7

Dark Dimension of Technology

"Terrorists use the Internet just like everybody else"
–Richard Clarke (2004)

7.1 Introduction

Conversations around surveillance focus mostly on the use of encryption in communications technologies. This debate has caught increasing attention due to the decisions of Apple, Google, and other major providers of communications services and products to facilitate end-to-end encryption in certain applications, on smartphone operating systems, while terrorist groups try to use encryption to hide their communication from surveillance.

Most recently, terrorist attacks in San Bernardino and Paris along with increasing concern about the terrorist group ISIS have shifted the focus onto the issues of surveillance and encryption. These developments have led to new invitations for the government and private sector to work together on the going dark issue.

According to Resnick (1999), there are types of Internet politics. Resnick defines "Politics within the Net" as the political life of online communities and related activities that impact the life off the Net only to a minimal extent. Another category that Resnick (1999) defines is "Politics which Impacts the Net" that involves policy issues emerging due to the use of the Internet as both a means of mass communication and a tool for business. The last category that Resnick (1999) defines is "Political Uses of the Net," which involves the use of the Internet by citizens, activists, or government to fulfill political goals that don't relate to the Internet *per se*. In other words, this relates to influencing political activities offline (1999, pp. 55–56).

This section mainly focuses on the third category,' especially terrorist' use(s) of the Internet.

Rash (1997), referred to eight different uses of the Net by political groups and categorized them as follows:

- Tactical communications,
- Organization,
- Recruitment,
- Fundraising,
- Strategic positioning,
- Media relations,
- Affinity connections, and
- International connections (1997, pp. 176–177).

Similarly, in terms of the main uses of the Net by terrorists, Furnell and Warren (1999) made the following classification: propaganda/publicity, fundraising, information dissemination, and secure communications (1999, pp. 30–32).

While Cohen (2002) provides his readers with a similar list of uses (pp. 18–19), Thomas (2003) explains the terrorist uses of the Net in more detail. In addition to his discussion of several possible terrorist' uses of the Internet, Thomas (2003) refers to "cyberplanning" as the digital coordination of a comprehensive plan across geographical boundaries that may or may not result in bloodshed (p. 113).

Furthermore, Weimann (2004) refers in one of his reports for the US Institute of Peace to the following ways of the terrorists' use of the Internet: psychological warfare, publicity and propaganda, data mining, fundraising, recruitment and mobilization, networking, information sharing, and planning and coordination (pp. 5–11).

Given this overlap among the uses of the Net by terrorist, Table 7.1 analyzes and explains in more detail these classifications.

The vents with regard to the introduction of built-in encryption by Apple, Google, and other technology companies can be summarized as follows:

- In September 2014, Apple announced its decision to use a default encryption of the password-protected contents of its devices in the then-next version of its mobile operating system, iOS 8. Data generated by many of the system applications on iOS 8 and later versions are encrypted when data is stored locally on the phone, in transit, and stored on Apple's servers. The decryption keys are tied to the device password and only stored locally on the phone.

Table 7.1 Terrorist uses of the net

Author(s)	Furnell and Warren (1999)	Cohen (2002)	Thomas (2003)	Weimann (2004)
Uses	(1) Propaganda and publicity (2) Fundraising (3) Information Dissemination (4) Secure communications	(1) Planning (2) Finance (3) Coordination and operations (4) Political action (5) Propaganda	(1) Profiling (2) Propaganda (3) Anonymous/ Covert communication (4) Generating "Cyberfear" (5) Finance (6) Command and control (7) Mobilization and recruitment (8) Information gathering (9) Mitigation of risk (10) Theft/Manipulation of data (11) Offensive use (12) Misinformation	(1) Psychological warfare (2) Publicity and propaganda (3) Data mining (4) Fundraising (5) Recruitment and Mobilization (6) Networking (7) Sharing information (8) Planning and coordination

- Afterward, Google announced that Lollipop, its next version of Android OS, would enable device encryption by default.
- Then, WhatsApp, the popular instant messaging service for smartphones now owned by Facebook, announced its support for TextSecure, which is an end-to-end encryption protocol.
- In March 2015, Yahoo introduced a source code for an extension that encrypts messages in Yahoo Mail, though it requires users to run a key exchange server.

