Regulating Social Network Services for Lawful Interception

Esti Peshin(✉)

Cyber Programs, ELTA Systems Ltd, Jerusalem, Israel
epeshin@elta.co.il

Abstract. Lawful interception has evolved over the past decades from the target based monitoring and interception of telecomm conversations, to the monitoring and interception of packet switched communications. The lawful monitoring and interception of both telecomm and packet switched communications is regulated by law enforcement agencies, with the cooperation, under the Lawful Interception regulation and legislation, of the service providers.

Social networks are also a means of communicating; but the nature of communication therein is extremely more complex, as it allows both for linear communication (one to one) and broadcasting of information (one to many/crowd) to selected groups and communities.

Social networks are a haven for criminals and insurgents. The open nature of the media provides criminals with ample access to potential victims and provides insurgents with a virtual Hyde Park, where they can openly voice their opinions, gain followers and instigate and organize disruptive activities.

The nature of the communication within social networks, the ease of establishing fake identities therein, the fact that the client-server communication can be encrypted, and the huge amount of data that passes through these networks on a daily basis - however, are far from law-enforcement friendly. Furthermore, the fact that social networks are operated by commercial, usually foreign based, companies, which do not necessarily adhere to the local Lawful Interception legislation and regulation, increases the challenge of monitoring of communication with social media.

The paper will discuss the technological challenges that law-enforcement agencies face when trying to monitor social networks, and the technological, regulatory and legislative provisions that can and should be put in place, by the operators of the Social Network Services and local law enforcement agencies, in order to prevent social network services from continuing to foster criminals and insurgents.

This paper is based on public domain information.

Keywords: Lawful interception · Social networks · Regulation · Cyber intelligence · Cyber crime · Cyber security · Law enforcement

P. Gladyshev et al. (Eds.): ICDF2C 2013, LNICST 132, pp. 119–129, 2014.
DOI: 10.1007/978-3-319-14289-0_9

1 Introduction: Social Networks - An Unregulated Communication Medium

Lawful interception (LI) is defined [1] as obtaining telecommunication data for the purposes of analysis or evidence. The obtained data may consist of signalling information, network management information and the content of the communications themselves.

Lawful interception is regulated by law enforcement agencies (LEAs), with the cooperation, under global lawful interception regulation and legislation, of the telecomm, Internet and network service providers.

The principal global legal instrument relating to LI is the Convention on Cybercrime treaty, also known as the Budapest Convention, which entered into force on July 1st, 2004, and sought to address computer and Internet crimes by harmonizing national laws, improving legislative techniques and increasing international cooperation [2]. As of October 2010, 30 countries signed, ratified and acceded to the convention, whereas 16 additional countries have signed the convention, but have not ratified it [3].

Individual countries have different legal requirements relating to lawful interception. The European Telecommunications Standard Institute (ETSI) [4] standardized the manner in which information should be transferred from the Telecomm and Internet service providers to the law enforcement agencies. This standard was adopted by European and other countries. The US passed the Communication Assistance for Law Enforcement Act (CALEA), also known as the US "wiretapping" law, in 1994 [5]. The European Council (EC) resolved in 1995 to mandate similar, though not identical, measures to CALEA within Europe [6].

Lawful Interception (LI) has evolved over the past decades from monitoring and interception of telephone (voice) conversations, to the monitoring and interception of packet-switched (IP) communications (such as emails, instant messages, web browsing activities, etc.).

However, throughout the evolution, the nature of the communication remained linear, where the initiator communicates with one, or a number of, recipients. In telephone communications, generally, all of the participants in the call were online, i.e. active participants during the call. After the introduction of packet-switched communications, some of the interaction between the participants became turn-based, where the recipients receive the information from the initiator, and may decide to respond or not, after an interval. Good examples of turn-based communication means are emails or instant messages (IM), where the sender, the initiator of the interaction, submits a message to one or several recipients, from whom he may or may not receive a response.

