‘Going Dark’ Versus a ‘Golden Age for Surveillance’

by Peter Swire, Kenesa Ahmad
November 28, 2011

Law enforcement and national security agencies are worried that they are “going dark” due to new technology. Their fear is that they will not be able to wiretap and decode new forms of Internet and other communications. This concern is correct in certain respects. In some instances, agencies do lose access to categories of information they previously relied upon.

This post, however, argues that “going dark” is the wrong image. Instead, today should be understood as a “golden age of surveillance.” Compared with earlier periods, surveillance capabilities have greatly expanded. Consider three areas where law enforcement has far greater capabilities than ever before: (1) location information; (2) information about contacts and confederates; and (3) an array of new databases that create “digital dossiers” about individuals’ lives. This information about any individual suspect is made even more useful because of the way data mining can help identify suspects.

The battle between the images of darkness and light is important. If the overall truth were that agencies are “going dark,” then legislatures and agencies would have an important argument for expanding surveillance powers. On the other hand, careful review of the facts shows that we do live in a “golden age of surveillance.” Skepticism should accompany agency requests for new powers. Our current research, and this post, explains why we should be skeptical about the bad encryption rules being instituted in India, China, and other nations around the world. We are undertaking ongoing research on encryption, lawful access, and globalization. More broadly, the existence of a “golden age of surveillance” supports efforts such as the Digital Due Process Coalition [3], which is seeking to reinstitute protections for our communications and personal data in our modern networked environment.

The “Going Dark” Problem

Law enforcement and national security agencies object to the use of strong encryption in electronic communications for one main reason: The agencies are losing some surveillance capabilities they previously relied upon. Wiretaps and relatively easy access to stored records have historically been important tools for these agencies. When strong encryption is used to secure emails or mobile phone calls, agencies can access the communications but are unable to decipher their encrypted forms. If agencies gain access to encrypted laptops or other forms of encrypted data at rest, the lawful interception process is similarly frustrated.

In 2011 testimony, FBI General Counsel Valerie Caproni described the problem: “We call this capabilities gap the ‘Going Dark’ problem. As the gap between authority and capability widens, the government is increasingly unable to collect valuable evidence in cases ranging from child exploitation and pornography to organized crime and drug trafficking to terrorism and espionage—evidence that a court has authorized the government to collect.”

“Going dark” is an evocative and compelling image. The phrase invites us to imagine communications shrouded in darkness—cloaked in encryption—so that the eyes of the agency are blind. Although we may want justice to be “blind” in order to achieve impartiality, we surely do not want our police to be blind.

In the 1990’s, the “going dark” argument was often made by the FBI and NSA, although the term itself was not widely used. In 1994, the Communications for Law Enforcement Act was passed to address FBI concerns that the shift from copper wires to fiber optics made traditional phone wiretaps less useful. The NSA’s ability to collect communications was threatened during this period as a greater proportion of international calls shifted from

radio communications (often easy to intercept by the agency) to fiber optic cables (generally easy to intercept only at a switch controlled by a telecommunications company). Coupled with the rapid development and widespread availability of strong encryption, the agencies faced the likelihood that many communications would not be as readily accessible as before.

Despite these risks, in 1999 the U.S. government decided to embrace the use of strong encryption. Arguments in favor of Internet security, civil liberties, and international trade prevailed over the surveillance agencies' objections. The government ultimately recognized the private sector's need for and dependence on strong encryption, and identified the inherent value in using strong encryption for law enforcement and national security purposes. Despite losing what were termed the "crypto wars," important agency concerns were addressed. The FBI received enhanced funding for its technical capabilities, and this funding has continued to grow over time. Together, government and industry leaders worked to develop the system of public-private partnership that continues today, in which industry experts meet with the government about encryption and technology for the carrying out of lawful intercepts.

Today as a "golden age for surveillance"

The Internet and the advancement of IP-based communications present new obstacles to lawful interception. At the same time, these developments provide law enforcement and national security agencies with powerful new surveillance capabilities. The discussion here highlights three areas where law enforcement has far greater capabilities than ever before: (1) location information; (2) information about contacts and confederates; and (3) an array of new databases that create "digital dossiers" about individuals' lives. This information about any individual suspect is made even more useful because of the way data mining can help identify suspects.

