PRIVACY INTERNATIONAL

In Advance of a Parliamentary Consultative Process

Privacy International's Analysis of the Italian Hacking Reform, under DDL Orlando

March 5 2017

PRIVACY INTERNATIONAL

05 May 2017

Privacy International's Analysis of the Italian Hacking Reform, under DDL Orlando, in Advance of a Parliamentary Consultative Process

Executive Summary

Privacy International is a non-profit, non-governmental organization based in London, the United Kingdom ("UK"), dedicated to defending the right to privacy around the world. Established in 1990, Privacy International undertakes research and investigations into government and corporate surveillance with a focus on the technologies that enable these practices. To ensure universal respect for the right to privacy, Privacy International advocates for strong national, regional and international laws that protect privacy. It has litigated or intervened in cases implicating the right to privacy in the courts of the United States, the UK, and Europe, including the European Court of Human Rights and the European Court of Justice. It also strengthens the capacity of partner organizations in developing countries to identify and defend against threats to privacy. Privacy International employs technologists, investigators, policy and advocacy experts, and lawyers, who work together to understand the technical underpinnings of novel surveillance technologies, and to consider how existing legal definitions and frameworks map onto such technologies.

Privacy International generally opposes hacking as a tool for surveillance. This position is grounded in two primary concerns. First, hacking has the potential to be far more intrusive than any other existing surveillance technique, including the interception of communications. Hacking permits governments to remotely access systems and therefore all of the information stored on those systems. Second, and equally worrisome, hacking has the potential to undermine the integrity, not only of the targeted system, but also of the internet as a whole. Hacking techniques are fundamentally designed to allow an unauthorized party to access and control another party's system. The security hole used by the government can also be exploited by anyone with the relevant technical expertise.

When reviewing Italy's sixth periodic report on the implementation of the International Covenant on Civil and Political Rights in its 119th Session of March 2017, the UN Human Rights Committee expressed concerns about state hacking:

> "The Committee is concerned about reports alleging a practice of intercepting personal communications by intelligence agencies and the employment of hacking techniques by them without explicit statutory authorization or clearly defined safeguards from abuse... The State party should review the regime regulating the interception of personal communications, hacking of digital devices, and the retention of communications data with a view to ensuring (a) that such activities conform with its obligations under Article 17 including with the principles of legality, proportionality, and necessity; (b) that robust independent oversight systems over surveillance, interception, and hacking, including by providing for judicial involvement in the authorization of such measures in all cases and affording persons affected with effective remedies in cases of abuse, including, where

possible, an ex post notification that they were subject to measures of surveillance or hacking..."[1]

While the DDL Orlando is an opportunity to fill the current legislative gap in the use of hacking for investigative purposes, PI believes that it falls short of the requirements of existing international human rights law.

Background

It has been well documented that Italian law enforcement has been utilizing malware[2] (commonly referred to as 'Trojans' in Italian discourse) to engage in hacking for criminal investigation purposes.[3] In fact, according to one report "the use of malware is the method of choice for Italy's law enforcement".[4] Initially the Courts did not consider hacking-based surveillance of devices to constitute a wiretap.[5] As a result such hacking did not require a warrant from the judge in charge of preliminary investigations. Rather the order of the Public Prosecutor alone was deemed sufficient.[6]

---

[1] Concluding Observations on the Sixth Periodic Report of Italy, Human Rights Committee, U.N. Doc. CCPR/C/ITA/CO/6, paras. 36-37 (28 Mar. 2017).

[2] Malware, a contraction of "malicious software," refers to computer code designed to perform actions on a system (such as a computer, laptop, or mobile phone) that, but for the malware, would not occur. In this context it is worth distinguishing between an "exploit" and a "payload," which is often conflated with malware. An "exploit" takes advantage of a security vulnerability in a computer system or application to permit malware to run. The "payload" refers to that part of malware that actually performs the intended actions on the system. For further reading see Brief of *Amicus Curiae* Privacy International in Support of Defendant-Appellee and in support of affirmance of the decision below, *U.S. v. Alex Levin*, United States Court of Appeals for the First Circuit, Case No. 16-1567, pp. 5-8 (10 Feb. 2017), *available at* https://www.documentcloud.org/documents/3458395-U-S-v-Levin-Privacy-International-Amicus-Brief.html.

[3] For further reading see Carola Frediani, *Intercettazioni col trojan, ecco la proposta di legge*, LA STAMPA (31 January 2017), *available at* http://www.lastampa.it/2017/01/31/italia/cronache/intercettazioni-col-trojan- ecco-la-proposta-di-legge-MP8BJ2PB0jCwMt84ofRSlM/pagina.html (noting that MP Quintarelli has said in a press conference that: "Today these tools are used without a system of guarantees and we do not even know how many people are subjected [to such measures of control]"); Bill Marczak et. al., *Mapping Hacking Team's "Untraceable" Spyware*, CitizenLab (17 February 2017), *available at https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/* (noting that Italy "is one of the most prolific users" of Remote Control System (RCS), a sophisticated computer spyware marketed and sold exclusively to governments by Milan-based Hacking Team).

[4] Legal Frameworks for Hacking by Law Enforcement, Study Commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, at the request of the Parliament Committee on Civil Liberties, Justice, and Home Affairs (LIBE) (March 2017), p. 59, *available at* http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf (hereinafter European Parliament's Policy Department C Report).

