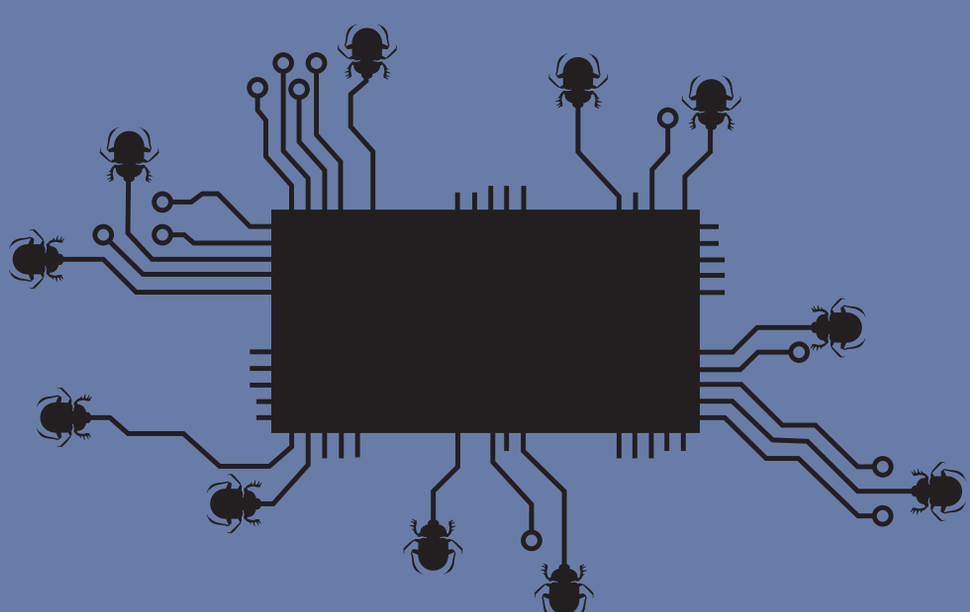
PRIVACY INTERNATIONAL

Government Hacking and Surveillance: 10 Necessary Safeguards



PRIVACY INTERNATIONAL

Government Hacking and Surveillance: 10 Necessary Safeguards

Table of Contents

Introduction

A growing number of governments around the world are embracing hacking to facilitate their surveillance activities. But many deploy this capability in secret and without a clear basis in law. In the instances where governments seek to place such powers on statutory footing, they are often doing so without the safeguards and oversight applicable to surveillance activities under international human rights law.

Hacking can present unique and grave threats to our privacy and security. For these reasons, even where governments conduct surveillance in connection with legitimate activities, such as gathering evidence in a criminal investigation or intelligence, they may never be able to demonstrate that hacking as a form of surveillance is compatible with international human rights law. To date, however, there has been insufficient public debate about the scope and nature of these powers and their privacy and security implications.

Our proposed safeguards are designed to help interested parties assess government hacking in light of applicable international human rights law. They are further designed to address the security implications of government hacking. Generally speaking, security considerations must be embedded into surveillance safeguards and oversight mechanisms. We separately explain the legal and conceptual bases for our proposed safeguards in "Government Hacking and Surveillance: Commentary to the 10 Necessary Safeguards."

These safeguards form part of a comprehensive strategy pursued by Privacy International and others across civil society to ensure that:

- Governments and industry prioritise defensive security;
- Our devices, networks and services are secure and privacy-protective by design and that these protections are maintained; and
- Legal and technological protections apply to everyone across the world.

Why We Are So Concerned about Government Hacking for Surveillance

Government hacking is unlike any other form of existing surveillance technique. Hacking is an attempt to understand a system better than it understands itself, and then nudging it to do what the hacker wants. Fundamentally speaking, hacking is therefore about causing technologies to act in a manner the manufacturer, owner or user did not intend or did not foresee.

Governments can wield this power remotely, surreptitiously, across jurisdictions, and at scale. A single hack can affect many people, including those who are incidental or unrelated to a government investigation or operation.

Governments may resort increasingly to hacking to facilitate surveillance in the future. In the digital age, data about individuals often resides in the hands of companies, and those companies may be based in a foreign jurisdiction. Governments have therefore typically relied on the cooperation of a third party – a company, foreign government, or even both – to access this data. This process is typically time-consuming and may prove fruitless if the company or foreign government is unwilling or unable to provide access. Hacking can therefore be more convenient than legal processes involving multiple parties.

Sometimes companies may place their users' data out of their own reach, for example, by choosing not to collect it or by encrypting it. Under claims of "going dark," governments are pressuring companies for privileged access to their systems and to redesign security mechanisms. All the while, governments are developing and procuring capabilities to hack those very same companies' products and services, which may allow them to collect data that would otherwise not be captured, or to bypass encryption and other security features.

Through hacking, governments may directly exert influence over or interfere with technologies, which are ever more seamlessly integrated into lives, economies, and societies. Government hacking capabilities are constrained only by a government's own resources and capacities. We believe we must prioritise systems and data security and that further constraints must be applied to restrict and restrain the power of governments to hack.