We are in a new age where most people carry a tracking device, the mobile phone. Location information comes standard with a wireless network – the phone company needs to know where your phone is to send you the call. A specific cell handles the call, so the network knows what cell you are in. Location information is tremendously useful for law enforcement and national security agencies. It can put a suspect at the scene of a crime, or establish an alibi. It can act as a "bug" without the need for the agency to place a bug on the suspect's person or property.

The precise rules for storing this location data vary by jurisdiction and wireless carrier. In many instances, though, the routine practice is that location data is stored for a significant period of time. Carriers in the U.S. are subject to data preservation orders, so location information on known suspects is retained once a proper agency request has been made. The number of requests from law enforcement for such location information has climbed sharply in recent years according to statistics in the U.S.

It is true that the cautious suspect can try to avoid this location tracking by using a prepaid cell phone or not carrying the phone when doing criminal activities. Some countries have placed limits on non-identified mobile phones, however, and the suspect has to worry that his or her confederates will show up at a meeting carrying their regular mobile phones. More generally, a tremendous number of people now carry cell phones as they go through their daily lives. Location information thus becomes available for surveillance purposes in ways never before possible.

Information about a suspect or witness' confederates is the second category of information newly available in rich detail to the agencies. For many investigations, *who* is called is at least as important as *what* is said in the call. The investigator gets leads on whom else to investigate and can follow those leads to the contact's contacts, and so on.

The importance of confederates has become famous in social networking. The term "social graph" was coined, in connection with social networks to describe the phenomenon of "the global mapping of everybody and how they're related." [4] For investigatory agencies, mapping everybody and how they are related is extremely useful. Social networking sites themselves will become an increasingly important source of investigatory material in coming years. The phenomenon is much broader, however:

- A generation ago, long-distance phone calls were expensive, and international calls a rare event in most people's lives. As costs have plummeted, the volume of local, long-distance, and international calls has grown dramatically. Calling records show the "to/from" information for calls already made, pen register orders reveal who a person is calling, and trap-and-trace orders show who is calling the person. The number of such orders in the U.S. has climbed sharply.
- The explosion of mobile phone use has supplemented the rise in wireline calls, and mobile use continues to increase rapidly. India, for instance, is showing an astonishing 17 million new wirelines per month in 2011.
- E-mails have become a pervasive feature of life for many people. The emergence of global web mail providers including Gmail and Hotmail gives investigatory agencies the convenience of serving many lawful requests to a small number of providers.
- The rise of unlimited text messaging plans in many jurisdictions provides numerous clues about a person's key confederates, and the time and date of their communications.
- VOIP (voice over Internet Protocol) calls are growing rapidly. Skype was sold to Microsoft for $8.5 billion in 2011. Even for calls whose content is encrypted, Skype connects the callers and the "to/from" information is subject to legal process.

These wireline calls, wireless calls, e-mails, texts, VOIP calls, and social networking records are treasure troves of information for investigatory agencies. In the bygone era of face-to-face communications, no trace was usually left regarding whom a suspect had talked with. Today, by contrast, an individual would need to abstain from many everyday activities to prevent the government from obtaining information about his or her contacts. The identity of those contacts helps lead investigators to additional targets of interest, thereby painting a broader and more precise picture of potential criminal or national security activity.

Information about location and a person's confederates, in turn, are simply examples of the larger trend towards detailed personal records. Consider the amount of information stored on an individual's personal computer. A standard laptop today often holds many gigabytes of data, more than a mainframe computer held 20 years ago. If the government obtains access to an individual's personal computer, it is highly likely that the computer will reveal detailed and diverse records about the person's life. The records retained on that computer, in turn, are only a small subset of the records stored on other computers – banks, hospitals, online advertisers, data brokers, government agencies, and other record holders possess exponentially more detailed data on individuals than in the past. Although a few people attempt to live "off the grid," this is not a feasible option for the vast majority of citizens in developed countries. Once an individual is identified as a target, the government–via lawful process–can access detailed information specific to that individual.

We live in a "golden age for surveillance" because investigatory agencies have unprecedented access to information about a suspect. In addition, data mining provides unprecedented tools for identifying suspects.