[5] *See, e.g.*, Italian Supreme Court of Cassation, Division V, Decision No. 24695 (14 Oct. 2009). This case legitimized the use of hacking tools to seize and copy documents already stored on a device, in this specific instance a computer hard disk used by the accused for work. The Court relied on a mischaracterization of the malware, grounding its decision on the erroneous analysis that hacking solely for the purpose of searching existing documents does not involve the interception of any "flow of communications" (as stated in Article 266-bis of the Italian Criminal Procedure Code), and thus does not constitute a wiretap. Downloading such documents, the Court ruled, merely involves an "operational relationship" with the microprocessor, falling short of interception. The ruling inaccurately describes the way hacking-based surveillance takes place and also ignores the potential use of malware for the collection of new documents or for manipulating data. The Court further endorsed this approach in a subsequent case. Italian Supreme Court of Cassation, Division VI, Bisignani Case – Decision No. 254865 (27 Nov. 2012).

[6] For further reading see Giuseppe Vaciago & David Silva Ramalho, *Online Searches and Online Surveillance: the Use of Trojans and Other Types of Malware as Means of Obtaining Evidence in Criminal Proceedings*, 13 Digital Evidence and Electronic Signature Law Review 88, 91-92 (2016).

2015 Supreme Court of Cassation Decision

In 2015 the Supreme Court of Cassation (*Corte Suprema di Cassazione*) stepped away from its previous precedent, concluding that hacking by law enforcement should be seen as "electronic surveillance" and thus should require a traditional "search and seizure" based warrant.[7] In doing so, the Court subjected such hacking to the Italian Code of Criminal Procedure. Article 266 of the Italian Code allows for the "interception of conversations or communications" in proceedings relating to a list of predefined serious crimes. Article 266-bis expands the surveillance powers authorized to include the "interception of the flow of communications related to computerized systems". Nonetheless, Art. 266(2) prohibits any interception carried out in a home or dwelling, or in another building or structure of private ownership, unless there is reason to believe that criminal activity has taken or is taking place within that building.

2016 Supreme Court of Cassation Decision (Joint Sections)

Given the qualifier in Article 266(2), concerning spying into dwellings, the Supreme Court of Cassation was asked to revisit its 2015 decision again in 2016. The question before the Court was whether Italian authorities could continue to hack devices, in light of the fact that such hacking could grant authorities unrestricted access to the device's environment (*i.e.* the dwelling), even in situations where no criminal activity has been undertaken inside them, in apparent contravention of Art. 266(2).[8] The Court acknowledged the varied uses of malware, mapping the capabilities of hacking to include: (1) the capture of all incoming or outgoing data traffic (*e.g.* browsing history, email usage, content of communications, geospatial location, text messages, and photos); (2) the ability to switch on and off the microphone and camera of a device, without its owner's knowledge; (3) searching the hard drive and copying all or part of the device's memory units; (4) deciphering everything that is typed on the keyboard, using key-loggers, and collecting anything that is seen on the screen, by taking screenshots, regardless of whether the owner uses encryption or other secure technologies.[9]

The Court noted that in light of the threats posed to society by "structured criminal organizations that have sophisticated technologies and significant financial resources", and in particular global terrorist organizations, the "current legislation as well as the constitutional principles" must "adapt effectively".[10] The Court distinguished between two categories of activities: "online searches" and "online surveillance". Whereas the former involved the copying of existing memory units, the latter involved all other forms of hacking-based surveillance. In light of the qualifier in Article 266(2), the Court ruled that as for "online surveillance" (*i.e.* "real time interception" using malware) such activities could be lawful under Article 266(2) but must be "limited exclusively to proceedings relating to offences of organized crimes" (namely mafia and terrorism related crimes).[11] The Court indicated that in

---

[7] Italian Supreme Court of Cassation, Division VI, Musumeci Case – Decision No. 27100 (26 May 2015).

[8] Italian Supreme Court of Cassation, Joint Sessions, Scurato Case – Decision No. 26889 (1 July 2016), Pres. Canzio, Conduct of Case, under "Svolgimento del processo", para. 2 (where the Court refers to "vera e propria intercettazione ambientale" - "real environmental interception").

[9] *Id*, under "Motivi della decisione", para. 2 (beginning with "Uno strumento tecnologico di questo tipo consente lo svolgimento di varie attività e precisamente", the Corut enumerates the various uses of a malware).

[10] *Id*. at para. 10.1.

[11] *Id*., at para. 11 (in the original Italian "Limitatamente ai procedimenti per delitti di criminalità organizzata, è consentita l'intercettazione di conversazioni o comunicazioni tra presenti mediante l'installazione di un captatore informatico in dispositivi elettronici portatili (ad es., personal computer, tablet, smartphone, ecc.) - anche nei

these circumstances, it would allow "the real-time interception of conversations or communications by installing a 'digital interceptor' (captatore informatico) in portable electronic devices (e.g. personal computer, tablet, smartphone, etc.)."[12] The Court therefore concluded that interception carried out by means of a "computer sensor" installed on a portable device would be in line with Article 266 of the Italian Criminal Code as well as Italy's constitution and obligations under Article 8 of the European Convention of Human Rights and Fundamental Freedoms,[13] which protects the right to privacy. It is worth noting that the Court did recognize that the judge authorizing the warrant is incapable of foreseeing the extent of the possible intrusion into the private home of the hacked individual, by the introduction of malware, "resulting in an inability to exercise adequate control over the actual compliance with the legislation".[14] Nonetheless, the Court did not find this to warrant against the exercise of hacking powers under the current regulatory framework.