All of these events bring to the mobile world some of the available technologies that were not enabled by default for personal computing operating systems, such as Apple's FileVault and Microsoft's Bitlocker.

The most significant aspects of these announcements are that the encryption takes place using keys solely in the possession of the respective device holders which is enabled by default.

When encryption is seamlessly integrated into a communication software, a user does not have to take any actions to encrypt or decrypt messages, and much of the process occurs on the back end of the software. In fact, an average user might not be able to recognize the difference between an encrypted and an unencrypted message. When these options are enabled by

default on popular devices and platforms, like the iPhone, a large part of communications is encrypted.

It should be kept in mind that this is not the first debate about the public's ability to use encryption and the government's ability to access communications. Before the PC and Internet era, telecommunications companies were providing a means for government actors to wiretap voice communications – in particular on the legacy telephone system. Within the framework of the CALEA (Communications Assistance to Law Enforcement Act), US telephone companies would ensure that their networks could be wiretapped, with appropriate legal process, as network technologies moved from analog to digital. Later on referred to as the "crypto wars," government access to encrypted communications has become a hot debate and restrictive policy as the government ultimately was relaxing many export-control restrictions on software containing strong cryptographic algorithms in 2000.

Later on in October 2014, shortly after the announcements from Apple and Google, FBI Director J. Comey stated that as the law hasn't kept pace with technology, an important public safety problem arose. He referred to the issue as "Going Dark," and mentioned that those responsible for protecting citizens cannot always access the evidence which is required to prevent terrorism despite their legal authority because of their lack of technical ability.

According to these statements, the going dark problem is exasperated by the stronger encryption standards and advent of default encryption settings on both networks and devices. As a result, the use of encryption may constrain the ability of law enforcement and the intelligence community to investigate and prevent terrorist attacks.

Although much of the debate was about whether the issue is for companies like Google and Apple to preserve access to user data, the FBI or other stakeholders of the law enforcement and intelligence communities made no formal proposals. There has been only an invitation for collaboration among academics, Congress, privacy groups, and others in order to be able to address the needs of various competing legitimate concerns. Specifically, the private sector was asked for help in identifying solutions that provide the public with security without disappointing lawful surveillance efforts (See Appendix B for a detailed discussion on cyber security).

Other countries in the EU have been witnessing similar debates. In the United Kingdom, an outright ban was proposed by the Prime Minister on end-to-end encryption technologies following the January 2015 attacks at the *Charlie Hebdo* offices in Paris. Following the more recent November

attacks in Paris, French authorities also started to question policies about the availability of encryption software.

Many geopolitical partners to the United States are actively engaged in discussions about promoting cyber security and the appropriate limits of surveillance across borders. For example, due to the concerns about the US intelligence community's ability to access data, the US-EU Data Protection safe harbor, which provided a legal framework for commercial cross-border data flows, was recently ruled invalid by the Court of Justice of the European Union. The U.N. also preferred a limited extent on encryption because of seeing it as a required aspect for the exercise of the right to freedom of expression (Emery et al., 2004).

Meanwhile, many US companies must also answer to governments of foreign countries as they have to make a difficult decision due to the pressure from foreign government agencies to produce data about citizens abroad. Several companies refuse to change the architecture of their services to allow such surveillance. However, if the US government were to require architectural changes, surveillance would be made easier for both the US government and foreign governments. Needless to say, the well-developed legal doctrines, and redress mechanisms as part of the US government's surveillance activities are not available worldwide.

Although use of encryption may hinder surveillance, it may not be impermeable. For example, intrusions at the end points, a technique often used in law enforcement investigations may not be prevented by encryption. Also metadata, such as e-mail addresses and mobile-device location information that must remain in plaintext to serve a functional purpose, is not protected by encryption. Through means of cloud backups and syncing across multiple devices, data can also be leaked into unencrypted media (Emery et al., 2004).