Social networks are, by nature, a means of interacting and communicating. However, unlike voice and IP interactions, the nature of communication in social networks can be linear, one to one; exponential - one to many; and viral, in case the recipients of the communication proceed to forward the communication to many more participants. The viral nature of social networks allows a sender to reach a huge number of recipients. However, the recipients of the communication

do not, necessarily, actively participate in the communication; some do not even opt to receive it.

Users are able to conduct practically any type of interaction through social networks. They are able to broadcast information to their connections and/or to the general public, respond publicly or privately to information within the network, send email-like messages (AKA direct messages), chat with one of more users via instant messages, and even conduct voice conversations.

The use of social networks has soared over the past few years. Facebook reached 1 billion monthly active users on September 14th, 2012 [7], including 600 million mobile users, and an average of 584 million daily active users [8]. It is humbling to note that the number of Facebook users, as of September 2012, is more than three times the population of the United States, and in fact, exceeds the population of all the countries in the world, except for China and India.

However, the crux of the matter is that although social networks are an extremely prominent communication medium, social networks are, generally, not regulated by specific and adequate Lawful Interception (LI) legislation as a unique means of communication. Rather, the monitoring and interception of social network traffic is still regulated under the legislative provisions for the interception of packet- switched (IP) communications and data. The subsequent chapters will show why this is a highly undesirable situation.

2 Social Networks - A Haven for Insurgents and Criminals

Social networks are a haven for insurgents and criminals. Social networks, by nature, can provide anonymity and obscurity. Practically anyone can join a social network without any scrutiny, define a profile for themselves and start gaining followers and friends.

The open nature of social networks provides insurgents with a viral platform, where they can voice their opinions, gain followers and support, and instigate disruptive action.

The Guardian argues, in a February 2011 article [9], that social networks played several distinct and crucial roles in the Middle East and North Africa uprisings. Social networks provided the instigators and leaders of the uprisings with the means to gain followers and distribute ideas and information within their countries. Furthermore, social networks served a means to communicate openly with the outside world, and gain international public support. Social networks were used to smuggle sensitive footage and videos; material which was subsequently used by the mainstream media, in its coverage of the events, and which was instrumental in moulding the public opinion with regard to the events.

It is interesting to note that several social networks were prominently used and best suited to play a different role during the uprisings. Facebook was effective as a means of finding others with similar political views and planning street protests; YouTube was suited for citizen journalism by broadcasting videos, which were in turn picked by the mainstream global television channels and seen around

the world; Twitter enabled on-the-move coordination and communication, and was also used for outreach to the international media and communities in the Diaspora [10].

The widespread and easy access to these online communication tools posed new and threatening challenges to the regimes. The simultaneous, coordinated and multi-dimensional utilization of all these different types of social networks created a very strong communication network which became difficult to disrupt.

Consequently, the uprisings triggered a surge of growth in the user base of Social Networks. The memeburn.com blog [11] quotes data according to which more than 200,000 Tunisians joined Facebook during the January 2011 uprising - a 11.4 % growth in the Tunisian Facebook users over the span of a month. Similarly, between January 20th and 25th, 217,600 Egyptians joined Facebook - a 4.2 % growth in the user base over the span of only 5 days.

The open nature of social networks provides criminals with access to potential victims, allowing them to leverage the users' personal details into financial gain.

The National White Collar Crime Center (NW3C) published in 2011 a study on criminal use of social networks [12]. NW3C cites various types of crimes enabled by or instigated on social networks: perpetrators may utilize social networks to look for potential victims in the vicinity who will not be at home at a certain time; perpetrators may utilize social engineering techniques within social networks in order to gain information from unsuspecting users or in order to manipulate them into an undesired action; and, finally, perpetrators may take advantage of the social network users' tendency to click on links, view files and respond to messages in order to infect their computer with malware.

A proof of concept conducted by Comsec Consulting in 2011 exhibited how simple it was to establish a fake identity of a corporate employee, and within one day, gain 74 friends from the same company [13]. A fake persona with so many friends from within the company would have inherent credibility, and could immediately proceed to engage in social engineering attacks, or, to utilize his fake, and now credible, identity to publish online content on behalf of or pertaining to the company.