Legislative Proposals

In recent years four different draft legislative proposals have been put forward, which seek to explicitly regulate hacking-based surveillance.[15] None of these proposals have advanced in Parliament. Nonetheless, what was unique about the two most recent proposals – the 'Casson' amendment and the 'Quintarelli' draft law – was that they differentiated between the various capabilities of malware "as the degree of invasiveness differs across functions".[16] Both, thus, introduced enhanced oversight, safeguards, and minimization procedures, in light of the specific features of hacking as a distinct field of surveillance activities.

DDL Orlando

On 15 March 2017, the Italian Senate voted on a Bill, put forward by Justice Minister Andrea Orlando, that will amend the Code of Criminal Procedure (hereinafter: "DDL Orlando", or "the Bill").[17] The Bill is now pending approval by the Italian House of Representatives (*Camera dei Deputati*). The Bill is part of a broader reform of the Italian justice system, and it includes a commitment to amend Article 268 of the Rules of Criminal Procedure (the Rule which operationalizes and sets limitations on Article 266, discussed above). Under DDL

---

luoghi di privata dimora ex art. 614 c.p., pure non singolarmente individuati e anche se ivi non si stia svolgendo l'attività criminosa"). See also para. 10.1.

[12] *Id*.

[13] *Id*, at para. 10.2.

[14] *Id*. at para. 6.

[15] As summarized by Vaciago & Ramalho, *supra* note 6, at 92-93 ("In addition to case decisions, during the last year in Italy there has been a succession of four draft laws to bring the investigative tool within the scope of Italian Code of Criminal Procedure: the first draft law was presented as part of a new law on responding to terrorism. In this draft law, a misguided attempt was made to add into Article 266-bis that regulates computer surveillance, the capability of carrying out such type of activity 'also through the use of a tool or software for the remote acquisition of communications and data found in a computer system'. Fortunately, this amendment was criticized by several members of Parliament and by the Prime Minister himself, inasmuch as it introduced the possibility of undertaking utterly invasive activities vis-à-vis citizens without any legal guarantee other than that of viewing such a tool as a mere instance of electronic surveillance. The same fate was met by the 'Greco' Bill of 2 December 2015. At the beginning of 2016, two draft laws were developed ('Casson' amendment and 'Quintarelli' draft law) with a seemingly different approach from the ones of the previous year.").

[16] European Parliament's Policy Department C Report, *supra* note 4, at p. 86. For a detailed analysis of the Quintarelli draft law, see pp. 87-89. *See also*, Letter by Access Now to Stefano Aterno, Re: Disciplina dell'uso dei captatori legali nel rispetto delle garanzie individuali (29 March 2017), *available at* www.civicieinnovatori.it/?page_id=211.

[17] Changes to the Criminal Code, Criminal Procedure Code and Penal Procedure Bill (15 Mar. 2017), *available at* http://www.senato.it/service/PDF/PDFServer/BGT/01009188.pdf.

Orlando, the Government is mandated to regulate (via a legislative decree) hacking for criminal investigations. In so doing, the Bill, as currently drafted, provides the Government with some general guidance on what such a Decree might entail. Below is Privacy International's Summary of the Bill's section relating to hacking, as well as our initial legal analysis of the proposal. We hope that this information will assist both the legislative and executive branches in their consultative processes surrounding both the Bill and the potential Decree.

Summary of DDL Orlando's Provisions on Hacking

Article 82 of DDL Orlando empowers the Government to adopt a legislative decree for the reform of the law on the interception of communications in line with the guidelines set forth in Article 84. Article 84, subsection (e), concerns the regulation of interception of communications by malaware ("disciplinare le intercettazioni di communicazioni mediante immisione di captatori informatici"), i.e. one form of hacking-based surveillance. The Bill proceeds to offer 8 general guidelines concerning such regulation (Article 84(e)(1-8)):

1. The activation of a microphone on a device does not occur automatically, and can only be performed manually in accordance with a warrant from a judge and limited to the instructions laid out in that warrant.

2. Any audio recording done through such activation must follow the same logging and documentation requirements laid down in Article 268 to the Rules of Criminal Procedures on regular communications interception, including start and end times of the interception.

3. The activation of the device can be justified for the prevention of crimes listed in Article 51 paragraphs 3-a and 3-quarter of the Criminal Procedure Code (relating to organized crime, including mafia and terrorism), or otherwise only in such dwellings where a criminal activity is taking place. In any event, the authorization decree of the judge must state the reasons for why hacking is necessary for the conduct of the investigation.

4. All recording must be transferred to to a server controlled by the public prosecutor in order "to ensure originality and integrity of all records". Once the recording is completed, on the recommendation of the Judicial Police, the malware must be deactivated "and rendered permanently inoperable".

5. All malware used for criminal investigations must conform to technical requirements established by ministerial decree to be issued within thirty days from the date of entry into force of the legislative decree. The ministerial decree must constantly take into account technical developments to ensure that operations meet "suitable standards of technical reliability, safety, and efficacy".

6. Without prejudice to the powers of Courts in ordinary cases, a Prosecutor may authorize the above-mentioned interception without prior judicial authorization in "cases of urgency". In the emergency decree, the Prosecutor must explain the specific circumstances that make it impossible to apply to a court and the reasons why the hacking in question is necessary for the conduct of investigations. The Prosecutor is

also required to seek subsequent validation of the Court within a period not exceeding 48 hours.