Privacy

Hacking permits governments remote access to systems and therefore potentially to all of the data stored on those systems. For an increasing number of people, personal digital devices contain the most private information they store anywhere, replacing and consolidating address books, physical correspondence, journals, filing cabinets, photo albums and wallets. Increasingly, governments may direct their hacking powers towards new and emerging devices, like the Internet of Things and body-worn and –embedded devices, such as health sensors.

Hacking also permits governments to conduct novel forms of real-time surveillance. Hacking permits governments to covertly turn on a device's microphone, camera, and GPS-based locator technology. Through hacking, a government can also capture continuous screenshots of the hacked device or see anything input into and output from that device, including login details and passwords, internet browsing histories, and documents and communications the user never intended to disseminate.

Hacking permits the manipulation of data in a world that is increasingly data-driven. By controlling the functionality of systems, hacking permits governments to delete data or recover data that has been deleted. Hacking also permits governments to corrupt or plant data, send fake communications or data from the device, or add or edit code to add new capabilities or alter existing ones and erase any trace of the intrusion. In a world where information about us is increasingly expressed as data, minute changes to that data – a password, GPS coordinates, a document – can have radical effects.

The privacy intrusions of hacking are enormously amplified should a government interfere with communications networks and their underlying infrastructure. By hacking a network provider, for instance, a government might gain access not only to the provider's system, but also through the data stored there, to the systems of all its users. Governments may also interfere with different types of networks and their infrastructure, such as those connecting banks. Hacking directed at networks could be for the purpose of conducting surveillance against specific individuals, groups or countries, or across numerous jurisdictions.

Government hacking also encompasses the hacking of devices in the government's physical custody. While this type of hacking raises many of the same concerns articulated above, it also presents unique privacy implications. Data that resides on devices can include data that the user of that device does not even know exists and cannot access. For instance, mobile phones may contain data the user believes was deleted or sensor-generated data unknown and unavailable to the user that could divulge biographic, physiological or biometric information.

Security

Government hacking for surveillance is equally concerning from a security perspective. Computer systems are complex and, almost with certainty, contain vulnerabilities. People are also complex and their interactions with systems also give rise to vulnerabilities; they can be exploited to interfere with their own systems.

Identifying vulnerabilities, testing them by developing exploits, and sharing these results is necessary for security. But government hacking for surveillance does not seek to secure systems. In the surveillance context, the government identifies vulnerabilities, not to secure systems through testing and coordinated disclosure, but to exploit them to facilitate a surveillance objective. This activity may not only undermine the security of the target system but also of other systems.

Security concerns also abound when governments take advantage of people to interfere with their own systems. Phishing, for example, is a common social engineering technique whereby a hacker impersonates a reputable person or organization. Phishing attacks typically take the form of an email or text message, which may contain a link or attachment infected with malware. These techniques prey on user trust, which is critical to maintaining the security of systems and the internet as a whole.

Security is hard and the government is not the only critical actor. For a more detailed discussion of the interplay between security and hacking, see our piece, “A conflict of security: why we are so concerned about government hacking from a security perspective.”

Scope of Our Safeguards

The term "hacking" is difficult to define. For these safeguards, Privacy International posits the following definition:

> Hacking is an act or series of acts, which interfere with a system, causing it to act in a manner unintended or unforeseen by the manufacturer, user or owner of that system. System refers both to any combination of hardware and software or a component thereof.

Privacy International recognises that there may be instances of government hacking that do not conform to this definition and should nonetheless be subject to scrutiny. We are open to feedback as to how to alter this definition to accommodate those other forms of government hacking.

Governments conduct hacking for a broad range of purposes. The safeguards only address hacking activities whose purpose is either to gather evidence in a criminal investigation or intelligence or to assist the evidence or intelligence gathering process. The safeguards do not address hacking that rises to the level of a threat or a use of force or armed attack, or which is conducted as part of an active armed conflict. For example, a hacking operation to shut down critical infrastructure, such as an energy grid, in a foreign country would not be covered by these safeguards. However, an operation to re-route the traffic of a telecommunications provider so that such traffic will flow past an interception point, would be subject to these safeguards.

The safeguards apply to government hacking conducted both within the territory of a state and extraterritorially. One of the safeguards also explicitly addresses hacking conducted extraterritorially. The safeguards apply regardless of whether hacking is conducted by government officials or persons exercising elements of governmental authority, directed or controlled by a government, or whose conduct is later acknowledged and adopted by a government as its own.

Government Hacking and Surveillance: 10 Necessary Safeguards

1. Legality

Government hacking powers must be explicitly prescribed by law and limited to those strictly and demonstrably necessary to achieve a legitimate aim. That law must be accessible to the public and sufficiently clear and precise to enable persons to foresee its application and the extent of the interference. It should be subject to periodic review by means of a participatory legislative process.

