Info Telecom

CTC Community of Telecommunications Consultants | neotelis

WITHIN

THIS ISSUE

FEATURES

Allstream and Cisco Bring UCaaS to Yellow Pages

Two years ago, Yellow Pages Group (YP) decided to simplify and standardize its telephony infrastructure to accelerate the transformation of its business model. Specifically, the company wanted to enhance employee collaboration to achieve productivity gains and increase profitability. The objective was to establish a common platform that was flexible and offered a range of powerful tools that provided the best return on investment. YP ultimately chose Allstream's Hosted Collaboration Solution (HCS). The planning and deployment process was done in collaboration between YP, Allstream and Cisco. In June 2014, HCS was simultaneously deployed for some 1,000 head office employees. There are now nearly 3,000 YP employees using HCS. "By deploying a unified communications as a service platform, employees have become more efficient and can concentrate on the tasks that contribute to YP's growth", said Luc Dubois, general manager of Infrastructure and IT operations at YP. According to Dubois, network management has become much easier since HCS was deployed, and costs are more predictable and flexible.

BILL C-51 AND THE TELECOM INDUSTRY

DAVID CROWE

David Crowe has been involved in the telecom, IT and wireless industries since 1984, and a consultant in standards, system design and numbering systems since 1992. He runs his own consulting company, Cellular Networking Perspectives, is on the board of IFAST (ifast.org) and is chairman of TIA subcommittee TIA TR-45.8. David is a member of the Community of Telecommunications Consultants (CTC) *and can be reached at (403) 289-6609 or David.Crowe@cnp-wireless.com.*

I first learned about Bill C-51 in 1995. It wasn't because I've got ESP, nor was it called Bill C-51 then. It wasn't even Canadian, it was American legislation known as CALEA – the Communications Assistance for Law Enforcement Act. I was young and naïve back then (I'm definitely not young any more), and I assumed that CALEA brought more wiretapping options. But all it actually authorized was more convenient access to communications by putting a giant plug in the switch site and sucking out whatever law enforcement authorities could persuade the phone company to give them.

It might have seemed, back in the days of analog, that law enforcement agencies didn't need the assistance of the cellular phone operators, they could just use an FM scanner to pick up any analog cellular channel they wanted. Technically, it was that easy, but practically it was impossible because phones moved between frequencies and cells frequently, so unless the target was stationary or you could physically follow them, you could not reliably monitor them. Certainly, it was possible to sit outside Buckingham Palace, the White House or Parliament and just scavenge tidbits of information but, to get access to cellular communications, law enforcement needed to target the switch, where the links from all the cell sites come together and where phone calls get connected to other networks. In the intervening twenty years, the network topology hasn't changed that much, even with text messaging and data – networks still need to concentrate traffic from cell sites, possibly with a copy being sent to law enforcement.

Newer technologies always introduce problems in terms of the two prevalent legal standards for eavesdropping. Think of the postal system. Getting access to what one could observe on the outside of a letter or parcel – the address, the return address, the date of mailing – was easy to justify, but steaming open the envelope to actually read the content required a higher legal standard. Applied to the wired phone system, the dialed number, the caller ID, the originating switch, the time and the duration were the envelope of the call (the metadata), while actually listening in on the content required a higher legal standard.

The first problem that came with the advent of cellular was the issue of location. Law enforcement wanted this to be part of the metadata, making it easy to obtain. But is this the cell site location, which only identifies a position within several square kilometers, or the GPS position, accurate within a few meters? Is it whatever is captured by the network during normal operations, or tracked in real time? The simple division between envelope and content breaks down with more complicated communications technologies. In the United States, this is still a contentious issue, with some judges ruling a warrant is necessary for GPS location, and some ruling that it's not. Canadian Bill C-51 treats historical location data as metadata (probably just cell site location), but treats real-time location tracking data more like content, requiring a specific judicial warrant.

While cellular phone calls weren't dramatically different than landline (they still had a dialed number, caller ID and time parameters), the concept of envelope versus content collapsed with IP-based data. In order to get the envelope of, say, an email, you need the entire content, with a promise from law enforcement to not look at the body of the message and any attachments without authorization. Thus we get to a place where, as Edward Snowden has shown us, law enforcement and intelligence agencies are sucking up vast quantities of data onto their servers, analyzing it, keeping the useful tidbits and promising to not look at or keep the rest. We are supposed to trust them, but it is clear there is no meaningful oversight. The FISA (Foreign Intelligence Surveillance Act) court in the United States, for example, rubberstamps court orders that cover virtually every call in one network over a period of time, without anyone representing non-governmental interests (such as our privacy).