7. Information gathered from malware and originally authorised for a specific crime, can be used as evidence in the prosecution of other crimes listed in Article 380 of the Code of Criminal Procedure (such as for example drug trafficking or theft), if it is later found "indispensable" for the investigation of such crimes.

8. The Bill acknowledges the potential for the "occasional" capture of collateral data, of individuals not connected to the matter under investigation. The Bill establishes a limited safeguard, whereby such information, if intercepted, should not be disclosed, shared, or otherwise made known.

Legal Analysis of DDL Orlando's Provisions on Hacking

At the outset, it is important to strongly affirm Privacy International's policy position opposing hacking as a tool for surveillance. This position is grounded in two primary concerns. First, hacking has the potential to be far more intrusive than any other existing surveillance technique, including the interception of communications. Hacking permits governments to remotely access systems and therefore all of the information stored on those systems. Moreover, a growing number of devices making up the "Internet of Things" – such as a refrigerator that records when and what a person eats or a television that records what a person watches and his or her reactions – are documenting intimate details about the lives of individuals. By accessing this information, governments can acquire a deep and comprehensive view into a person's life, revealing his or her identity, thoughts, relationships, interests, and activities. Hacking also permits government control over the functionality of systems, as has been discussed above, and thus allows for the complete and continuous monitoring of a person's life. The privacy intrusions of hacking are enormously amplified should a government target network infrastructure itself (imagine the hacking of a DNS server used by a company, and through it the hacking of the systems of all of the server's users, the employees of that company).

Second, and equally worrisome, hacking has the potential to undermine the integrity, not only of the targeted system, but also of the internet as a whole. Hacking techniques are fundamentally designed to allow an unauthorized party to access and control another party's system. The security hole used by the government can be exploited by anyone with the relevant technical expertise.

Certainly a Government can never justify reliance on hacking as a "method of choice", as the report by Parliament Committee on Civil Liberties, Justice, and Home Affairs (LIBE) seems to suggest is happening in Italy.[18] As was further noted by the U.N. Special Rapporteur on Freedom of Expression:

> "Offensive intrusion software such as Trojans, or mass interception capabilities, constitute such serious challenges to traditional notions of surveillance that they cannot be reconciled with existing laws on surveillance and access to private information. These are not just new methods for conducting surveillance; they are new forms of

[18] *See supra* note 4.

> surveillance. From a human rights perspective, the use of such technologies is extremely disturbing."[19]

This is particularly true considering the fact that one of the core motivations behind previous iterations of hacking bills in Italy has been to provide State investigators with the capacity to circumvent encryption technologies.[20] As the preamble to the Quintarelli Bill notes, for example, "impenetrable encryption" has allowed users to engage in communications which are "inaccessible" to law enforcement. It is in this context that hacking is perceived as a desirable tool despite the fact that it weakens the security that individuals may enjoy online.[21]

Those general concerns notwithstanding, the regulation of hacking powers through public legislation is a necessary first step, if only because the Italian authorities have already been using hacking capabilities without explicit statutory authorization as the Human Rights Committee has rightly criticized.[22] Therefore, such regulation moves Italy a step closer towards meeting the standard of legality required under international human rights law. That said, the Bill suffers from a number of structural deficits and lacks safeguards and minimization procedures, which render it, in its current form, incompatible with Italy's international human rights obligations. Privacy International wishes to bring to the attention of Parliament and the Executive the following ten key concerns:

1. Legality

As adopted by the United Nations General Assembly, "surveillance of digital communications must be consistent with international human rights obligations and must be conducted on the basis of a legal framework, which must be publicly accessible, clear, precise, comprehensive and non-discriminatory".[23] At the heart of the principle of legality stands an important assumption that placing "intrusive surveillance regimes on a statutory footing" allows for their subjection "to public and parliamentary debate."[24]

It is in this context, that the means by which the current Bill was passed in the Senate raises concerns. The bill was hastily put together and incorporated into a broader justice reform initiative that has been pending for years. Significant amendments or parliamentary scrutiny

---

[19] *See supra* note 1.

[20] *See e.g.* the 'Quintarelli' draft, Prposta di Legge, Disciplina dell'uso dei Captatori legali nel rispetto delle garanzie individuali, Preamble, 2(1-ter). The full Italian bill, and its summary in English are both available at http://www.civicieinnovatori.it/wp-content/uploads/2017/02/Sintesi-PDL-captatori-EN.pdf.

[21] U.N. Human Rights Council Resolution on the Safety of Journalists, U.N. Doc. A/HRC/33/L.6 (26 Sept. 2016) ("*Emphasizes* that, in the digital age, encryption and anonymity tools have become vital for many journalists to exercise freely their work and their enjoyment of human rights, in particular their rights to freedom of expression and to privacy, including to secure their communications and to protect the confidentiality of their sources, and calls upon States not to interfere with the use of such technologies, with any restrictions thereon complying with States' obligations under international human rights law"); Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, U.N. Doc. A/HRC/29/32 (22 May 2015) ("States should not restrict encryption and anonymity, which facilitate and often enable the rights to freedom of opinion and expression. Blanket prohibitions fail to be necessary and proportionate. States should avoid all measures that weaken the security that individuals may enjoy online, such as backdoors, weak encryption standards and key escrows").

