Regulation of Online Surveillance in Israeli Law and Comparative Law

Amir Cahane with Yuval Shany

THE ISRAEL DEMOCRACY INSTITUTE

מרכז המחקר להגנת הסייבר
CYBER SECURITY RESEARCH CENTER

Policy Paper 123

Abstract

Policy Paper 123

REGULATION OF ONLINE SURVEILLANCE IN ISRAELI LAW AND COMPARATIVE LAW

Amir Cahane
with Yuval Shany

January 2019

Text Editors [Hebrew]: Yehudit Yadlin, Keren Gliklich
Series and Cover Design: Studio Tamar Bar Dayan
Typesetting: Nadav Shtechman Polischuk
Printed by Graphos Print, Jerusalem

ISBN: 978-965-519-247-6

The Israel Democracy Institute
4 Pinsker St., P.O.B. 4702, Jerusalem 9104602
Tel: (972)-2-5300-800; Fax: (972)-2-5300-867
E-mail: orders@idi.org.il
Website: en.idi.org.il

The Federmann Cyber Security Center – Cyber Law Program
The Faculty of Law, The Mount Scopus Campus Jerusalem
Box 80, ZIP Code: 9190501
E-mail: hcsrcl@mail.huji.ac.il
Website: https://csrcl.huji.ac.il

ABSTRACT

In 2013, Edward Snowden, who was employed by a National Security Agency (NSA) subcontractor, exposed documents that described the extent of online surveillance of communication networks conducted by American intelligence agencies, including of U.S. citizens. These revelations ignited a public debate about the agencies' surveillance practices and led to a number of statutory reforms. The exposure of the NSA's cooperation with its foreign counterparts opened the door to similar discussions in other countries concerning the desirable degree of their cooperation with foreign intelligence agencies, and the online methods of intelligence collection used by national intelligence agencies.

Online surveillance, or the surveillance of communication networks, is an intelligence activity designed to gather, retain, process, and analyze digital information from electronic communication networks—whether landline telephony networks, cellular communication networks, or computer data communication networks. Surveillance can be conducted in various ways, including interception and retrieval of information from the network or from front-end devices; collection of communications data (metadata) from communications service providers; and processing

open and hidden information, which can include data-mining techniques or machine learning. In an era in which a significant portion of human communication is conducted via electronic media, harnessing modern technology for the widescale collection, storage, and powerful statistical analysis of communications data can yield richer and more detailed intelligence information on surveillance targets than ever before.

However, alongside the advantages of intelligence gathered from online surveillance of communication networks, consideration must also be given to the significant violation of privacy inflicted on the subjects of surveillance. Those whose rights are harmed by the process include not only the intelligence targets themselves, but also those with whom they are in contact. Moreover, when bulk collection methods, which extract massive amounts of communications data and content from a main communications link rather than targeting a particular subject of surveillance are employed, the circle of those affected grows dramatically. The harm caused to individuals by online surveillance is not limited to infringement of their right to privacy. More broadly, the chilling effect caused by such surveillance may impair their general sense of freedom and their freedom of expression. When individuals are aware that they are, or may be, under surveillance, they are likely to modify their conduct accordingly.

Instances of technological surveillance by the state, other than those perceived as related to terror threats, prompt lively public debate in Israel. The “Big Brother Law” and the Biometric Database Law were discussed extensively in the media, and both found their way to the courts. By contrast, there has been almost no discussion of the rules regulating online surveillance for security purposes; in particular, there has been little discussion of existing legislation and its compatibility with today’s social and technological realities and with human rights norms.

Main Conclusions

1. Lack of regulation addressing essential issues

Examination of Israeli legislation applying to online surveillance of communication networks shows that Israeli law suffers from under-regulation of a series of issues for which comparative law offers solutions. For example, Israeli law has no general ban on bulk collection of communications, not even a ban coupled with provisions for exceptional cases in which such activity would be permitted, subject to criteria of proportionality and absolute need. Similarly, the territorial application of Israeli online surveillance laws has not yet been regulated. Thus, the question remains of what is permitted or prohibited with respect to communications beyond the borders of the State of Israel, including in the Occupied Territories under Israel's control.