The telecom and IT industry is caught in the middle. It provides the networks that are targets for eavesdropping, and manufactures the equipment that is used both in those networks and necessary for eavesdropping. Governments that do the eavesdropping are usually customers of the IT industry, big customers. And, even if a telecom company didn't mind losing its lucrative government contracts, they have ways to make you listen.

In 2013, for example, the US-based secure email

Learning the Alphabet

Google announced in August a major plan to simplify the structure of the much-diversified company. It will involve a separation of Google's non-core operations from its core Internet business, and will make all entities, including Google itself, wholly-owned subsidiaries of a new parent company named Alphabet. "Our company is operating well today, but we think we can make it cleaner and more accountable," said Google co-founder Larry Page in a statement. "Alphabet is mostly a collection of companies. The largest of which, of course, is Google. This newer Google is a bit slimmed down, with the companies that are pretty far afield of our main Internet products contained in Alphabet instead," he explained. "We are not intending for this to be a big consumer brand with related products – the whole point is that Alphabet companies should have independence and develop their own brands," Page added.

service provider Lavabit suddenly shut down. It appears that the only way for the government to tap one of their email accounts (probably Edward Snowden's) was to tap all. Rather than turn his company into a charade, the owner committed commercial hari-kari.

Life was easier when all the eavesdropping, authorized or not, was unknown to the public. The telecom industry was happy to let its customers bask in the bliss of ignorance, but once customers cottoned on to the amount of data being collected they started to demand more security. American companies started to lose business overseas. It was no longer just Chinese equipment that was viewed with suspicion. Companies were probably also upset that when the US National Security Agency (NSA) couldn't get what they wanted they just tapped unencrypted internal links.

It is worth asking why a lot of intelligence insiders want to monitor and store everything. For all the NSA's mass surveillance that sweeps up vast quantities of the communications of its own citizens, there are no terrorist attacks known to have been thwarted on the basis of this information. If the NSA leaked anything, it would be their own successes. But there are benefits to bulk collection apart from keeping the public safe. Bureaucrats can build a bigger empire by hypothesizing threats that require monitoring, something they don't yet have. And because their budget is often secret, as well as the nature of the postulated threats, and the surveillance techniques and targets, their cost to the taxpayer is relatively immune from criticism.

A common saying in the field of surveillance is "We used to be looking for a needle in a haystack. Now they're making the haystack bigger", and increasing the number of haystacks to look through. But are you willing to be the politician who wouldn't authorize a full search when it's discovered that the needle is in a haystack you were too cheap to pay for examining? If we think analytically, the chances of finding something useful decrease as you collect more. The mathematics of this is known as the Positive Predictive Value (PPV), a simple and powerful, but counter-intuitive, analysis. Let's say that one communication out of a billion contains evidence of a previously unknown terrorist plot. And our software is 99% accurate at determining whether a communication is innocent or nefarious. This means that out of one billion communications we will be faced with 10 million innocent communications flagged as potentially nefarious (1%)… and only one truly nefarious communication. We achieve a PPV of 1 out of 10 million with a test that's 99% accurate (that's the counter-intuitive part).

Furthermore, all the communications surveillance in the world is unlikely to detect the so-called lone wolf attacks, where someone, often mentally disturbed, decides on his own to cause mayhem. This appears to have been the case with both the Couture-Rouleau attack that killed Warrant Officer Patrice Vincent, and the Zehaf-Bibeau attack that killed Corporal Nathan Cirillo – cases that were used to justify Bill C-51. What we do see when a terrorist attack occurs is that details are uncovered almost instantaneously, because once the name of the perpetrator is known it is easy to go back through stored communications and precisely target what you missed before. But that's of little consolation to the victims. It could help catch the perpetrators but in most cases the perpetrators die in the attack (the Boston Marathon bombing in 2013 was a rare exception).

Most everyone supports the search for criminals and terrorists so they are likely to care little about the risk of surveillance on them. Because, after all, they're not doing anything wrong, so why should they worry? But governments now have huge power to go through a web of connections, and catch people up in guilt by association. And they have the power when any one of us runs for public office or becomes an effective government critic to comb through our history looking for one awkward thing to bring us down.

Maher Arar is a good example of an everyman, actually a telecom engineer, who was caught up in the so-called "War on Terror" when the United States decided to deport him to Syria where they knew he would be tortured, and the Canadian government, rather than squawking, did very little, as evidenced by the $10 million settlement and apology direct from the Prime Minister.

The alternative to mass surveillance is targeted surveillance, because doing nothing in a world that does have a good number of criminals and violent radicals is clearly not an option. More traditional policing and intelligence gathering, following leads and rumors, gathering public information, and trying to identify people behaving strangely, does work and doesn't require massive surveillance empires.

