GOVERNMENT SURVEILLANCE, HACKING, AND NETWORK SECURITY: WHAT CAN SUBMARINE CABLE OPERATORS AND THEIR CUSTOMERS DO?

Kent Bressie
Harris, Wiltshire & Grannis LLP
kbressie@hwglaw.com

Abstract: Tensions between network security, cybersecurity, and privacy on one hand and surveillance undertaken in the name of national security and law enforcement on the other have only grown more acute since September 11, 2001. Telecommunications providers remain caught in the middle, as uneasy partners in surveillance activities typically mandated by law and also as targets for spying. Government surveillance and access requirements can weaken security and undermine customer confidence. While some measures, such as encryption and robust network security protections, can help to protect operators and their customers, others, such as bypass infrastructure, remain mostly for show.

A fundamental tension exists between network security, cybersecurity, and privacy on one hand and government surveillance activities undertaken in the name of national security and law enforcement, on the other. For governments to have access, they must deprive bad actors of the ability to conceal their communications. Nevertheless, allowing for such access and gathering of data can itself create network and cybersecurity risks and new targets. This tension has become more acute after the September 11th attacks in the United States and subsequent attacks around the globe, with security becoming—and remaining—an overwhelming policy and regulatory priority for many countries. Governments have significantly expanded their surveillance activities to detect and monitor threats and called for new levels of access—particularly as electronic communications proliferate in more and more aspects of contemporary life.

Thanks to WikiLeaks and Edward Snowden, the extensive U.S. surveillance programs have received the most publicity, but they are not unique. Revelations about spying have placed submarine cable operators and their customers—whether traditional carriers or over-the-top providers—in the middle. They face erosion of customer confidence and potential legal claims. Governments have enlisted the telecom industry—willingly or not—to ensure access and to protect the confidentiality of such surveillance. In other cases, they have targeted the telecom industry. Submarine cable operators and their customers have little choice but to comply with domestic laws that enable surveillance and spying. Failure to comply can lead to prosecution and fines, loss of operating licenses, and/or loss of government contracts. Operators have responded with a variety of measures, some more effective than others, to protect themselves and bolster customer confidence.

1. AN ATTRACTIVE TARGET

Fiber-optic technology and encryption techniques have made surveillance and hacking of communications traffic on contemporary submarine cables more difficult, but not impossible, as compared with analogue, coaxial cables with unencrypted communications—as evidenced by disclosures in the mid-2000s about U.S. intelligence agencies using

beam splitters to access communications from trans-Pacific submarine cables. The United States pioneered tapping of submarine cables with Operation Ivy Bells, which targeted Soviet cables in the Sea of Okhotsk in the 1970s, and is alleged to have equipped its more contemporary submarine, the USS Jimmy Carter, with fiber-tapping capabilities. More recently, reports surfaced in late 2015 claiming that Russian ships were conducting reconnaissance near installed submarine cables serving the United States.

Certainly, submarine cables remain a focal point for network security and surveillance, not least of all because they aggregate so much information in discrete locations. They remain vitally important to national security and economic activity, and they carry the vast majority of the world's international Internet, voice, and data traffic—a fact that make them potentially attractive targets for causing harm and for gathering information to prevent harm. Developments in "fiber tapping" have made access to a fiber-optic cable's communications stream feasible. Applications of vast computing power and storage capabilities for breaking encryption and searching data have also opened up the possibility of access to vast communications streams that can provide law enforcement and intelligence agencies with reams of data.

2. AFTERMATH OF SEPTEMBER 11TH

The tension between security and access has become more acute in the last 15 years due to: the September 11th attacks in the United States and subsequent terrorist attacks around the world; wars (and their aftermaths) in Afghanistan, Iraq, Libya, Syria, and the regions occupied or threatened by the Islamic State or Boko Haram; and a rising tide of cyberattacks. Post-September 11th, many governments have significantly expanded their surveillance activities to detect and monitor threats.

Each new incident brings new calls for more extensive information and intelligence-gathering. The UAE Government cited the assassination of a Hamas official in Dubai in 2010 as justification for proposing a ban on Blackberry Messenger, email, and web browsing services pending negotiation of a compromise with Blackberry developer Research in Motion to obtain access to encrypted messages. Following the attack on *Charlie Hebdo*'s offices in Paris in 2015, the French Government proposed to adopt a surveillance law similar to the intrusive USA PATRIOT Act.