Choosing between "going dark" and "a golden age for surveillance"

This post argues that the big picture for agency access to data is mostly "golden." The loss of agency access to information, due to encryption, is more than offset by surveillance gains from computing and communications technology. In addition, government encryption regulation harms cybersecurity. These conclusions will not be easily accepted by investigatory agencies, however, so it is important to work through the analysis in more detail.

Communications that were previously subject to wiretap may now be shrouded in encryption. In place of the old monopoly telephone network, agencies have to contend with a confusing variety of communications providers, some of which have little experience in complying with legal process. It is no wonder agency officials strenuously object to the use of new technology that hinders their ability to employ traditional surveillance methods.

Implementing wiretaps and reading the plaintext of communications are not the only goal, however. The computing and communications infrastructure are vital to economic growth, individual creativity, government operations, and numerous other goals. If there is a modest harm to investigatory agencies and an enormous gain,

societies should choose the enormous gain. In 1999 the U.S. government concluded that strong encryption was precisely that sort of valuable technology – it was worth going at least slightly "dark" in order reap the many benefits of effective encryption. Not even the attacks of September 11, 2001 changed that judgment.

The evidence suggests, furthermore, that the degradation of wiretap capability has been modest at most, and—at least statistically—wiretaps have become more useful over time. The number of wiretap orders implemented in the U.S. has grown steadily the last two decades. According to publcally available statistics, court approved wiretaps are now at a record high: 3,194 wiretap court orders were issued for the interception of electronic, wire, or oral communications in 2010, a 34% increase from the 2,376 issued in 2009. In the six instances where encryption was encountered, it did not prevent law enforcement from retrieving the plaintext forms of communication.

These numbers actually understate the expansion of wiretapping in the U.S., in part due to the shift to "roving" wiretaps. In earlier years, separate court orders were required for each device used by the target of an investigation. Over time, however, Congress authorized roving wiretaps so that one wiretap order could apply to all the devices used by a suspect. Additionally, wiretaps were authorized by investigation, rather than for each individual target within an investigation. This means that the statistics understate the growth in actual use of wiretaps.

What explains the agencies' sense of loss when the use of wiretaps has expanded, encryption has not been an important obstacle, and agencies have gained new location, contact, and other information? One answer comes from behavioral economics and psychology, which has drawn academic attention to concepts such as "loss aversion" and the "endowment effect." "Loss aversion" refers to the tendency to prefer avoiding losses to acquiring gains of similar value. This concept also helps explain the "endowment effect" – the theory that people place higher value on goods they own versus comparable goods they do not own. Applied to surveillance, the idea is that agencies feel the loss of one technique more than they feel an equal-sized gain from other techniques. Whether based on the language of behavioral economics or simply on common sense, we are familiar with the human tendency to "pocket our gains" – assume we deserve the good things that come our way, but complain about the bad things, even if the good things are more important.

A simple test can help the reader decide between the "going dark" and "golden age of surveillance" hypotheses. Suppose the agencies had a choice of a 1990-era package or a 2011-era package. The first package would include the wiretap authorities as they existed pre-encryption, but would lack the new techniques for location tracking, confederate identification, access to multiple databases, and data mining. The second package would match current capabilities: some encryption-related obstacles, but increased use of wiretaps, as well as the capabilities for location tracking, confederate tracking and data mining. The second package is clearly superior - the new surveillance tools assist a vast range of investigations, whereas wiretaps apply only to a small subset of key investigations. The new tools are used far more frequently and provide granular data to assist investigators.

Conclusion

This post casts new light on government agency claims that we are "going dark." Due to changing technology, there are indeed specific ways that law enforcement and national security agencies lose specific previous capabilities. These specific losses, however, are more than offset by massive gains. Public debates should recognize that we are truly in a golden age of surveillance. By understanding that, we can reject calls for bad encryption policy. More generally, we should critically assess a wide range of proposals, and build a more secure computing and communications infrastructure.

For tech policy updates, follow us on Twitter at @CenDemTech [5].

Source URL: http://www.cdt.org/blogs/2811going-dark-versus-golden-age-surveillance

Links:
[1] http://cdt.org/cdt-fellows-focus
[2] http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1960602
[3] http://digitaldueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163
[4] http://www.cbsnews.com/stories/2010/04/21/tech/main6418458.shtml
[5] http://twitter.com/#%21/CenDemTech