INSS Insight No. 643, December 17, 2014

Law Enforcement and National Security vs. Global Business Interests

Yoram Hacohen

Three interesting processes are underway as a direct result of Edward Snowden's revelations about the extent of the access by US security services to personal information stored and processed in the IT systems of global American companies. One of these processes is essentially technological, the second is legal, and the third is of a business nature. All three processes are designed to constrict access by American government agencies to personal information held by those companies, in their effort to preserve national security and enforce the law.

In June 2013, Snowden, a systems administrator who worked for a subcontractor of the National Security Agency (NSA), gave Glenn Greenwald, a journalist at *The Guardian*, tens of thousands of documents that revealed the far-reaching extent to which American security agencies were collecting personal information from American-originated global companies such as Google, Facebook, Microsoft, Apple, and Yahoo. The documents indicate that with the approval of a special court for intelligence matters operating under the Foreign Intelligence Surveillance Act (FISA), computerized interfaces had been constructed for the automatic transfer of information from the companies to the NSA. According to Snowden, the transferred information included search requests for search engines, e-mail, instant messaging, video, VoIP calls, and documents, as well as information about each of these items (i.e., metadata such as sender, receiver, time of delivery, IP address, and so on). In addition, among Snowden's more sensational disclosures was information about the NSA's monitoring of world leaders, including leaders of friends of the US.

Ostensibly, Snowden's revelations should have disturbed mainly civil rights activists anxious about violation of the constitutional rights of American and foreign citizens, such as the right to privacy, due process of law, and freedom of expression. Surprisingly however, the primary response has come from the global technology companies.

When Apple released its new version of its operating system for smartphones, IOS8, it announced that it would include an encryption mechanism for the instant messaging system and calls (iMessage and FaceTime) that would prevent the company from

decoding the communications content and would not enable Apple to disclose information to law enforcement authorities. Google announced that it will have similar solution in the new version of its Android operating system. The WhatsApp application, acquired by Facebook, announced recently that it too was implementing an encryption mechanism of this sort in its messaging system. Google and Yahoo reported that they were taking steps to enable their customers to perform encryption in their respective e-mail services. Thus, more and more companies are announcing the implementation of technological means that would make the companies incapable of cooperating with the authorities and complying with orders from them, even if approved by the court.

At the same time, global companies are challenging federal orders in the legal sphere. Several months ago, Microsoft initiated a legal proceeding following an order issued by a local New York City judge at the request of the United States law enforcement authorities for information about its customers stored on the company's servers in Ireland. These servers operate under a European jurisdiction, and Microsoft claimed that in certain aspects the US court order violates the rights of its customers under the European legal framework. Microsoft decided to take this order to the highest legal authority available to it for a ruling, asserting that the US government had no right to search and seizure for communications stored in a foreign country. This stance was supported in the legal process by other global corporations, among them Apple and Cisco.

The third area in which a change has apparently taken place is the realm of business. After years of developing business models based mainly on providing "free services," such as Facebook, Google, and Twitter, which finance their operations through usage of users' personal information for online advertising services, a market may be emerging based on providing privacy protection services. This process is just beginning, but venture capital funds report growth in the startups in this field.

The global companies' motivation for introducing technological changes in their products such as encrypting their customers' information, as well as challenging the requests for disclosure of such information, is due to their realization that their business is built on worldwide user trust. Anxiety about being perceived as collaborators with American intelligence and law enforcement agencies is forcing them to signal that customer interests everywhere around the globe are identified and secured. Businesses that provide privacy protection services may see an emerging market for products that protect against state and global corporations surveillance that collects large amounts of personal information.

The history of modern encryption shows that academic inventions and their business applications can be quite problematic for state agencies, as happened following the development of the Diffie-Hellman key exchange public-key cryptography in the 1970s (and the ensuing development of the RSA algorithm for generating encryption keys).

Another example is the opposition to the Clinton administration idea in the 1990s to build an encryption device with a built-in backdoor into the hardware used for communications (the Clipper chip).

With this background, several processes are underway that are likely to affect the war against terrorism significantly, as well as law enforcement in cyberspace.

The first process is continued development and implementation of encryption means that are subject to the exclusive control of the end user. These methods operate in a decentralized way, and do not require centralized management functions that can be monitored. In addition to the communications content, all these means may also conceal metadata, making it difficult to map and identify the activity taking place, and certainly to distinguish it from the innocent activity that accounts for most uses of the internet. Despite the recent success by American law enforcement authorities in dealing with criminal activity using the TOR anonymous service network, it required large scale resources, and the breaches found are likely to be closed.

The second process, signs of which began to appear immediately after Snowden's disclosures, is the development of state-centered internet services, i.e., services for which legal jurisdiction and law enforcement authority lie with a sovereign state, since they operate solely within the sovereign state, and most of their users are its citizens. Evidence of such initiatives has been seen in Europe, Russia, and China. Beyond the business effect of this trend on global companies, the significance for law enforcement is that in order to obtain information from remote services for the purpose of fighting terrorism or law enforcement, agencies will require an international mechanism for assistance in law enforcement and intelligence – with all the political and international ramifications of this sort arrangement. Covert penetration of these services obviously incurs a risk of international tension, due to the infringement of sovereignty involved.

The third process is public pressure in various countries for clearer regulation of the authority and monitoring capabilities of the intelligence and law enforcement agencies at both the local and the international level. One indication of this was the initiative by Democratic senators, with support from the NSA, to define and circumscribe the NSA's monitoring authority. The initiative was eventually rejected due to opposition by the Republican majority in the Senate. In addition, the European Commission is promoting regulation on privacy and protection of personal data, and the European Parliament passed a resolution in favor of measures to break up the "digital monopolies" (which are the attractive global vendors from which to collect data). Although these are ostensibly civilian matters, this initiative will also have a major impact, since it puts the volume of information collected in global information services in the spotlight.

These processes, insofar as they expand, are likely to challenge and complicate the effort at law enforcement and the fight against terrorism throughout the world, including Israel. Today, a significant part of the preparation for crime and terrorism takes place in cyberspace, and cyber terror and cybercrime activities are conducted in this venue. Access to this information at the preparatory stages for preventative purposes is critical. The law enforcement and intelligence agencies must understand the opposing processes and interests – civilian, technological, and business – and make sure that on the one hand, these interests are not harmed unnecessarily, and on the other hand the ability to fight 21st century crime and terrorism is maintained.