2. Security and Integrity of Systems

Prior to carrying out a hacking measure, government authorities must assess the potential risks and damage to the security and integrity of the target system and systems generally, as well as of data on the target system and systems generally, and how those risks and/or damage will be mitigated or corrected. Government authorities must include this assessment in any application in support of a proposed hacking measure.

Government authorities must not compel hardware or software manufacturers or service providers to facilitate government hacking, including by compromising the security and integrity of their products and services.

3. Necessity and Proportionality

Prior to carrying out a hacking measure, government authorities must, at a minimum, establish:

(i) A high degree of probability that:

a. A serious crime or act(s) amounting to a specific, serious threat to national security has been or will be carried out;

b. The system used by the person suspected of committing the serious crime or act(s) amounting to a specific, serious threat to national security contains evidence relevant and material to the serious crime or act(s) amounting to a specific, serious threat to national security interest alleged;

c. Evidence relevant and material to the serious crime or act(s) amounting to a specific, serious threat to national security alleged will be obtained by hacking the target system;

(ii) To the greatest extent possible, the identity of the person suspected of committing the serious crime or act(s) amounting to a specific, serious threat to national security and uniquely identifying details of the target system, including its location and specific configurations;

(iii) All less intrusive methods have been exhausted or would be futile, such that hacking is the least intrusive option;

(iv) The method, extent and duration of the proposed hacking measure;

(v) Data accessed and collected will be confined to that relevant and material to the serious crime or act(s) amounting to a specific, serious threat to national security alleged and the measures that will be taken to minimize access to and collection of irrelevant and immaterial data;

(vi) Data will only be accessed and collected by the specified authority and only used and shared for the purpose and duration for which authorisation is given;

(vii) The potential risks and damage to the security and integrity of the target system and systems generally, as well as of data on the target system and systems generally, and how those potential risks and damage will be mitigated or corrected, so as to enable an assessment of the proportionality of the proposed hacking measure against its security implications.

4. Judicial Authorisation

Prior to carrying out a hacking measure, government authorities must make an application, setting forth the necessity and proportionality of the proposed measure to an impartial and independent judicial authority, who shall determine whether to approve such measure and oversee its implementation. The judicial authority must be able to consult persons with technical expertise in the relevant technologies, who may assist the judicial authority in understanding how the proposed measure will affect the target system and systems generally, as well as data on the target system and systems generally. The judicial authority must also be able to consult persons with expertise in privacy and human rights, who may assist the judicial authority in understanding how the proposed measure will interfere with the rights of the target person and other persons.

5. Integrity of information

Government authorities must not add, alter or delete data on the target system, except to the extent technically necessary to carry out the authorised hacking measure. They must maintain an independently verifiable audit trail to record their hacking activities, including any necessary additions, alterations or deletions. Where government authorities rely on data obtained through an authorised hacking measure, they must disclose the method, extent and duration of the hacking measure and their audit trail so that the target person can understand the nature of the data obtained and investigate additions, alterations or deletions to information or breaches of the chain of custody, as appropriate.

6. Notification

Government authorities must notify the person(s) whose system(s) have been subject to interference pursuant to an authorised hacking measure, regardless of where the person(s) reside, that the authorities have interfered with such system(s). Government authorities must also notify affected software and hardware manufacturers and service providers, with details regarding the method, extent and duration of the hacking measure, including the specific configurations of the target system. Delay in notification is only justified where notification would seriously jeopardize the purpose for which the hacking measure was authorised or there is an imminent risk of danger to human life and authorisation to delay notification is granted by an impartial and independent judicial authority.

7. Destruction and Return of Data

Government authorities must immediately destroy any irrelevant or immaterial data that is obtained pursuant to an authorised hacking measure. That destruction must be recorded in the independently verifiable audit trail of hacking activities. After government authorities have used data obtained through an authorised hacking measure for the purpose for which authorisation was given, they must return this data to the target person and destroy any other copies of the data.

8. Oversight and Transparency

Government authorities must be transparent about the scope and use of their hacking powers and activities, and subject those powers and activities to independent oversight. They should regularly publish, at a minimum, information on the number of applications to authorise hacking approved and rejected; the identity of the applying government authorities; the offences specified in the applications; and the method, extent and

duration of authorised hacking measures, including the specific configurations of target systems.

9. Extraterritoriality

When conducting an extraterritorial hacking measure, government authorities must always comply with their international legal obligations, including the principles of sovereignty and non-intervention, which express limitations on the exercise of extraterritorial jurisdiction. Government authorities must not use hacking to circumvent other legal mechanisms – such as mutual legal assistance treaties or other consent-based mechanisms – for obtaining data located outside their territory. These mechanisms must be clearly documented, publicly available, and subject to guarantees of procedural and substantive fairness.

10. Effective Remedy

Persons who have been subject to unlawful government hacking, regardless of where they reside, must have access to an effective remedy.