[22] *See supra* note 1.

[23] U.N. General Assembly Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/RES/69/166 (18 Dec. 2014).

[24] Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, U.N. Doc. A/HRC/34/61, para. 36 (21 Feb. 2017).

are unlikely in light of this process. Moreover, the *modus operandi* of the Bill, whereby Parliament merely sets generalized guidelines while the Executive is the one that actually translates those guidelines to operative provisions (free from any additional parliamentary scrutiny) is unsatisfactory.

As for the requirement of foreseeability, Italy is under an obligation to clearly and narrowly define the conditions under which hacking capabilities may be utilized.[25] The scope of application of the Bill is unclear and leaves significant regulatory loopholes.

a. *Subjects of Regulation*: The Bill applies to criminal investigations launched by the Public Prosecutor and conducted by law enforcement under the Italian Criminal Code. In this regard the Bill carves out hacking conducted by Italian intelligence agencies, namely the Information and External Security Agency (Agenzia Informazioni e Sicurezza Esterna, AISE), the Information and Internal Security Agency (Agenzia Informazioni e Sicurezza Interna, AISI), and the Department of Information and Security (Reparto Informazioni e Sicurezza, RIS). It is important to note that the Italian Intelligence agencies have reportedly engaged in hacking activities in the past.[26] Hacking that is not regulated should not be permitted as it will run in contradiction with the principle of legality. In this regard it is important to clarify, as the European Court of Human Rights has done in *Liberty v. U.K.*, that there is no ground to apply different levels of protections between law enforcement and intelligence agencies.[27]

b. *Material Scope of Regulation*: The current Bill only addresses one aspect of hacking operations (the use of the "payload"[28]), and within it only addresses one such use (the activation of a microphone). The Bill is silent as to the use of the payload for other purposes (such as the ones listed in the 2016 Supreme

---

[25] *See e.g.* Leander v. Sweden, App. No. 9248/81, European Court of Human Rights, Judgment, para. 51 (26 March 1987) ("However, the requirement of foreseeability in the special context of secret controls of staff in sectors affecting national security cannot be the same as in many other fields. Thus, it cannot mean that an individual should be enabled to foresee precisely what checks will be made in his regard by the Swedish special police service in its efforts to protect national security. Nevertheless, in a system applicable to citizens generally, as under the Personnel Control Ordinance, the law has to be sufficiently clear in its terms to give them an adequate indication as to the circumstances in which and the conditions on which the public authorities are empowered to resort to this kind of secret and potentially dangerous interference with private life. In assessing whether the criterion of foreseeability is satisfied, account may be taken also of instructions or administrative practices which do not have the status of substantive law, in so far as those concerned are made sufficiently aware of their contents. In addition, where the implementation of the law consists of secret measures, not open to scrutiny by the individuals concerned or by the public at large, the law itself, as opposed to the accompanying administrative practice, must indicate the scope of any discretion conferred on the competent authority with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference.").

[26] *See e.g.*, Pierluigi Paganini, *Italian intelligence is planning to invest in solutions that could allow its counter-terrorism agents to monitor Sony's PlayStation Network*, Security Affairs (30 Nov. 2015), *available at* http://securityaffairs.co/wordpress/42397/hacking/italian-intelligence-monitoring-playstation.html. *See also* Italian Intelligence Agency Steals Sensitive Info from Indian Embassy, The Indian Express (30 July 2011), *available at* http://archive.indianexpress.com/news/italian-intelligence-agency-steals-sensitive-info-from-indian-embassy/824712/.

[27] Liberty and Others v. the United Kingdom, App. No. 58243/00, European Court of Human Rights, Judgment, para. 63 (1 July 2008).

[28] *See supra* note 2.

Court of Cassation Decision abovementioned).[29] Once again, let us repeat that any hacking, including any functionality of a malware, that is not expressly regulated, violates the principle of legality and should thus not be permitted. Moreover, no guidelines are offered as to other aspects of hacking operations, including for example what are lawful propagation methods (*e.g.* social engineering attacks,[30] or zero-day exploits[31]), nor does it address other uses of malware in the course of "online surveillance" as the Italian Supreme Court understands it.

c. *Temporal Scope of Regulation*: Under Article 267(3) of the Italian Criminal Code, the interception of telecommunications can be authorized for up to 15 days, subject to extensions of two weeks at a time. Such extensions may continue without limit (*i.e.* there is no overall cap on extensions), nor are there specific requirements in law as to what the Government is required to show in order to receive an extension. The Bill would seem to apply this provision *mutatis mutandis* to the hacking powers granted to the Police.[32] Considering the intrusiveness of hacking, such periods are disproportionately extensive and cannot be justified. Moreover, the Bill sets a lower standard for review on hacking in "emergency situations" than the one that exists for regular communications interceptions under Article 267(2). Whereas for the latter, a Court must be notified within 24 hours (and given 48 hours to determine whether to allow the interception to proceed), under the Bill, notifications for "emergency situations" may be transmitted to a Court within 48 hours, not 24. Coupled with the fact that both the Code and the new Bill do not identify what such "emergency situations" entail, the Bill does not meet the standard of legality.[33]

2. Extraterritoriality

The Bill does not expressly state its territorial scope of application.[34] It is thus open for interpretation whether under the Bill a judge may authorize the hacking of devices outside the territory of Italy. In accordance with international law, the *enforcement* jurisdiction of States to investigate, prosecute, or apprehend an offender extraterritorially is limited by the territorial sovereignty of the foreign State.[35] The principal tool in such cases "is to utilize a

---

[29] *See supra* note 9.