Intelligence agencies continue to demand that their governments ensure access. A number of intelligence agencies and observers have renewed calls for a backdoor mechanism similar to the Clipper Chip, a chip set developed by the U.S. National Security Agency ("NSA") that used an encryption key escrow to provide governments with a back door to access encrypted communications. In 2016, Microsoft continues to challenge U.S. Federal Bureau of Investigation ("FBI") attempts to access data stored in its Irish data center and assertions that the FBI can compel disclosure of data stored anywhere in the world if the provider is based in the United States. Also in 2016, the FBI remains embroiled in litigation with Apple, seeking to force Apple to unlock iPhones, particularly one used by one of the perpetrators of a bombing in San Bernardino, California in 2015.

3. ACCESS AND DATA CAN EASILY BE ABUSED

There is disagreement about what does and should constitute a bad actor sufficient to justify surveillance. Is a bad actor:

- An imminent security threat, such as a terrorist bomber or a proliferator of nuclear or biological weapons?
- An economic competitor?
- A government critic, political dissident, democracy activist, or a non-governmental organization like Greenpeace or Amnesty International?

Once access is created and data is gathered, there is always a temptation to use it—or misuse it—for other purposes. Government overreaching can undermine customer confidence, as it has done with U.S. cloud services providers following disclosures by WikiLeaks and Edward Snowden.

4. TELECOM AND ELECTRONIC COMMUNICATIONS INDUSTRIES: UNEASY PARTNERS, TARGETS, OR BOTH?

Telecommunications and electronic communications providers and infrastructure owners have long been caught in the middle of government surveillance activities. In some cases, governments have enlisted the telecom and electronic communications industries—willingly or not—to ensure access and to protect the confidentiality of such surveillance. AT&T and Verizon were accused of breaking U.S. law to cooperate with U.S. Government surveillance activities, and the resulting litigation was resolved only when the U.S. Congress changed the law in 2008 to grant retroactive immunity to the carriers. In other cases, the telecommunications and electronic communications industries have been the target of surveillance. Government security efforts will likely continue to focus on telecom and other electronic communications networks given the integration of electronic communications in almost all aspects of contemporary life.

WikiLeaks and Edward Snowden are largely—but not entirely—responsible for new public awareness of surveillance and spying. They also provide a misimpression that the United States is unique with its spying efforts, when in fact some U.S. efforts are simply the most exposed. These efforts include:

- **ECHELON**. This is the signals intelligence collection and analysis network of the "Five Eyes" (Australia, Canada, New Zealand, the United Kingdom, and the United States) dating to the 1960s. The United States later expanded ECHELON from original focus on diplomatic and military traffic to include private and commercial traffic. It long focused on exploiting satellite communications.
- **Xkeyscore**. This NSA data-retrieval system allows access to telephone calls, emails, social media, and metadata. It has been shared with the Five Eyes countries, Germany, and Sweden. The German Government, which objected strenuously to revelations that the United States had spied on the telephone conversations of Chancellor Angela Merkel, has ironically been the biggest paying customer for Xkeyscore data. In March 2015, the *New Zealand Herald* revealed that New Zealand's Government Communications Security Bureau ("GCSB") was spying on South Pacific island nations in exchange for access to Xkeyscore. The *Herald* revealed documents showing the tracking of the installation of Blue Sky's American Samoa Hawaii and

Samoa American Samoa cables, which GCSB feared would deprive it of access by replacing satellite connectivity.

- **PRISM**. This NSA program collects stored Internet communications of non-U.S. persons held by major U.S. Internet companies.
- **Room 641A**. This interception facility on AT&T's premises in San Francisco used beam splitters in fiber-optic networks—particularly submarine ones—to access IP-based traffic.

Revelations about spying have placed electronic communications providers in the middle. Carrier compliance with government requests has resulted in an erosion of customer confidence, particular for U.S.-based networks and cloud computing providers. Allegations of complicity with Chinese Government spying have largely foreclosed access to the U.S. market by Huawei Technologies.