Government Hacking and Surveillance: Commentary to the 10 Necessary Safeguards

Introduction

Government hacking for the purposes of surveillance can present unique and grave threats to our privacy and security. The 10 Necessary Safeguards are designed to help interested parties assess government hacking in light of applicable international human rights law. They are further designed to address the security implications of government hacking.

This Commentary explains the legal and conceptual bases for each safeguard. It also elaborates on the application of the safeguards in practice. The "Legal Commentary" section beneath each safeguard articulates the legal underpinning for that safeguard by reference to the international human rights framework. The "Implementation Notes" that follow provide guidance on the application of the safeguard.

1. Legality

Government hacking powers must be explicitly prescribed by law and limited to those strictly and demonstrably necessary to achieve a legitimate aim. That law must be accessible to the public and sufficiently clear and precise to enable persons to foresee its application and the extent of the interference. It should be subject to periodic review by means of a participatory legislative process.

Legal Commentary

- International human rights law provides that any interference with the right to privacy must be in accordance with the law.[1] At the heart of the principle of legality is the important premise that placing "intrusive surveillance regimes on a statutory footing" subjects them to "public and parliamentary debate."[2] Legality is also closely tied to the concept of "arbitrary

[1] See Article 17(1), International Convention on Civil and Political Rights ("ICCPR") ("No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence . . . ."); Article 11, American Convention on Human Rights ("ACHR") ("2. No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence . . . . 3. Everyone has the right to the protection of the law against such interference . . . ."); Article 8(2), European Convention of Human Rights ("ECHR") ("There shall be no interference by a public authority with the exercise of [the right to respect for private and family life] except such as is in accordance with the law . . . ."); see also U.N. Human Rights Committee, General Comment No. 16 (Article 17 ICCPR), 8 Apr. 1988, para. 3 (noting that "[t]he term 'unlawful' means that no interference can take place except in cases envisaged by the law" and that "[i]nterference authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant"); Principle 1, International Principles on the Application of Human Rights to Communications Surveillance ("Necessary and Proportionate Principles"). The Necessary and Proportionate Principles seek to apply established international human rights law to modern communications surveillance. They are the outcome of a global consultation with civil society groups, industry, and international experts in communications surveillance law, policy and technology and have been endorsed by over 600 organizations around the world.

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

interference," the idea being that the exercise of a secret power carries the inherent risk of its arbitrary application.[3]

- The meaning of "law" implies certain minimum qualitative requirements of accessibility and foreseeability. The U.N. Human Rights Committee has elaborated on the meaning of "law" for the purposes of Article 19 of the International Covenant on Civil and Political Rights ("ICCPR"), which protects the right to freedom of opinion and expression, as follows: "[A] norm, to be characterized as a 'law,' must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly and it must be made accessible to the public. . . . Laws must provide sufficient guidance to those charged with their execution to enable them to ascertain what sorts of expression are properly restricted and what sorts are not."[4]
    - The Inter-American Commission on Human Rights ("IACHR") has similarly determined, in its interpretation of Article 11 of the American Convention on Human Rights ("ACHR"): "Article 11.2 specifically prohibits 'arbitrary or abusive' interference with th[e] right [to privacy]. This provision indicates that in addition to the condition of legality, which should always be observed when a restriction is imposed on the rights of the Convention, the state has a special obligation to prevent 'arbitrary or abusive' interferences. The notion of 'arbitrary interference' refers to elements of injustice, unpredictability and unreasonableness . . . ."[5]
    - The requirements of accessibility and foreseeability are also reflected in the jurisprudence of the European Court of Human Rights ("ECtHR"): "Firstly, the law must be adequately accessible: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case. Secondly, a norm cannot be regarded as a law unless it is formulated with sufficient precision to enable the citizen to regulate his conduct; he must be able—if need be with appropriate advice—to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail."[6]
- The U.N. General Assembly has recognized the application of the principle of legality to the surveillance context, resolving that the "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."[7]

---

[3] Malone v. United Kingdom, European Court of Human Rights, App. No. 8691/79, 2 Aug. 1984, para. 67 ("Especially where a power of the executive is exercised in secret, the risks of arbitrariness are evident."); see also U.N. Human Rights Committee, General Comment No. 16, supra, at para. 4 (noting that "the expression 'arbitrary interference' can also extend to interference provided for under the law" and that "[t]he 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").

[4] U.N. Human Rights Committee, General Comment No. 34 (Article 19 ICCPR), 12 Sept. 2011, para. 25.

[5] Ms. X and Y v. Argentina, Inter-American Commission on Human Rights, Case 10.506, Report No. 38/96, 15 Oct. 1996, para. 92.

[6] Sunday Times v. United Kingdom, European Court of Human Rights, App. No. 6538/74, 26 Apr. 1979, para. 49.