In addition, there are no provisions in Israeli law with respect to temporal limitations on the retention of communications data by communications providers, as can be found in legislation in the European Union, the United Kingdom, and Germany. This refers both to the communications content itself and to metadata, which consist of information about the communication other than its content, and from which (among other things) details of the parties to the communication, and of where and when it occurred, can be ascertained.

Similarly, data-mining activities carried out in this context—that is, using statistical techniques to analyze databases obtained by means of online surveillance, including cross-referencing them with other government databases—are barely addressed in Israeli legislation, in contrast to foreign law. (In certain cases, European law restricts decision-making based on data derived from automatic information-processing activities conducted without any human involvement, even in law enforcement contexts.)

It appears that in Israel, the possibility of requiring authorization for the collection of open-source intelligence information (OSINT) from telecommunications networks has yet to be explored. Due to its nature, traditional intelligence gathering, which relies on open sources of mass communication, does not require authorization. However, it may be now necessary to legislate provisions for the use of open-source intelligence gathering that also utilizes publicly available information on social media. This is because mass monitoring of the publicly available activities of social media users, including automated analysis of this information, may lead to actual privacy violations. While similar practices are used by private organizations for commercial gain, the state's exceptional police powers may lead to more severe violations of privacy and have more severe practical implications for the products of open-source intelligence.

2. Confidential rules and lack of transparency

Current Israeli legislation affords the government broad discretion in setting rules to regulate the Israel Security Agency's (the ISA or General Security Service) surveillance of communications networks, and to regulate the orders issued to telecommunication licensees (licensed to provide telecommunications services including telephony, internet, and cellular services) to assist the security forces (including the Israel Police). These rules, and a portion of the parliamentary and administrative oversight thereof and of online surveillance practices, are kept secret.

While this secrecy facilitates flexible interpretation and application of the law to meet pressing operational needs, the concealed nature of this interpretive flexibility—the soundness of which is not open to public scrutiny—means that it is liable to lead to breaches of human rights protections.

3. Partial judicial review

In Israel, judicial review of various authorizations for online surveillance is limited in scope. The law absolves security agencies seeking a wiretapping order from applying to the courts and settles for a permit granted in advance by the minister responsible; in urgent cases, retroactive ministerial authorization is allowed, as long as the use of these powers is reported to the attorney general. In urgent cases, the use of wiretapping even for crime prevention and detection purposes does not require authorization by a judicial order, except when its extension is needed. The Wiretap Act exempts certain types of wiretaps from requiring any authorization at all, and these may fall under the legal arrangement that allows collection of open information on the internet, including from social networks.

Judicial review in Israel with respect to obtaining and collecting metadata is limited to non-urgent cases in which the police require metadata for investigation purposes and law enforcement. There is no provision that prohibits the police from employing communications data collection technologies that do not involve requesting data from telecommunication licensees. Collection of communications data by the ISA (via direct interception, online access, or occasional request) is not subject to any judicial authorization. Moreover, the applicable legal provisions may be interpreted so that the mere collection of communications data does not require authorization from the head of the ISA, and such authorization is only necessary for using of the acquired information.

Although a review of comparative law reveals that in other countries as well there is no sweeping judicial review of online surveillance practices, it seems that the scope of judicial review elsewhere is broader than in Israel. For example, in Germany and the United States, collecting content and metadata for purposes of crime prevention and law enforcement is generally subject to judicial review. In these two countries, there are

also arrangements for the judicial or quasi-judicial review of wiretapping permits for national security purposes.