A good example of a plot that traditional methods probably stopped because it involved communications was the neo-nazi terrorist attack in Halifax thwarted in February 2015, only a few days before three conspirators allegedly planned a mass shooting. They left a significant footprint of disturbing imagery and comments on their social networks that could have (and probably did) justify any number of search and production warrants. And this was before Bill C-51 was passed, so clearly the additional powers were not necessary.

Bill C-51 is designed to do a lot of things that could affect telecommunications companies, including the

following, from the official parliamentary legislative summary, with emphasis added by myself:

- "Provide that hate propaganda offences can be committed **by any means of communications and including making hate material available**"
- "Create the offence of **possession of a computer virus** for the purpose of committing mischief"
- "Make it possible for law enforcement agencies to make a demand or obtain a court order **for the preservation of electronic evidence**"
- "Creating new judicial production order for obtaining **data relating to the transmission of communications or data for tracking a thing or individual**"
- "Create warrants for **obtaining transmission data in real time and for the remote activation of tracking devices** in certain types of technologies"
- "New production orders can be used by Canadian authorities who receive **assistance requests from other countries**"

In my non-legal opinion, this could have significant repercussions:

- Governments and judicial systems may decide that telecom companies are not just facilitators of communications, but they are also responsible for the contents. Ask Kim Dotcom, founder of Megaupload, who was accused of knowingly facilitating copyright infringement by providing a generic file sharing service and is now in New Zealand hoping that the US Department of Justice will not be able to extradite him – so far he's holding out now that he's back in his mansion after a (later ruled to be illegal) raid and arrest by men descending from real black helicopters.
- In the new world of cloud-everything, someone may well be creating and storing malware in your network or using your equipment. Could you reasonably have known this when something bad emerges?
- Cellular phone companies will be the target of more production orders for location information and for continuously reporting the location of a target. Bill C-51 could make it legal for Canadian authorities to implant malware to do this, likely needing cooperation of telecom companies.
- Telecom companies may be ordered to preserve data or, even if not asked, "a TSP [telecommunications service provider] may still voluntarily preserve data and provide it to a law enforcement agency, even where there is no demand or order." How voluntary is "voluntary" when men in dark suits with suspicious bulges come to your office and suggest that maybe, just maybe, it would be good for your long-term interests if you 'voluntarily' kept certain information. You might just decide to keep everything, much longer than you would prefer, meaning that your company will be doing the long-term storage of data on a large swath of Canadians that the government can then deny doing.

- Bill C-51 authorizes surveillance on behalf of foreign governments, not all of which have good human rights records.

I wasn't planning to write this article during a Canadian federal election, but I am. I really don't know whether C-51 will become an election issue (by the time you read this, you will know more than me), and even if it does I have no idea whether the discussion will influence the voting decisions of many Canadians. However, you should familiarize yourself with the Bill and if you really like it, and think it will keep Canadians safer, you know who to vote for (you know, the guy who really likes it, not the guy who said he disliked it but voted for it anyway). And if you really don't like it you should vote for the other guy (or the other gal), because they have been vocally and consistently opposed to it. And, if you're ambivalent, maybe vote for the ambivalent guy.

For a critique of Bill C-51, start with the writings of Craig Forcese, Associate Professor of Law at the University of Ottawa and Kent Roach, Professor of Law at the University of Toronto. In a June 2015 article, *Stumbling toward Total Information Awareness*, they wrote, "[C-51's concept of activities that undermine the security of Canada] is a new and astonishingly broad concept that is much more sweeping than any definition of security in Canadian national security law. In important respects, it comes close to a 'total information awareness' approach or, at least, a unitary view of governmental information holding and sharing. In that respect, we consider it a radical departure from conventional understandings of both national security interests and privacy."

On the other hand, Royal Military College Associate Dean and Associate Professor Christian Leuprecht wrote in the Globe and Mail: "Far from creating a police state, C-51 is merely getting Canada caught up to the rest of the civilized world. Most of [our allies] have long had in place the provisions in C-51 that have caused such heated debate in Canada: measures of detention that are clearly distinct from arrest, risk-diminishment mandates for security intelligence, more robust provisions to stop people from boarding planes, and very robust provisions for sharing data."

Telecom and IT companies are affected by legislation like Bill C-51 because, without them, the legislation cannot be implemented. If the past is a predictor of the future, telecom and IT companies will be getting more and more requests, although we are at a point where opposing currents are flowing, and it is also possible that countries will move to more targeted surveillance, with real oversight, and the load and moral burden on the telecom industry will be reduced. The reality will probably be a messy and flawed compromise.