[7] U.N. General Assembly Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/RES/71/199, 19 Dec. 2016 ("2016 U.N. General Assembly Resolution on the Right to Privacy in the Digital Age"); see also U.N. Human Rights Council Resolution on the Right to Privacy in the

- The ECtHR has explicitly applied the principle of legality to the surveillance context. In *Weber & Saravia v. Germany*, the Court elaborated on the "minimum safeguards that should be set out in statute law in order to avoid abuses of power" where the state conducts surveillance: "[1] the nature of the offences which may give rise to a[ ] [surveillance] order; [2] a definition of the categories of people liable to [be subject to surveillance]; [3] a limit on the duration of [surveillance]; [4] the procedure to be followed for examining, using and storing the data obtained; [5] the precautions to be taken when communicating the data to other parties; and [6] the circumstances in which recordings may or must be erased or the tapes destroyed."[8]
- The Inter-American Court of Human Rights ("IACtHR") has also explicitly applied the principle of legality to the surveillance context. In *Escher et al. v. Brazil*, the Court held that surveillance measures "must be based on a law that must be precise." The Court further observed that the law must "indicate the corresponding clear and detailed rules, such as the circumstances in which this [surveillance] measure can be adopted, the persons authorized to request it, to order it and to carry it out, and the procedure to be followed."[9]
- In 2013, the U.N. and IACHR Special Rapporteurs on Freedom of Expression issued a Joint Declaration on surveillance, in which they emphasized the application of the principle of legality in the surveillance context: "[S]tates must guarantee that the interception, collection and use of personal information, including all limitations on the right of the affected person to access this information, be clearly authorized by law in order to protect them from arbitrary or abusive interference with their private interests. The law must establish limits with regard to the nature, scope and duration of these types of measures; the reasons for ordering them; the authorities with power to authorize, execute and monitor them; and the legal mechanisms by which they may be challenged."[10]

International human rights law requires that any interference with the right to privacy must not only be in accordance with law but must also be necessary and proportionate.[11] The principle of necessity, which is partially reflected in this safeguard, is sometimes expressed as requiring that any interference with

Digital Age, U.N. Doc. A/HRC/34/7, 23 Mar. 2017 ("2017 U.N. Human Rights Council Resolution on the Right to Privacy in the Digital Age") ("1. Recalls that States should ensure that any interference with the right to privacy is consistent with the principles of legality, necessity and proportionality").

8 Weber & Saravia v. Germany, European Court of Human Rights, App. No. 54934/00, 29 June 2006, para. 95; see also Malone v. United Kingdom, supra, at para. 67 (noting that "the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence").

9 Escher et al. v. Brazil, Inter-American Court of Human Rights, Judgment (on Preliminary Objections, Merits, Reparations, and Costs), Series C No. 200, 6 July 2009, para. 131.

10 U.N. Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression and the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Joint Declaration on Surveillance Programs and their Impact on Freedom of Expression, 21 June 2013, para. 8.

11.1 See U.N. Human Rights Committee, Toonen v. Australia, Comm. No. 488/1992, U.N. Doc. CCPR/C/50/D/488/1992, 31 Mar. 1994, para. 8.3 ("[A]ny interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case."); Office of the U.N. High Commissioner for Human Rights, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37, 30 June 2014, para. 23, ("These authoritative sources [HRC General Comments

the right to privacy be "necessary to achieve a legitimate aim."[12] The legal commentary for the "Necessity and Proportionality" safeguard addresses the principle of necessity in further detail.

Implementation Notes

- This safeguard provides that government hacking powers be "explicitly prescribed by law." Generally speaking, laws that grant the government broad, vague surveillance powers cannot authorise hacking pursuant to the principle of legality. The use of the word "explicitly" also emphasises that government hacking powers must be subject to a regulatory framework tailored to its unique privacy and security implications, which the safeguards as a whole seek to address. The interpretation of an existing framework, which authorises other surveillance activities such as wiretapping, to authorise hacking will therefore fall afoul of the safeguards. Similarly, a legal framework authorising hacking that copies and pastes verbatim frameworks that apply to other surveillance activities will also fall afoul of the safeguards.
- This safeguard also provides that any law explicitly prescribing government hacking powers "be subject to periodic review by means of a participatory legislative process." The development of new technology, especially the internet, has transformed and continues to transform the way individuals communicate with each other and increased the amount of information that can be collected by orders of magnitude. As modern communications have evolved, governments have developed in parallel novel methods of collecting, storing and analysing communications and data. Hacking is an example of a novel form of surveillance, but is itself constantly evolving to comprise new techniques. The pace of technological change in the surveillance context, and the lack of clarity that new technologies pose to the application of legal principles, demand periodic review of laws authorising government hacking.

16, 27, 29, 31, and 34 and the Siracusa Principles] point to the overarching principles of legality, necessity and proportionality . . . ."); 2017 U.N. Human Rights Council Resolution on the Right to Privacy in the Digital Age, supra, at para. 2 ("Recall[ing] that States should ensure that any interference with the right to privacy is consistent with the principles of legality, necessity and proportionality").