FBI Assistant Director, Mr Gordon M. Snow, addressed the threats of crime on social networks in a testimony he gave before the House Judiciary Subcommittee on Crime, Terrorism and Homeland Security on July 28th, 2010 [14]. Mr Snow testified that "[...] the surge in use of social networking sites over the past two years has given cyber thieves and child predators new, highly effective avenues to take advantage of unsuspecting users".

Mr Snow, subsequently, outlined how the threat of social engineering attacks, where a user is fooled online by persons claiming to be somebody else, is accentuated in social networks. Mr Snow testified that "Unlike the physical world, individuals can misrepresent everything about themselves while they communicate online, ranging not only from their names and business affiliations (something that is fairly easy to do in-person as well), but extending as well to their gender, age, and location (identifiers that are far more difficult to fake in-person)".

The nature of the communication within social networks; the huge amounts of data that pass through these networks on a daily basis; and, the ease with which an identity can be set up and gain credibility, are far from being law-enforcement friendly. Furthermore, the fact that social networks are operated by commercial companies that do not necessarily adhere to local Lawful Interception legislation and regulation, increases the complexity of monitoring communications and interactions within social networks.

3 Lawful Interception of Social Networks

Lawful interception and monitoring of packet-switched data generally relies either on known identities and/or on the identification of content of interest.

By way of example, a law enforcement agency may obtain a court order for monitoring a certain individual, and may proceed to monitor their unique packet-switched IDs (IP address, MAC address, email address, Instant Messaging ID, etc.).

A malicious user may attempt to set up a completely anonymous framework for communication. A user can quite simply set up an anonymous email account (Hotmail, Yahoo, Gmail or other), communicate via emails, only from public hotspots, and never from their own computer; and, potentially, utilize TOR [15], a freeware platform of anonymous worldwide servers, enabling users to surf the web through an ever-changing network of proxies. A LEA would be hard pressed to intercept such a communication based on the user's distinct IDs; however, notwithstanding legislation and regulation, which may require in certain countries a warrant related to a distinct ID, a LEA may be able to intercept such an email based on its content, by identifying pre-defined keywords that were included within the email.

The European Parliament and Council adopted, in 2006, advanced and unique LI legislation, in the form of the Data Retention Directive, regulating how electronic data should be captured, retained and provided, upon request, to Law Enforcement Agencies [16]. The Data Retention Directive requires service providers to retain, for a predefined amount of time, information regarding calls, emails, websites visited, etc. Thus, if an email address, for example, is identified over time, as belonging to a suspect individual, the LEA would be able to obtain from the service provider data related to previous communications involving the same email address.

It should be noted that since its passage, the Data Retention Directive has faced intense criticism and has been opposed by legislators in the European Parliament who argue that it fosters a surveillance society and undermines fundamental human rights [16]. In April 2011, the European Commission published an evaluation report of the Directive that revealed inconsistencies with how EU members implement the legislation and which authorities can access the data [16]. In May 2011, the European Data Protection Supervisor (EDPS) published his evaluation of the EU report and expressed the view that the Directive does not meet the requirements imposed by the fundamental rights to privacy and data protection [17].

The interception and monitoring of an individual's traffic within social network services is compounded by three major factors: First and foremost, an individual can set up a completely anonymous and bogus profile within a few minutes in a large set of social networks. Furthermore, their activity will be masked within more than 2.5 billion content items, which according to Facebook statistics released in August 2012 [18], are shared by Facebook's users every day. Finally, and this is a crucial point, the corporations operating the social networks - the social network service providers or social network operators - are not regulated as of yet.

By way of example, let us consider criminal or insurgent activity conducted within a certain country through a social network. Even if the activity and/or instigators would eventually be identified by a LEA, would the affected country be able to obtain retroactive information from the foreign corporation that operates the social network? It is quite safe to assume that, more often than not, the answer would be negative. The social network operators are presently not required to do so by law, and quite naturally, would tend to favour the privacy of their user base - their raison d'être - over the security needs of a foreign country.