At the same time, judicial review is not the be-all and end-all means of oversight. An empirical examination of the data regarding Israel Police requests for orders under the Wiretap Act and the Criminal Procedure Law (Enforcement Powers—Communication Data) shows that the proportion of requests rejected by the court was lower than 0.5% throughout the entire period reported. A similarly low rejection rate can be found in the reports of the Administrative Office of the U.S. Courts regarding wiretapping requests for law enforcement and crime prevention purposes. We should be wary of concluding from these data that the mechanism of *a priori* judicial review of wiretapping requests is seemingly nothing more than a rubber stamp, since the court may approve requests while also imposing restrictions on the orders issued, and may issue orders that contain stricter procedures. Likewise, judicial review itself can create incentives for investigative bodies to filter out inappropriate requests before they are even submitted to the court. Still, the very small number of wiretapping or online surveillance requests that are rejected by the court calls into question the efficacy of judicial review and justifies an examination of the need to create additional guarantees.

In comparative law, mechanisms can be found that address the concern that judicial review of wiretapping orders will become automatic or will tend to systematically support the position of the investigative authorities. In UK law, for example, there are provisions that give detailed structure to the considerations that must be taken when applying judicial review; and in U.S. law, there are provisions enabling the court to appoint an *amicus curia* (an independent external individual) so that the application hearing for the order, which is usually held *ex parte*, becomes more adversarial.

4. An independent supervisory authority and parliamentary supervision

Judicial and quasi-judicial review of surveillance of communication networks is reactive, and its response is limited to specific applications or orders. This kind of oversight does not address cases in which the authorities avoided applying for the relevant orders due to the absence of a legal obligation to do so or due to a narrow interpretation of the existing statutory obligations. As a result, some legal systems have empowered administrative or quasi-judicial authorities to oversee the security bodies' online surveillance activity.

In Israel, the Privacy Protection Authority (formerly the Israel Law and Technology Authority—ILTA) is the regulatory, supervisory, and enforcement body under the Protection of Privacy Law, the Credit Data Law, and the Electronic Signature Law. However, due to exemptions in the Protection of Privacy Law, the Authority does not, in practice, oversee the online surveillance activity of security and law enforcement agencies.

Establishing an independent supervisory body—or alternatively, expanding the powers of the Privacy Protection Authority so that it can oversee the propriety of data processing activities, including collection and retention, carried out as part of the surveillance of communication networks for security or policing purposes—may serve to introduce an additional actor dedicated to protecting the privacy interests of those under surveillance. It is desirable that such a body, in addition to being independent, should have the full oversight powers required to fulfill its role, such as powers to investigate in response to complaints lodged or at its own initiative, and powers to provide advisory and professional guidance regarding aspects of privacy protection in relevant regulation. Alongside investigative and inquiry powers, it should be granted the ability to make rulings with practical implications for the practices being scrutinized.

Currently, the scope of the Knesset's parliamentary review of police and Israel Security Agency online surveillance practices is restricted to statutory reports pursuant to the Wiretap Act, some of which are delivered behind closed doors. Similar reports under the provisions of the Communications Data Act were submitted for a limited period by virtue of a temporary provision in the law, which has since expired. An attempt to obtain these secret reports through a request under the Freedom of Information Law was rejected by the Supreme Court which, in a side comment, recommended that the state disclose these details voluntarily and before they are leaked, in order to secure public trust.

Recommendations

1. Issues lacking regulation under Israeli law

(**1**) **The extent of the powers granted each of the security and law enforcement bodies**. Regulation of the extent of the various powers of the police, the Israel Security Agency, the Military Intelligence Directorate, the Mossad, and other investigatory bodies should refer to the practices in which they are allowed to engage, the scope of collection permitted, the controls to be put in place, and the territorial application of these powers.

(**2**) **Bulk collection**. Israeli law should implement a general ban on bulk collection, unless strictly necessary for attaining narrow and detailed objectives, and subject to procedures that guarantee that the violation of rights is kept to the bare minimum.