[30] Social engineering involves tricking someone into performing a specific action, such as revealing a username or password, to compromise a target system's security and permit unauthorized access. A common social engineering technique, called phishing, is to send an email to someone while impersonating a reputable person or organization, in order to obtain sensitive information. Phishing emails may also contain a link or attachment infected with malware, which installs on the target system once clicked by the unsuspecting user.

[31] A "zero-day exploit" is an exploit unknown to the software of hardware manufacturer.

[32] By embedding hacking powers within the regulatory provisions which govern traditional wiretapping.

[33] For the reasons discussed, the temporal scope of the regulation also fails to meet the standards of necessity and proportionality. Those standards are discussed in further detail below.

[34] This failure directly relates to the principle of legality but also raises issues distinct from it.

[35] *S.S. Lotus (France v. Turkey)*, 1927 P.C.I.J. (Ser. A), No. 10, pp. 18-19 ("Now the first and foremost restriction imposed by international law upon a State is that – failing the existence of a permissive rule to the contrary – it may not exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention"); INTERNATIONAL BAR ASSOCIATION, REPORT OF THE TASK FORCE ON EXTRATERRITORIAL JURISDICTION, p. 10 (2009) (noting that a "state cannot investigate a crime,

Mutual Legal Assistance Treaty ("MLAT"), a treaty-based mechanism that facilitates law enforcement cooperation and assistance in support of an on-going criminal investigation or proceeding".[36] As Recognized by the U.N. Special Rapporteur David Kaye, "the inability of the mutual legal assistance treaty regime to keep pace with cross-border data demands may drive States to resort to invasive extraterritorial surveillance measures".[37] A State should not circumvent the MLA process, but rather work to bring it into the digital age.[38] This is of particular concern in the context of devices using anonymizing technology, where the practice of certain law enforcement authorities has been to assume that "anonymized targets are *territorially located* in all stages of implementation and enforcement," to avoid the need to rely on MLATs.[39]

3. Necessity and Proportionality[40]

The Bill authorizes the use of microphone activation not only in cases of threats of organized crime against the integrity of the State, namely terrorism and mafia, but in other crimes as well (so long as they are being committed from within a dwelling). Hacking, if ever authorized, must be limited only to the most serious crimes, a point which was made by the Supreme Court of Cassation 2016 Decision.[41] Moreover, the Bill suffers from a series of deficiencies that fall short of meeting the principles of necessity and proportionality. In particular:

a. The Bill does not set a limitation whereby hacking can only be applied when it is absolutely necessary for the purposes of conducting the investigation, and where all less intrusive means have been exhausted (a last resort standard). The Bill further does not set any evidentiary standards on what information will be deemed relevant and material to establishing suspicion of a magnitude that would justify a hacking operation.

---

arrest a suspect, or enforce its judgment or judicial process in another state's territory without the latter state's permission").

[36] Ahmad Ghappour, Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web, Stan. L. Rev. 20 (forthcoming, 2017).

[37] Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, U.N. Doc. A/HRC/32/38, para. 61 (11 May 2016).

[38] *See e.g.*, U.N. Security Council Res. 2322, Threats to International Peace and Security Caused by Terrorists Acts U.N. Doc. S/RES/2322, OP13(B) (2016) (Calls upon all States to: ...(b) enact and, where appropriate, review and update extradition and mutual legal assistance laws in connection with terrorism-related offences, consistently with their international obligations, including their obligations under international human rights law, and to consider reviewing national legal assistance laws and mechanisms related to terrorism and updating as necessary in order to strengthen their effectiveness, especially in the light of the substantial increase in the volume of requests for digital data").

[39] Ghappour, *supra* 36, at 20-21.

[40] U.N. Human Rights, General Comment No. 16: Article 17 (Right to Privacy), U.N. Doc. HRI/GEN/1/Rev.1 at 21 (8 Apr. 1988) ("The expression 'arbitrary interference' is also relevant to the protection of the right provided for in article 17. In the Committee's view the expression 'arbitrary interference' can also extend to interference provided for under the law. The introduction of the concept of arbitrariness is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances."); Digital Rights Ireland Ltd. v. Minister of Communications, Marine and Natural Resources et al. (C-293/12); Kärntner Landesregierung and others (C-594/12), Joined Cases, Court of Justice of the European Union, Grand Chamber, Judgment (8 Apr. 2014) ("according to the settled case-law of the Court, the principle of proportionality requires that acts of the EU institutions be appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives").