The social network operators' bias of favouring privacy over security was exemplified in the uprisings in Tunisia and Egypt in the beginning of 2011.

The uprisings demonstrated the importance of a viable and widespread communication means in promoting, facilitating, and, most importantly, accelerating insurgent activities.

The Atlantic published a fascinating article [19] on how Facebook openly aided the Tunisian insurgents during the uprisings. According to the Atlantic, quoting Facebook's Chief Security Officer, Joe Sullivan, the Facebook security team realized, early January 2011, that the Tunisian Internet service providers (ISPs) were running a malicious piece of code - allegedly, a keystroke logger - that was recording users' credentials and passwords when they accessed secure sites like Facebook. Facebook responded by routing all Tunisian requests for Facebook to an HTTPS server, which encrypts the information sent across, and thus renders the information insusceptible to monitoring, interception and the key-logging strategy that was utilized by the regime. Facebook further employed a "roadblock"[1], ensuring that users that were affected by the regime's hack, are indeed who they claim to be.

It is tempting to commend the role social networks can play when utilized by self- proclaimed forces of freedom, the good guys. However, we must not lose sight for an instant that the same means can be and are used also by insurgents and terrorists - the bad guys - aiming to destabilize, harm and potentially overthrow legitimate governments and regimes.

Facebook itself announced on January 26th, 2011 [20], that it is allowing users to choose full SSL/HTTPS encryption to secure all communications between the users' browsers and the Facebook Web servers. Twitter added, in March 2011, a

[1] A roadblock is a technique where a user is identified by a question or a series of questions, such as asking users to identify photos of their friends before allowing them to log into the network.

user setting that allows users to always use HTTPS when accessing the Twitter site [21]. At the onset, both social network operators left it up to their users to decide whether to encrypt their traffic or not. Users who chose to encrypt their traffic significantly impaired, knowingly or not, the local LEAs ability to intercept and monitor their traffic.

Facebook has taken another leap forward and announced [22] in its developer blog that it is starting, as of November 2012, to roll out default HTTPS encryption for all North America users, and will be soon rolling out default encryption to the rest of the world. *The immediate derivative is that once the change is rolled- out, coverage of all Facebook traffic - the traffic of 1 billion users worldwide - via legacy packet-switched (IP) Monitoring systems will be lost.* Needless to say, this development may have severe impact on security.

Granted, the increased security is important for legitimate users, assisting them in preventing identity theft. However, the fact that social networks use strong encryption further hampers the ability of LEAs to intercept and monitor the traffic without the cooperation of the social network service providers.

The immediate conclusion is that social networks must not remain unregulated!

4 Social Networks Must be Regulated!

The lawful interception regulation and legislation must undergo a paradigm shift in order to ensure the cooperation, under the proper legislation, of corporations operating widespread social networks with a significant user base.

This can and should be achieved, in the long run, through the international standardization and certification of social networks, to include the necessary provisions for local lawful interception. Similarly to the manner in which telecommunications and Internet service providers are required, by law, to facilitate the local LEAs interception of the communications thereof, widespread social network service providers should be required, prior to launching their services within a country or region, to undergo an international certification process and to ensure that the local LEA has access to the communications pertaining to and affecting the country and/or region.

Furthermore, the LI legislation and regulations must eventually be amended, where necessary, to ensure that the LEAs are legally allowed to scrutinize all the traffic within the social networks, and not be limited only to the traffic of identified targets. This would naturally require employing also data retention provisions, allowing LEAs retroactive access to the social networks' traffic. The timeframe for such access should be pre-defined and limited, in order to minimize the potential violation of privacy.

The wheels have already been set in motion. ETSI published in April 2012 a draft technical report addressing the Lawful Interception of Cloud/Virtual Services [23]. ETSI addresses one of the main regulatory/legal challenges pertaining to the lawful interception of social network traffic, or for that matter any cloud based traffic, pertaining to a nation state - the fact that *the imposition of LI requirements is largely oriented around national jurisdiction and geography.*

Hence, it is unlikely that LEAs can serve a warrant on a social network operator directly unless that operator has an "in country" presence.