[12] Article 30 ACHR provides that restrictions of the rights recognized by the Convention "may not be applied except in accordance with laws enacted for reasons of general interest and in accordance with the purpose for which such restrictions have been established." Article 8 ECHR is somewhat more specific, providing that "[t]here shall be no interference by a public authority with the exercise" of the right to privacy "except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others." See also Office of the U.N. High Commissioner for Human Rights, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37, 30 June 2014), para. 23 ("OHCHR Report on the Right to Privacy in the Digital Age") ("The limitation must be necessary for reaching a legitimate aim . . . . The onus is on the authorities seeking to limit the right to show that the limitation is connected to a legitimate aim."); Principle 2, Necessary and Proportionate Principles ("Laws should only permit Communications Surveillance by specified State authorities to achieve a legitimate aim that corresponds to a predominantly important legal interest that is necessary in a democratic society.").

2. Security and Integrity of Systems

Prior to carrying out a hacking measure, government authorities must assess the potential risks and damage to the security and integrity of the target system and systems generally, as well as of data on the target system and systems generally, and how those risks and/or damage will be mitigated or corrected. Government authorities must include this assessment in any application in support of a proposed hacking measure.

Government authorities must not compel hardware or software manufacturers or service providers to facilitate government hacking, including by compromising the security and integrity of their products and services.

Legal Commentary

- The U.N. Special Rapporteur on Freedom of Expression has explained that individuals exercise their right to privacy by communicating in a manner that is "private" and "secure." The Special Rapporteur defined these terms as follows: "Privacy of communications infers that individuals are able to exchange information and ideas in a space that is beyond the reach of other members of society, the private sector, and ultimately the State itself. Security of communications means that individuals should be able to verify that their communications are received only by their intended recipients, without interference or alteration, and that the communications they receive are equally free from intrusion."[13] The Special Rapporteur has also explained the linkage between the right to privacy and security, noting that as individuals have adopted "e-mail, instant-messaging, Voice-over-Internet Protocols, videoconferencing and social media," they have also "developed a need for security online, so that they could seek, receive and impart information without the risk of repercussions, disclosure, [or] surveillance." The Special Rapporteur further noted that it is "critical that individuals find ways to secure themselves online, that Governments provide such safety in law and policy and that corporate actors design, develop and market secure-by-default products and services." The Special Rapporteur concluded that "States should avoid all measures that weaken the security that individuals may enjoy online."[14]
- The U.N. Special Rapporteur on Freedom of Expression has also identified the important role corporate actors play in both "the changes in the way we communicate, receive and impart information" as well as "in facilitating State surveillance," including by "respond[ing] to requirements that digital networks and communications infrastructure be designed to enable intrusion by the State." The Special Rapporteur therefore recognised the need for States "to meet their international human rights obligations when they contract with, or legislate for, corporate actors where there may be an impact upon the enjoyment of human rights" and to "ensure that the private sector is able to carry out its functions independently in a manner that

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

[14] Report of the U.N. 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, paras. 6, 11, 60 ("2015 Report of the U.N. Special Rapporteur on Freedom of Expression").

promotes individuals' human rights." The Special Rapporteur concluded that "States must refrain from forcing the privacy sector to implement measures compromising the privacy [and] security . . . of communications services."[15]

Implementation Notes

- This safeguard provides that government authorities must undertake a security assessment prior to carrying out a hacking measure and include this assessment in any application in support of such a measure.
    - As discussed in the legal commentary above, the exercise of the right to privacy is linked to the security of the devices, networks and services individuals rely on to communicate with each other. Accordingly, the security implications of a hacking measure are relevant to an assessment of the scope and nature of that measure's interference with the right to privacy.
    - The potential scale of the threats posed to security by government hacking for surveillance also undergird the requirement that government authorities undertake a security assessment prior to carrying out a hacking measure. Computer systems, almost with certainty, contain flaws. These flaws may be vulnerabilities that can impact a system's integrity and they may be exploited to interfere with a system, causing it to act in a manner unintended or unforeseen by the manufacturer, user or owner. Hacking is essential to identifying vulnerabilities, testing them by developing exploits, and sharing these results, which is critical for security. But in the surveillance context, the government seeks vulnerabilities, not to secure systems through testing and disclosure, but to exploit them to facilitate a surveillance objective. This activity has the potential to undermine the security not only of the target system but also of other unrelated systems.
        - The government's exploitation of a vulnerability to facilitate a surveillance objective is a choice to perpetuate the insecurity of a system, which many people may use, and may therefore be susceptible to similar attacks by other actors. Exploiting vulnerabilities in this manner is in considerable tension with the broader goal of securing systems.
        - The government's hacking measure(s) themselves may also proliferate to systems beyond the target system. When a government deploys malware, for example, it may be challenging to fully control its distribution. In a social engineering attack, a link infected with malware, directly emailed to a target, might be forwarded onto others or posted on social media. A "watering hole" attack, even when targeting a specific group of individuals, cannot entirely control who lands on an infected website.
    - As we continue to integrate computer systems into the fabric of our lives, economies and societies, safeguarding the security of those systems