(**3**) **Data retention**. Israeli law should apply provisions regarding the maximum period for which telecom providers can retain data. The authorities' ability to order providers to deviate from these provisions and retain data for a longer period would be subject to judicial order, limited to the attainment of narrow and detailed objectives, and subject

to procedures that guarantee that the violation of rights is kept to a minimum.

(**4**) **Data-mining and collection of open-source information (OSINT)**. Legislation should permit and prohibit actions related to cross-referencing of various databases, the different uses that can be made of the products of statistical processing, and the extent of automation and lack of human involvement in the process to be allowed. With respect to OSINT practices in social networks, the powers of the authorities to act in this arena should be defined, and limits placed on collection practices that are not absolutely passive (such as the use of fictional profiles to obtain access to information that is not entirely public).

(**5**) **Obtaining information from global communications platform providers**. Procedures for obtaining information from online communications platform providers, such as Facebook and Google, should be regulated by law. They should be limited to narrow objectives involving serious crime and national security and subjected to a test of near certainty and to judicial review.

(**6**) **Intercepting communications data**. Similar to the general ban on wiretapping, a general prohibition should apply to active interception of communications data—as opposed to the procurement of non-real-time data under the terms of the Criminal Procedure Law (Enforcement Powers—Communication Data), or according to the rules promulgated pursuant to the Israeli Security Agency Law. Regulations should be created to provide for cases in which said interception would be permitted, similar to the arrangements in the Wiretap Act.

2. Increasing transparency

(**1**) The veil of secrecy should be removed from the rules that govern the methods used by the Israeli Security Agency to obtain communications data from telecom providers, and the annual reports of the use of these

methods should be publicly disseminated to the extent possible. Similarly, the annual reports of the ISA's use of its powers under the Wiretap Act should also be published, to the extent possible.

3. Expansion of judicial review of online surveillance practices

(**1**) The scope of judicial review of online state surveillance should be extended to wiretapping carried out by the Israeli Security Agency and the Military Intelligence Directorate for security purposes, and to every request for communications data including urgent requests.

(**2**) The existing judicial review mechanism should be strengthened. Judicial discretion in granting orders may include instructions to consider alternatives with lesser violations of privacy, as well as restrictive procedures intended to ensure that no use of the information will be made beyond that which is required.

(**3**) It is possible to create an adversarial process by means of which public representatives, special advocates, or *amici curiae* could protect the interests of both public privacy and the privacy of the subject of the surveillance. Strengthening the adversarial basis of the process could be achieved by granting *locus standi* to communications providers, and by recognizing the surveillance subjects' and third parties' notification rights as a relative right subject to security considerations, which would enable compensation claims to be filed after the fact.

4. An independent supervisory authority

(**1**) An independent supervisory authority should be established, to review government authorities' ongoing online surveillance activities, to assess compliance with the provisions of orders, and to advise and provide professional guidance regarding the privacy protection aspects of relevant regulation.

(**2**) An alternative to the establishment of such a body would be an expansion of the Privacy Protection Authority's (formerly ILTA) powers, granting it supervisory powers over privacy protection in the online surveillance activities of the security and law enforcement authorities.

(**3**) Another alternative is the establishment of an ombudsman for privacy issues in online surveillance—an independent, impartial body with reactive powers to investigate complaints, find solutions without the need for extensive formalities, and periodically publicize its findings while keeping the complainants' identities secret.

5. Parliamentary supervision

(**1**) The heads of the security services should be obligated to report annually to the Knesset's Constitution, Law and Justice Committee and the Foreign Affairs and Defense Committee regarding the number of wiretaps carried out for state security purposes. The level of detail reported should be identical to that reported annually by the Ministry of Public Security on the exercise of these powers by the Israel Police.

(**2**) The temporary order contained in the Criminal Procedure Law (Enforcement Powers—Communication Data) should become permanent and require the Israel Police to report annually on their use of the powers granted by this law.

www.en.idi.org.il