[41] *See supra* note 11.

b. The Bill allows for the use, as evidence, of data relating to other crimes, other than the ones which were the subject of the warrant, which were incidentally collected as part of a lawful operation. This could incentivize the overly broad use of hacking, in order to catch through such means information of relevance to other investigations. Information gathered by a hacking technique should only be used for the purposes for which it was gathered, under the warrant, so as to minimize access to irrelevant and immaterial information.

c. The Bill does not set any limitations on the method, extent, and duration of the proposed hacking operations.

d. The Bill does not acknowledge potential risks and damage to the security and integrity of the targeted system and systems generally, and how those risks and damage will be mitigated or corrected, so as to enable an assessment of the proportionality of the hack against its security implications.

e. The Bill amorphously references the "occasional" interception of communications concerning innocent bystanders. The Bill only establishes a limited safeguard whereby such information should not be shared. Any collection of collateral data must be taken into consideration in the proportionality analysis, and such considerations must be introduced in law. Moreover, stronger safeguards should be introduced in the case of such incidental collection, for example the obligation to immediately delete any irrelevant information gathered. In this regard it is important to clarify that all hacking operations must be targeted and based on reasonable suspicion,[42] and that any collection (let alone access to) incidental communications must be mitigated to the greatest extent possible.

f. Particular importance should be given to individuals whose communications are likely to be subject to professional secrecy or immunities under Italian law. This includes journalists, lawyers, judges, medical professionals, social workers, mental health specialists, members of the clergy, parliamentarians, and diplomats. The Bill does not provide any additional protections for these individuals' devices and information.[43]

---

[42] *See e.g.*, Roman Zakharov v. Russia, App. No. 47143/06, European Court of Human Rights, Judgment, para. 260 (4 Dec. 2015) ("Turning now to the authorisation authority's scope of review, the Court reiterates that it must be capable of verifying the existence of a reasonable suspicion against the person concerned, in particular, whether there are factual indications for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures, such as, for example, acts endangering national security. It must also ascertain whether the requested interception meets the requirement of 'necessity in a democratic society', as provided by Article 8 § 2 of the Convention, including whether it is proportionate to the legitimate aims pursued, by verifying, for example whether it is possible to achieve the aims by less restrictive means.").

[43] *See e.g.*, Kopp v. Switzerland, App. No. 23224/94, European Court of Human Rights, Judgment, paras. 71-75 (25 Mar. 1998) (regarding surveillance of lawyers); U.N. Doc. A/HRC/29/32, *supra* note 21, para. 59 (22 May 2015) (regarding surveillance of journalists and human rights defenders).

4. Judicial Authorization

As the European Court of Human Rights noted in the *Klass v. Germany* case, as early as 1978:

> "Review of surveillance may intervene at three stages: when the surveillance is first ordered, while it is being carried out, or after it has been terminated. As regards the first two stages, the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual's knowledge. Consequently, since the individual will necessarily be prevented from seeking an effective remedy of his own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding the individual's rights. In addition, the values of a democratic society must be followed as faithfully as possible in the supervisory procedures if the bounds of necessity, within the meaning of Article 8 para. 2 (art. 8-2), are not to be exceeded. One of the fundamental principles of a democratic society is the rule of law, which is expressly referred to in the Preamble to the Convention. The rule of law implies, inter alia, that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence, impartiality and a proper procedure."[44]

The Bill only calls on the Government authorities to seek a warrant in a case of microphone activation. It is important to reiterate that any other hacking operation, not introduced by law and not further authorized by a Judge, should be prohibited. This approach is in line with longstanding positions of both the Human Rights Committee and the European Court of Human Rights (ECtHR) to require a targeted warrant for any surveillance activity.[45]

Moreover, the Bill as currently drafted only calls on the Government to provide the judge with information as to "the reasons for which hacking is necessary for the conduct of the investigation". This language does not cover the full scope of information required for a Judge to engage in a necessity and proportionality analysis, which in itself is not directly mandated in the current draft of the Bill. Prior to any hacking operation the Government must, at a minimum, establish:

- a high degree of probability that:
    - a serious crime has been or will be carried out;

---

[44] Klass and Others v. Germany, App. No. 5029/71, European Court of Human Rights, Judgment, para. 55 (6 Sept. 1978).

[45] *See e.g.*, Concluding Observations on the Fourth Periodic Report of the Republic of Korea, Human Rights Committee, U.N. Doc. CCPR/C/KOR/CO/4, para. 43 (3 Dec. 2015); Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, App. No. 62540/00, European Court of Human Rights, Judgment, paras. 85-88 (28 June 2007).

- the targeted system contains information relevant and material to the serious crime or acts amounting to a specific threat to the national security interest alleged; and
- evidence relevant and material to the investigation of the serious crime or acts will be obtained by hacking the targeted system

The request for a warrant thus must be specific and targeted and provide robust information about the identity of the person who uses the system, its location, and other identifying details regarding the system.[46] The request for a warrant must also provide information concerning the methods to be employed and the scope of their intrusion into the targeted system.

The requests for such warrants are likely to involve information of a technical nature, and judges reviewing such warrants thus must be able to consult technical advisers with competence in the relevant technologies. The Bill as currently drafted does not address this point.

5. Retention and Destruction of Information

On the issue of destruction of information, the European Court of Human Rights ruled in *Weber and Saravia v. Germany* that:

> "the destruction of personal data as soon as they [are] no longer needed to achieve their statutory purpose, and [...] the verification at regular, fairly short intervals of whether the conditions for such destruction [are] met, constitute an important element in reducing the effects of the interference with the secrecy of telecommunications to an unavoidable minimum."[47]

The Bill ignores these important safeguards by not establishing any obligations on the means by which data collected by hacking is to be retained or destroyed. The Bill only establishes that once the hacking operation has ceased, malware must be deactivated "and rendered permanently inoperable". However, the Bill does not address the question of the retention and the destruction of information gathered by malware. The Bill must clarify that any irrelevant or immaterial information that is obtained pursuant to an authorized hack must be immediately destroyed, and that relevant and material information obtained by a hack should be retained subject to clear temporal limitations. Finally, the Bill should clarify whether any sharing of hacked information with other law enforcement agencies or with foreign governments is subject to the same regulatory frameworks that exist for all other forms of surveillance.