ETSI states social network operators (or any cloud based service provider) should implement a Cloud Lawful Interception Function (CLIF), which will allow them to intercept traffic on behalf of LEAs.

Addressing the challenge of jurisdiction and geography, ETSI further states that in order for the social network operator (or any cloud based service provider) to be able to intercept traffic on behalf of a local LEA, the LEA must pass the following tests:

- The warrant must be legal in that country.
- The traffic must be routed or handled in the same country.
- The traffic must be distinguishable from others in order to prevent collateral interception.

Finally, ETSI mandates, that in case the traffic is encrypted, the entity responsible for key management must ensure it can be decrypted by the social network operator or by the LEA.

ETSI's technical draft makes a lot of sense. As each new form of communication was introduced and evolved, it presented the LI community with new challenges. Some examples are the evolution of public switched telephone networks (PSTNs) from fixed-line analog telephony systems to digital cores and mobile networks; the exponential growth of packet-switched networks, the introduction of Voice over IP (VoIP) communications, and so on. Faced with these challenges, and in order to maintain their monitoring capabilities, regulators, governments and LEAs have had to adjust their LI regulations and legislation, and industry was required to come up with the enabling technologies.

The adoption of new standards, regulations and technologies may take time. In the meantime, the charter of international law enforcement agencies, such as the Interpol, and international and regional cooperation bodies, should be extended to act as intermediaries for obtaining lawful interception information in foreign countries.

However, and until the international standardization and certification of social networks is achieved, governments and law enforcement agencies should ensure, through technological means, international cooperation and other means, that they have the capabilities to access, intercept, and monitor the social network traffic of suspect individuals pertaining to and affecting their own country.

4.1 The Snowden and PRISM Case-Study

An example of a controversial program aiming to gain access, intercept and monitor social network services and cloud based services is the PRISM program.

PRISM is a clandestine mass electronic surveillance data mining program operated by the United States National Security Agency. The PRISM program was publicly revealed when classified documents about the program were revealed to The Guardian [24] and The Washington Post [25] by Edward Snowden.

The leaked documents included PowerPoint slides, which were published in the news articles [26], and which identified several US based technology companies as participants in the PRISM program. The identified companies included Microsoft, Yahoo!, Google, Facebook, Paltalk, YouTube, AOL, Skype and Apple. The slides reveal that the PRISM program allows for collecting data and information directly from the companies' servers. In order to comply with the US laws, the specified targets should be a foreign national who is overseas at the time of collection. The collected data includes emails, chats, videos, photos, stored data, VoIP, File Transfers, video conferencing and notifications of targets activity (logins, etc.).

To conclude, PRISM, essentially, allows the US to bypass the Lawful Interception challenge illustrated in this article by enlisting the cooperation of the major commercial corporations running social network services and cloud bases services. Notwithstanding, *the controversy and adverse public sentiment following the disclosure of the program, illustrate that the path to regulating the access of LEAs to the data and information within social networks and cloud bases services is expected to be lengthy and rocky.*

5 Summary

To conclude, social networks have emerged as a prominent medium of communication, with unique viral, exponential and multi-dimensional characteristics. Social networks provide privacy and can ensure anonymity. However, social networks are yet to be regulated in terms of Lawful Interception, and, as such, can be a safe haven for insurgents and criminals. Governments, Law Enforcement Agencies, and international cooperation and standardization bodies, must proceed rapidly to ensure the proper Lawful Interception regulations, legislation, certification processes, international treaties and technologies are adjusted and adopted in order to provide LEAs with a similar level of access to the traffic within social networks, as their access to telecom and packet-switched traffic.

