been requested by Cabinet Office to 'engage with' Twitter. However, up-to-the-moment interactivity is hard to manage in an environment where one needs three levels of approvals to say anything in public. Governments using Twitter or other social media tend to use them for pushing out announcements, a parallel path for news releases, rather than for active discussions with stakeholders or the public. Some attempts have been made to use social media technology for internal discussions among public servants across departmental boundaries; it is too early to tell if some of the promising results can be maintained or whether they are a novelty effect only.

User-generated content can be problematic for governments as well. Offensive comments on a government blog may have political as well as legal consequences. Does government have the will and the resources to monitor comment sites effectively, and is it liable for the content if it does not?

The social media are distinct from using the Internet to solicit feedback on government proposals. That kind of system can work reasonably well, and several governments in Canada are using that system. See for example Ontario's Regulatory Registry, and before that the Environmental Registry. The 'open data' movement is hitting municipalities first in Canada. Allowing access to municipal information invites members of the public to aggregate and rework it for public-interest ends (as well as for private profit, no doubt).

Indemnification

Both provincial and federal departments may be strictly limited in agreeing to indemnify outside bodies for harm done to them. In Ontario, the Financial Administration Act bans any such agreement without the written consent of the Minister of Finance. But signing up for most social media sites requires agreeing to terms of use that include indemnification of the site owner against harm from bad conduct by the member, whether defamation, infringement of intellectual property, or otherwise. If such clauses are unenforceable because of the statute, does the whole agreement fail?

4. Conclusion

Governments have tended to follow their citizens online, to communicate with them and to provide them services. Over time, public sites have become more interactive, though how the interaction works can be problematic at times. The need for authentication is sometimes re-examined, and some of the methods of getting there are taking interesting turns. The demands for privacy are often difficult to meet, and there is some conflict between the abstract right to privacy and people's apparent willingness to lay out their personal information for all to see – and law enforcement officials are among those interested. The explosion of social media invites governments once again to follow their subjects, but the pitfalls are novel and numerous.

In short, the student or the practitioner of the law of electronic government will not lack material of great interest and greater challenges.

Sources: A collection of writing from the same author is available at www.euclid.ca

The views expressed here are not necessarily those of the Ministry.

John D. Gregory is General Counsel in the Justice Policy Development Branch, Ministry of the Attorney General (Ontario). After clerking for the Chief Justice of Canada, he was called to the Bar in 1977. He chaired the working groups of the Uniform Law Conference of Canada that produced the Uniform Electronic Evidence Act and the Uniform Electronic Commerce Act, both widely adopted across the country. From 1997 to the present he has been a member of the Canadian delegation to the United Nations Commission on International Trade Law (UNCITRAL) working group on electronic commerce.

John is on the Editorial Advisory Board of the Canadian Journal of Law and Technology. He is active in the Cyberspace Committee of the American Bar Association (Section of Business Law). See www.euclid.ca.