[15] 2013 Report of the U.N. Special Rapporteur on Freedom of Expression, supra, at paras. 72-73, 76-77, 96 (citing Office of the U.N. High Commissioner for Human Rights, Guiding Principles on Business and Human Rights, 2011); see also 2015 Report of the U.N. Special Rapporteur on Freedom of Expression , supra, at para. 28.

becomes increasingly important. Government authorities seeking to carry out a hacking measure – and judicial authorities determining whether to authorise such a measure – must therefore embed a security assessment into their decision-making processes.

- This safeguard also provides that government authorities must not compel companies to facilitate government hacking activities, including by compromising the security and integrity of their products and services. Our devices, networks and services are, by and large, designed, manufactured and sold by companies and companies therefore play a critical role in securing them. When government authorities seek to compel companies to facilitate hacking, they are asking companies to undermine the security of their own products and services, which can in turn imperil the security of all users of those products or services. This form of assistance is unlike other forms of company assistance in the surveillance context, which, in the digital age, has typically consisted of accessing and disclosing data stored by the company.

3. Necessity and Proportionality

Prior to carrying out a hacking measure, government authorities must, at a minimum, establish:

(1) A high degree of probability that:

   b. A serious crime or act(s) amounting to a specific, serious threat to national security has been or will be carried out;

   c. The system used by the person suspected of committing the serious crime or act(s) amounting to a specific, serious threat to national security contains evidence relevant and material to the serious crime or act(s) amounting to a specific, serious threat to national security interest alleged;

   d. Evidence relevant and material to the serious crime or act(s) amounting to a specific, serious threat to national security alleged will be obtained by hacking the target system;

(2) To the greatest extent possible, the identity of the person suspected of committing the serious crime or act(s) amounting to a specific, serious threat to national security and uniquely identifying details of the target system, including its location and specific configurations;

(3) All less intrusive methods have been exhausted or would be futile, such that hacking is the least intrusive option;

(4) The method, extent and duration of the proposed hacking measure;

(5) Data accessed and collected will be confined to that relevant and material to the serious crime or act(s) amounting to a specific, serious threat to national security alleged and the measures that will be taken to minimise access to and collection of irrelevant and immaterial data;

(6) Data will only be accessed and collected by the specified authority and only used and shared for the purpose and duration for which authorisation is given;

(7) The potential risks and damage to the security and integrity of the target system and systems generally, as well as of data on the target system and systems generally, and how those potential risks and damage will be mitigated or corrected, so as to enable an assessment of the proportionality of the proposed hacking measure against its security implications.

Legal Commentary

- International human rights law requires that any interference with the right to privacy must not only be in accordance with law but must also be necessary and proportionate.[16] These principles were authoritatively confirmed in the U.N. Human Rights Council resolution on "the right to privacy in the digital age," adopted by consensus in March 2017.[17]
- The principle of necessity "implies that restrictions must not simply be useful, reasonable or desirable to achieve a legitimate government objective," but rather, that "a State must demonstrate in 'specific and individualized fashion the precise nature of the threat' that it seeks to address, and a 'direct and immediate connection between the expression and the threat.'"[18] As discussed in the legal commentary for the "Legality" safeguard, this concept of necessity is also sometimes expressed as requiring that any interference with the right to privacy be "necessary to achieve a legitimate aim."[19]
    - The IACHR Special Rapporteur for Freedom of Expression has applied the principle of necessity to the surveillance context, noting that "in order for an online communications surveillance program to be appropriate, States must demonstrate that the limitations to the rights to privacy and freedom of expression arising from those programs are strictly necessary in a democratic society to accomplish the objectives they pursue." In addition, the Special Rapporteur observed that, "it is insufficient for the measure to be 'useful,' 'reasonable,' or 'opportune.'"

[16] See Toonen v. Australia, supra, at para. 8.3 ("[A]ny interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case."); OHCHR Report on the Right to Privacy in the Digital Age, supra, para. 23 ("These authoritative sources [U.N. Human Rights Committee General Comments 16, 27, 29, 31, and 34 and the Siracusa Principles] point to the overarching principles of legality, necessity and proportionality . . . .").

[17] 2017 U.N. Human Rights Council Resolution on the Right to Privacy in the Digital Age, supra, at para. 2 ("Recall[ing] that States should ensure that any interference with the right to privacy is consistent with the principles of legality, necessity and proportionality").

[18] Brief of Amici Curiae, U.N. Human Rights Experts in Support of Plaintiff-Appellant and Reversal, John Doe (Kidane) v. The Federal Democratic Republic of Ethiopia, D.C. Ct. App., No. 16-7081, 1 Nov. 2016, p. 14 (citing U.N. Human Rights Committee, General Comment No. 34, supra, at para. 35). The U.N. human rights experts authoring the brief were the U.N. Special Rapporteurs on Freedom of Expression, Freedom of Peaceful Assembly, and the Situation of Human Rights Defenders.