References

1. Wikipedia: Lawful Interception. http://en.wikipedia.org/wiki/Lawful_interception
2. Council of Europe: Convention on Cybercrime, 2001, ETS No. 185. http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm
3. Council of Europe: Convention on Cybercrime Treaty Signature Status (2010). http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=28/10/2010&CL=ENG
4. European Telecommunications Standards Institute: About ETSI. http://www.etsi.org/about
5. Electronic Frontier Foundation: CALEA F.A.Q. https://www.eff.org/pages/calea-faq
6. European Telecommunications Standards Institute: Lawful Interception (LI); Concepts of Interception in a Generic Network Architecture, Technical report, ETSI TR 101 943 v2.1.1 (2004–10)

7. Facebook: One billion - key metrics. http://newsroom.fb.com/download-media/4227
8. Facebook: Key Facts. http://newsroom.fb.com/Key-Facts
9. Beaumont, P.: The truth about Twitter, Facebook and the uprisings in the Arab world, The Guardian, 25 February 2011. http://www.theguardian.com/world/2011/feb/25/twitter-facebook-uprisings-arab-libya
10. Khamis, S., Gold, P.B., Vaughn, K.: Beyond Egypt's "Facebook Revolution" and Syria's "YouTube Uprising:" Comparing Political Contexts, Actors and Communication Strategies. Arab Media & Society, no. 15, Spring 2012
11. Daniel, J.: Surge in Facebook users coincides with North African uprisings, memeburn.com, 28 January 2011. http://memeburn.com/2011/01/surge-in-facebook-users-coincides-with-north-african-uprisings/
12. National White Collar Crime Center: Criminal Use of Social Media (2011). http://www.iacpsocialmedia.org/Portals/1/documents/External/NW3CArticle.pdf
13. Comsec Consulting: The Social Networking Corporate Threat, March 2011, http://www.comsecglobal.com/FrameWork/Upload/The%20Social%20Networking%20Corporate%20Threat%20-%20Comsec.pdf
14. Snow, G.M.: Statement before the House Judiciary Subcommittee on Crime, Terrorism and Homeland Security, 28 July 2010. http://www.fbi.gov/news/testimony/the-fbi2019s-efforts-to-combat-cyber-crime-on-social-networking-sites
15. Tor Project. https://www.torproject.org/
16. Electronic Frontier Foundation: European Union Mandatory Data Retention Directive. https://www.eff.org/issues/mandatory-data-retention/eu
17. European Data Protection Supervisor: Evaluation shows that the Data Retention Directive does not meet privacy and data protection requirements, says EDPS, EDPS/11/6, 31 May 2011. http://europa.eu/rapid/press-release_EDPS-11-6_en.htm?locale=en
18. King, R.: How Facebook Wrangles Big Data, CIO Journal, 23 August 2012. http://blogs.wsj.com/cio/2012/08/23/how-facebook-wrangles-big-data/
19. Madrigal, A.C.: The Inside Story on How Facebook Responded to Tunisian Hacks, The Atlantic, 24 January 2011. http://www.theatlantic.com/technology/archive/2011/01/the-inside-story-of-how-facebook-responded-to-tunisian-hacks/70044/
20. Rice, A.: A Continued Commitment to Security, Notes by Facebook, 26 January 2011. https://www.facebook.com/notes/facebook/a-continued-commitment-to-security/486790652130
21. Twitter: Making Twitter more secure: HTTPS, Twitter Blog, 15 March 2011. https://blog.twitter.com/2011/making-twitter-more-secure-https
22. Asthana, S.: Platform Updates: Operation Developer Love, Facebook Developers Blog, 15 November 2012. https://developers.facebook.com/blog/post/2012/11/14/platform-updates-operation-developer-love/
23. European Telecommunications Standards Institute: Lawful Interception (LI); Cloud/Virtual Services (CLI), Draft Technical Report, DTR 101 567 v0.05 (2012–04)
24. Greenwald, G., MacAskill, E.: NSA Prism program taps in to user data of Apple, Google and others, The Guardian, 7 June 2013. http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

25. Gellman, B., Poitras, L.: U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program, The Washington Post, 7 June 2013. http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html
26. The Washington Post, NSA slides explain the PRISM data-collection program, 10 July 2013. http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/