6. Transparency and Oversight

One of the key components of the United Nations General Assembly Resolution on the Right to Privacy in the Digital Age, adopted in consensus, concerns protecting transparency and oversight. The Resolution calls on all States:

---

[46] *See supra* note 42.

[47] Weber and Saravia v. Germany, App. No. 54934/00, European Court of Human Rights, Decision on Admissibility, para. 132 (29 June 2006).

> "To establish or maintain existing independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data."[48]

The Bill as currently drafted establishes no specific obligations to disclose information, even in aggregate, pertaining to requests to hack by law enforcement and intelligence agencies in Italy. The Bill also does not establish any specific *ex-post* review mechanisms (judicial, administrative, and parliamentary) to increase scrutiny by the general public and further protections from abuse of this power. These matters must be resolved prior to any use of hacking powers. As noted by the UN High Commissioner for Human Rights:

> "a lack of effective oversight has contributed to a lack of accountability for arbitrary or unlawful intrusions on the right to privacy in the digital environment. Internal safeguards without independent, external monitoring in particular have proven ineffective against unlawful or arbitrary surveillance methods. While these safeguards may take a variety of forms, the involvement of all branches of government in the oversight of surveillance programmes, as well as of an independent civilian oversight agency, is essential to ensure the effective protection of the law."[49]

7. Security and Integrity of Systems

The Bill must expressly prohibit the undermining of the security and integrity of devices and/or systems. In this regard it is troubling that the Bill ignores the method of propagation of malware, in particular whether law enforcement can use exploits (including zero day exploits[50]) to hack a device. To the extent that such attacks are permissible they may negatively impact the security and integrity of devices and systems, as they take advantage of security weaknesses that may affect devices and systems beyond those targeted. Moreover, certain propagation methods, such as for example a *watering hole* attack (where the attacker installs malware on a website, subsequently exploiting weaknesses in devices that access the site), is by default indiscriminate, and should therefore be explicitly prohibited.[51] The lack of propagation method regulation is therefore a significant concern.

The Preamble to the Council of Europe Convention on Cybercrime, to which Italy is a State party, establishes that "it is necessary to deter action directed against the confidentially, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data". It would be an unfortunate consequence, that in trying to defend the integrity and security of systems (by fighting against acts of cyber and physical terrorism, for example), the Italian Government would develop and employ tools that might cause the same effects.

---

[48] U.N. Doc. A/RES/69/166, *supra* note 23, at OP4.
[49] Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37, para. 37 (30 June 2014)
[50] *See supra* note 31.
[51] For further reading see Brief of *Amicus Curiae* Privacy International, *supra* note 2.

The introduction in the Bill of a requirement for the drafting of a "ministerial decree" that will ensure that operations meet "suitable standards of technical reliability, safety, and efficacy" is a welcome step. Nonetheless, the Bill does very little in offering significant guidance on the content of this decree and the means by which malware will not be used to imperil the security and integrity of systems.

8. Integrity of Information

The Bill does not expressly prohibit the tampering with or modification of data on the hacked device. The Bill must clarify that warrants issued in accordance with it may only allow for the passive collection of information, as opposed to offensive manipulation or deletion of data. Moreover, the target of an authorized hack must be informed, as we discuss below, of the method and extent of the hack, including all software used, so that he or she may understand the nature of the information obtained and investigate alterations or deletions to information or breaches of the chain of custody, as appropriate.

The fact that the Bill introduces an obligation whereby "all recording must be transferred to a controlled server in order "to ensure originality and integrity of all records," is a welcome provision. However, the Bill must establish access restrictions and procedural safeguards, to ensure that only qualified and trained personnel may access the obtained data and only for the purposes authorised in the warrant.

9. Notification

The Bill does not require any notification of the targeted person or entities, or of other identifiable users of a targeted system. The absence of this requirement runs counter to international human rights standards, as was described by the U.N. Special Rapporteur on Freedom of Opinion and Expression:

> "Individuals should have a legal right to be notified that they have been subjected to communications surveillance or that their communications data has been accessed by the State. Recognizing that advance or concurrent notification might jeopardize the effectiveness of the surveillance, individuals should nevertheless be notified once surveillance has been completed and have the possibility to seek redress in respect of the use of communications surveillance measures in their aftermath."[52]

Moreover, the Bill equally does not require the notification of affected service providers and software and hardware manufacturers on the method and extent of hacks involving their software and/or hardware.

10. Redress

The Bill does not establish any specific remedies or means of redress for aggrieved individuals whose devices were unlawfully hacked. As noted by the U.N. High Commissioner for Human Rights, effective remedies involve:

---

[52] Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, U.N. Doc. A/HRC/23/40, para. 82 (17 Apr. 2013).

"prompt, thorough, and impartial investigation of alleged violations... for remedies to be effective, they must be capable of ending ongoing violations, for example, through ordering deletion of data or other reparation. Such remedial bodies must have 'full and unhindered access to all relevant information, the necessary resources and expertise to conduct investigations, and the capacity to issue binding orders'. Fourth, where human rights violations rise to the level of gross violations, non-judicial remedies will not be adequate, as criminal prosecution will be required."[53]

[53] *See* U.N. Doc. A/HRC/27/37, *supra* note 49, at para. 41.