Law Enforcement 2.0: Regulating the Lawful Interception of Social Media

Esti Peshin

Lawful interception (LI) has evolved over the past few decades from target based monitoring & interception of telecomm conversations, to the monitoring & interception of packet switched (IP) communications. However, in spite of this evolution, the nature of the communication remained linear, where the initiator communicates with one, or a number of, recipients. Initially, with telecomm, all of the participants in the call were online, i.e. active participants at the time of the call; whereas, with the introduction of packet-switched or IP traffic, some of the interaction between the participants became turn-based, where the recipients receive the information from the initiator after an interval. Notwithstanding spam, the participants, more often than not, opted to receive the information.

Lawful monitoring & interception of both telecomm and packet-switched communications is regulated by law enforcement agencies, with the cooperation, under the global lawful interception regulation & legislation, of the telecomm and Internet service providers. Global interception regulations, legislation and standards include the Council of Europe's Convention on Cyber Crime treaty (2004); LI standards by the European Telecommunications Standard Institute (ETSI); The US' Communication Assistance for Law Enforcement Act (CALEA), passed in 1994; and, the European Parliament & Council's Data Retention Directive.

Social Network Services are a modern means of communication; however, the nature of communication therein is extremely more complex than in previous forms of communication.

The nature of communication in social network services is exponential, viral and borderless. An initiator may send or publish information to many recipients, who, in turn, may proceed to forward it, via a simple, one-click, action to many more participants, and so on and so forth. An initiator with a compelling message, thus, has the ability to reach a huge number of global recipients through social network services - Facebook alone had more than 750 million users as of June 2011[1]. In essence, the communication through social network services has similar characteristics as spam; but, unlike spam, in social network services, most recipients would like to receive the information, even if they do not actively participate & interact in the communication.

Furthermore, the proliferation of social network services has seen the emergence of multi-dimensional communication, which can involve communicating with the same participants via several means within a social network service (e.g. chat, direct

[1] Ben Foster: `http://www.benphoster.com/facebook-user-growth-chart-2004-2010/`

P. Gladyshev and M.K. Rogers (Eds.): ICDF2C 2011, LNICST 88, pp. 33–35, 2012.

message, wall post, public post, friend request, etc); communicating simultaneously across several social network services; and, combining the communication with other, more traditional, forms of communication (e.g. email, phone, SMS, instant messaging, etc).

Notwithstanding the clear and immediate benefits of social network services, their characteristics have turned them into a haven for criminals & insurgents.

The open nature of social network services provides criminals with ample access to potential victims and provides insurgents with a virtual Hyde Park, where they can openly voice their opinions and gain followers. The nature of communication within social network services; the ease of establishing fake identities therein, and of gaining credibility (via credentials, connections, participation in groups); the huge amount of data that passes through these networks on a daily basis - all render social network services far from lawful interception friendly.

Furthermore, the fact that the leading social network services, namely Facebook[2] & Twitter[3], implemented strong client-server encryption capabilities in 2011, which users can choose to activate via a simple setting, complicates even more the ability to monitor & intercept social network services' traffic via conventional lawful interception practices.

Finally, the fact that social network services are operated by commercial companies, which do not necessarily adhere to the local & international lawful interception legislation and regulation, increases even more the difficulty of monitoring communications therein.

A paradigm change is needed! Law Enforcement Agencies must proceed to take the necessary provisions for intercepting and monitoring the social network services traffic pertaining to and affecting their own countries.

Table 1. The Evolution of Communication and Lawful Interception

Means:	Telephony	Packet Switched (IP)	Social Network Services
Nature:	One to One	One to Many	**Broadcast**
Participation:	Online	Turn-Base	**Offline / Stream**
Targeting:	Target Based	Content Based	**A new LI paradigm is necessary!**
Interception:	Transaction	Mass	

This can be achieved, in the long run through international standardization and certification of social network services. Telecomm & Internet service providers are required, by law, to facilitate lawful interception; similarly, larger social network

[2] "Facebook offers 500 million users SSL crypto" Cade Metz, The Register. 26 January 2011 (http://www.theregister.co.uk/2011/01/26/facebook_https/)

[3] "Making Twitter More Secure: HTTPS." Twitter Blog, 15 March 2011 (http://blog.twitter.com/2011/03/making-twitter-more-secure-https.html)

service operators should, be required to undergo an international certification process and to ensure that Law Enforcement Agencies have access to the communications pertaining to and affecting their country.

Furthermore, lawful interception legislation and regulations must be amended, as necessary, to ensure that the Law Enforcement Agencies are legally allowed to scrutinize all the relevant traffic within social network services, and not be limited only to the traffic of pre-identified targets. This would naturally require employing also data retention provisions, allowing retroactive access to the social network services traffic, for a limited timeframe.

Finally and until the international standardization and regulation is in place, Law Enforcement Agencies should ensure, through technological means and international cooperation, that they have indigenous capabilities to access, intercept, and monitor the social network traffic of suspect individuals pertaining to and affecting their country.

In summary, social network services have proliferated as a wide-spread means of communication, with exponential, viral, borderless and multi-dimensional characteristics. This medium which provides privacy and can ensure anonymity is not sufficiently regulated to date in terms of lawful interception. As such, social network services can be a true haven for insurgents and criminals. Law Enforcement Agencies must proceed rapidly to ensure the proper lawful interception regulations, legislation, certification processes, international treaties and technologies are adjusted in order to provide them with an adequate level of access to the traffic within social network services.

Esti Peshin is the Managing Partner of ENP Solutions Ltd., a strategic management consulting firm that specializes in security and defense companies, focusing on company buildup and corporate development, sales and marketing processes, new business units, and growth fund raising and M&A processes. Ms. Peshin is also a Partner at Destino Ventures LLC, a private equity fund committed to investing in distressed companies and raising their value toward a subsequent milestone. Ms. Peshin is also a Partner at Hope Ventures Ltd, a Distributor and Business Development house, committed to representing and distributing high-end security products. She serves as the Director General (pro bono) of the Israeli Hi-Tech Caucus at the Knesset, the Israeli Parliament.

Prior to assuming these roles, Ms. Peshin was the CEO of Waterfall Security Solutions, a provider of a foolproof physical security gateway for homeland security and mission-critical installations. Previously, she held an Account Director position in the Lawful Interception division of Verint Systems, Inc., where she was responsible for large-scale projects and account management in the Asia-Pacific region. Before joining Verint, Ms. Peshin acted as a Project Manager in ECtel, managing large-scale international projects. She served 11 years in the Israeli Defense Forces, in an elite technology unit, where she was Deputy Director. Ms. Peshin holds a BA degree in computer sciences and management from the Open University of Tel-Aviv, Israel.