The "going dark" metaphor refers to the state of communications becoming out of reach and making us blind as an aperture is closed. The recent trajectory of technological development is not captured by this metaphor.

The following trends underpinning government access should be taken into account (Emery et al., 2004):

- Several business models rely on access to user data.
- Products are increasingly being offered as services, and centralized architectures are more common due to cloud computing and data centers. A service that involves a relationship between vendor and user lends itself much more to monitoring and control in comparison to a product,

where a technology is purchased once and then used without further vendor interaction.

- The Internet of Things (IoT) offers a new frontier for networking objects, machines, and environments in new ways. For example, when a television has a microphone and a network connection, and is reprogrammable by its vendor, it could be used to listen in to one side of a telephone conversation taking place in its room – regardless of how encrypted the telephone service itself might be. These aspects point to a trajectory toward a future with more opportunities for surveillance.

It should not be inferred that the problem will necessarily be solved by making data available or by providing government with the ability to gain access. Rather, the forces opening new opportunities for government surveillance mean that, whatever the situation with iOS 8 encryption versus its predecessor, "going dark" does not clearly refer to the long-term landscape for government surveillance (Emery et al., 2004). Any debate about surveillance capabilities today with potential lasting policy impacts should consider these larger trends (Hoo et al, 1997).

7.2 Encryption Runs Counter to the Business Interests of Many Companies

Implementation of end-to-end encryption is discouraged by current business models and therefore, there is an impediment to company and government access.

For the past 15 years, advertising has been the dominant business model of consumer-facing Internet companies that used ads to subsidize free content and services. Recently, due to the shift toward data-driven advertising, the related technology relies on user data for targeting ads based on demographics and behaviors. Companies such as Google and Facebook try to make behavioral assessments to match ads to individuals on the fly based on behavioral patterns, search queries, and other signals collected such as location, demographics, interests, and behavior (Emery et al., 2004).

Given the preference of companies to have unencumbered access to user data with relevant privacy settings which restrict dissemination of identifiable customer information, the implementation of an end-to-end encryption would be in conflict with the current advertising model (Zanini, 1999). In order not to get their revenues curtailed in this lucrative market, many Internet

companies will continue to fulfill the government's requests of providing access to communications of users.

For those companies who require to offer features in cloud services, end-to-end encryption is not practical as they need to access plain text data (Stern, 1999). Cloud computing enables businesses and individuals to extend their computing resources through the Internet at remote data centers, much like a utility service. For example, Google's various features in its web-based services must access plain text data, including full text search of documents and files stored in the cloud. In order for such features to work, Google must be able to access the plaintext. Also, Apple's encryption does not include all of its services although end-to-end communication in some of its applications is encrypted. This includes the iCloud backup service, which enables users to recover their data from Apple servers. Although Apple does encrypt iCloud backups, it holds the keys so that users who have lost everything are not left without any solution. As Apple holds the keys, it can produce user data that resides in iCloud whenever legal processes request the company to do so.

One of the main reasons why businesses do not make a shift to encryption or other architectures is that encryption schemes often add complexity to the user experience. For example, in the Android ecosystem, wireless providers and handset manufacturers may control smartphones by developing customized versions of the Android operating systems. Due to the additional resources required to make the customized features compatible with newer versions of Android, these companies have little incentive to update older phones. Moreover, although the next version of Android released by Google may contain apps that support end-to-end encryption, a manufacturer may change the software so that it includes its custom apps that do not support encryption (Garrido and Halavais, 2003). If the ecosystem is fragmented due to commercial interests in retaining access to plaintext communications, encryption is less likely to become all encompassing.

7.3 Other Surveillance Mechanisms: The Internet of Things and Networked Sensors

According to analysts and commentators representing the conventional wisdom, the IoT is the next revolution in computing which can shift the way we interact with our surroundings (Garrido and Halavais, 2003).

Several companies such as Amazon, Apple, Google, Microsoft, Tesla, Samsung, and Nike are all developing products with embedded IoT functionality, with sensors ranging from proximity sensors, microphones, speakers,

barometers to infrared sensors, fingerprint readers, and radio frequency antennae with the aim of sensing, collecting, storing, and analyzing detailed information about their surrounding environments (Garrido and Halavais, 2003).