Operators must comply with domestic laws that enable surveillance, although customers and NGOs have sometimes disagreed with operator assertions that the law required disclosure. Failure to comply can lead to prosecution and fines, loss of operating licenses, and loss of government contracts.

5. LIMITED RECOURSE FOR GOVERNMENT OVERREACHING

Telecommunications operators have limited recourse for government overreaching. They can mount legal challenges to a government's request for cooperation—but only in jurisdictions where such challenges are permitted. Even in the United States, industry has limited options for challenging national security-related requests in the U.S. Foreign Intelligence Surveillance Court. Telecommunications operators can also seek legislation granting immunity from private lawsuits. Consumers and residents of foreign countries have little or no recourse. For the most part, foreign governments can only raise objections at the diplomatic level or expel suspected spies, although the new EU-US Privacy Shield—adopted to replace the Safe Harbor agreement struck down by the European Court of Justice—bars the United States from conducting "indiscriminate" national security surveillance of Europeans and requires the U.S. Department of State to appoint an ombudsman to police compliance.

6. PROVIDER RESPONSES TO SURVEILLANCE AND SPYING

Governments will continue to conduct surveillance and hack as they always have. Although operators have limited leverage in challenging domestic legal requirements, they can bolster defenses against hacking and legal requirements that could weaken security. Some measures are more effective than others. Other measures are "for show" politically and ineffective.

(a) ***Bypass Infrastructure***. In response to revelations that the U.S. intercepted telephone conversations of Brazilian President Dilma Rousseff, Brazil implemented bypass measures to avoid routing communications through the United States. It has also actively promoted new submarine cables that would link Brazil directly to Europe. Bypass strategies ignore the fact that most government spy agencies operate beyond the boundaries of their home countries. Bypass is not a viable option if your customers want to access content stored in a country accused of spying. Given the

proliferation of new cables on the U.S.-Brazil route—including BRUSA, Monet, and Seabras-1—one must wonder whether the Brazilian Government's official policy is getting any traction.

(b) ***Data Localization and Data Sovereignty***. Data localization requires that data of a country's residents or citizens be stored in that country. A number of countries, including Brazil, have proposed this as a remedy for U.S. spying. While data localization might benefit local data-center operators, it is technically inefficient and potentially more expensive. It is disliked by civil libertarians and democracy activists, as it potentially enables political oppression of government opponents and dissidents by ensuring that communications from government critics are locally available. The United States has strongly opposed the adoption of data localization requirements and has sought to include provisions in the Trade in Services Agreement to mandate the free flow of data.

(c) ***Encryption***. More than anything else, government surveillance agencies remain highly concerned about the proliferation of encryption technology. They worry that bad actors will "go dark," *i.e.*, communicate only with encrypted communications so as to avoid detection altogether. The U.S. Government had long tried to assert that privately-developed encryption technology was classified and/or stolen, and it still subjects U.S.-origin encryption source code to U.S. export controls. Companies such as Apple and Yahoo have promoted encryption, including end-to-end encryption, in which a company could not provide the government with a master key.

(d) ***Robust Network Security and Cybersecurity Measures***. Many operators make themselves targets for hacking by bad actors and intelligence agencies by failing to maintain robust network security and cybersecurity policies and procedures. Operators can make themselves less attractive targets and better protect their businesses by adopting and implementing: security and privacy programs; vendor assurance programs for hardware and software; incident response plans; policies defining how threat and incident information will be shared with governments; and customer assurance programs.

(e) ***Litigation and Public Advocacy***. U.S. technology companies such as Microsoft, Yahoo, Google, and Cisco—all competing to maintain customer confidence—have systematically sought court rulings and negotiated with the U.S. Government to promote transparency through the disclosure of statistics regarding U.S. law enforcement requests. The clearer government practices are, the easier it is to structure services and operations and reassure customers. They have also vigorously opposed the addition of government backdoors to circumvent data protection mechanisms.

(f) ***International Agreements***. Microsoft has called for the adoption of an international convention on government access to data, an arrangement that would narrow access to address clear-cut law enforcement and national security concerns while speeding cross-border sharing of information that might otherwise be rendered less valuable as a result of procedural delays.