In February 2015, it was asserted that Samsung smart televisions were capable of listening to conversations due to an onboard microphone. Samsung warned its users in one of its statements within its privacy policy that they should be aware that any personal or other sensitive information, spoken will be among the data captured and sent to a third party via means of the Voice Recognition. A cloud infrastructure through a network connection was utilized to send the voice data to a remote server for processing and interpretations of that data back to the television as machine-actionable commands.

In a similar vein, by means of an onboard microphone in a laptop or desktop computer Google's Chrome browsing software supports voice commands. In order to activate the feature, the user has to say "OK Google" so that the resource-intensive voice processing occurs on Google's remote servers.

Given this impact of IoT, intelligence agencies may start to request orders from Samsung, Google, or others to push an update. It is crucial to appreciate these trends and to think carefully about how pervasively open to surveillance our surroundings should be.

As the expected substantial growth of networked sensors and the IoT there is potential for the surveillance mechanisms to be drastically changed (Garrido and Halavais, 2003). Through means of the still video, audio, images captured by these devices, real-time intercept and recording with after-the-fact access may be realized (Garrido and Halavais, 2003). So the inability to keep track of an encrypted channel could be offset by the ability to monitor from afar an individual via another channel.

Also, it should be kept in mind that metadata such as location data from cell phones, telephone calling records, header information in e-mail will mostly remain unencrypted in order for various systems to be able to operate among each other. This entails crucial surveillance data that was unavailable before these systems became widespread (Garrido and Halavais, 2003).

Governments and related stakeholders should address threats to fundamental human rights such as privacy and personal data protection by acting both within their own jurisdiction and in cooperation.

- Interception of communications, data collection over the Internet, and its analysis by law enforcement agencies and other related stakeholders must address clear objectives that are in alignment with the principles of

necessity and proportionality (Garrido and Halavais, 2003). Goals such as gain of political advantage or exercise of repression are not legitimate.
- In case of abuses, an appropriate redress of law should be possible and individuals whose right to privacy has been violated due to arbitrary surveillance should be offered access to an effective remedy.
- Users of free or paid services on the Internet must be equipped with an understanding or a choice over the deployment range of their data with regard to its commercial use, without being excluded from the use of these services (Garrido and Halavais, 2003). In the case of a security breach, a redress should also be offered by these businesses.
- Governments should not ask third parties to build "back doors" to access data as this might weaken Internet security. Integration of privacy-enhancing solutions including end-to-end encryption of data in transit and at rest should be encouraged.
- In collaboration with business sector and the civil society, governments must provide public training on cyber security to foster development of more secure and stable networks globally (See Appendix B for a detailed discussion on this topic).
- Due to the trans-border nature of digital intrusion, the ability of the target government to investigate and prosecute the related parties with regard to that intrusion is curtailed. There must be mutual support among states in order to prevent damage and to deter future attacks.

The debate over encryption which poses difficult questions about security and privacy must be approached from different perspectives.

From the perspective of national security, the question this debate poses is whether access to encrypted communications would also increase our vulnerability to digital espionage and other threats and also whether nations that do not embrace the rule of law would be able to exploit the same access.

From a civil liberties perspective, the question this debate poses is whether preventing the government from getting access to communications under circumstances that meet regulatory requirements will establish the right balance between privacy and security, particularly when terrorists and criminals seek to use encryption to evade government surveillance.

These questions should be examined by focusing on the trajectory of surveillance and technology. As the enhanced availability of encryption technologies hinders government surveillance under certain circumstances, the government is losing some surveillance opportunities. Yet, the combination

of technological developments and market forces will provide the government with new opportunities to collect critical information from surveillance.

Given the prevalence of network sensors and the IoT, new questions about privacy over the long term might be raised. So both the responsibilities of technology developers and operational procedures and rules should be re-considered to support the law enforcement and intelligence communities navigate the related issues.