[19] Article 30 ACHR provides that restrictions of the rights recognized by the Convention "may not be applied except in accordance with laws enacted for reasons of general interest and in accordance with the purpose for which such restrictions have been established." Article 8 ECHR is somewhat more specific, providing that "[t]here shall be no interference by a public authority with the exercise" of the right to privacy "except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others." See also OHCHR Report on the Right to Privacy in the Digital Age, supra, para. 23 ("The limitation must be necessary for reaching a legitimate aim . . . . The onus is on the authorities seeking to limit the right to show that the limitation is connected to a legitimate aim."); Principle 2, Necessary and Proportionate Principles ("Laws should only permit Communications Surveillance by specified State authorities to achieve a legitimate aim that corresponds to a predominantly important legal interest that is necessary in a democratic society.").

Rather, the State must clearly establish "the true and compelling need to impose the limitation."[20]

- The ECtHR has also applied the principle of necessity to interferences with the right to privacy in the surveillance context. In *Szabó & Vissy v. Hungary,* the Court indicated that given "the potential of cutting-edge surveillance technologies to invade citizens' privacy," the "legitimate aim" requirement had to be interpreted as follows: "A measure of secret surveillance can be found as being in compliance with the Convention only if it is strictly necessary, as a general consideration, for the safeguarding [of] democratic institutions and, moreover, if it is strictly necessary, as a particular consideration, for the obtaining of vital intelligence in an individual operation. In the Court's view, any measure of secret surveillance which does not correspond to these criteria will be prone to abuse by the authorities with formidable technologies at their disposal. The Court notes that both the Court of Justice of the European Union and the United Nations Special Rapporteur require secret surveillance measures to answer to strict necessity – an approach it considers convenient to endorse."[21]

- The principle of proportionality requires that the interference with privacy be both "in proportion to the aim and the least intrusive option available."[22] The U.N. Special Rapporteur for Counter-Terrorism has provided additional guidance to States on demonstrating proportionality in the surveillance context. He has submitted that "proportionality involves balancing the extent of the intrusion into Internet privacy rights against the specific benefit accruing to investigations undertaken by a public authority in the public interest."[23] He has also indicated that "[i]n the context of covert surveillance . . . [t]he proportionality of any interference with the right to privacy should . . . be judged on the particular circumstances of the individual case." He emphasized, however, that "in no case may the restrictions be applied or invoked in a manner that would impair the essence of a Covenant right." The Office of the U.N. High Commissioner for Human Rights has similarly observed that "any limitation to the right to privacy must not render the essence of the right meaningless and must be consistent with other human rights."[24]

---

[20] Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Freedom of Expression and the Internet, 31 Dec. 2013, paras. 159-60 ("IACHR Special Rapporteur for Freedom of Expression Report").

[21] Szabó & Vissy v. Hungary, European Court of Human Rights, App. No. 37138/14, 12 Jan. 2016, para. 73.

[22] OHCHR Report on the Right to Privacy in the Digital Age, supra, at para. 23; see also Toonen v. Australia, supra, at para. 8.3; Report of the U.N. Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, A/HRC/13/37, 28 Dec. 2009, para. 49 ("2009 Report of the U.N. Special Rapporteur on Counter Terrorism") ("[P]rotections [of the right to privacy] require States to have exhausted less-intrusive techniques before resorting to others. . . . States must incorporate this principle into existing and future policies as they present how their policies are necessary, and in turn proportionate."); Brief of U.N. Human Rights Experts, John Doe (Kidane) v. The Federal Democratic Republic of Ethiopia, supra, at pp. 14-15 (stating that proportionality requires that "the restrictions are . . . the least intrusive amongst those which might achieve their protective function . . . [and] proportionate to the interest to be protected"); Principle 5, Necessary and Proportionate Principles.

[23] Report of the U.N. Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, U.N. Doc. A/69/397, 23 Sept. 2014, para. 51 ("2014 Report of the U.N. Special Rapporteur on Counter Terrorism").

[24] OHCHR Report on the Right to Privacy in the Digital Age, supra, at para. 23; see also Zakharov v. Russia, European Court of Human Rights, App. No. 47143/06, 4 Dec. 2015, para. 232 (observing that there existed "the risk that a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it").

- The IACHR Special Rapporteur for Freedom of Expression has also discussed the proportionality analysis in the surveillance context, indicating that "in order to define if a measure is proportioned, its impact on the capacity of the Internet to guarantee and promote freedom of expression should be evaluated." The Special Rapporteur urged that "[g]iven the importance of the exercise of these rights in a democratic system, the law must authorize access to personal data and communications only under the most exceptional circumstances defined in the law." The Special Rapporteur further observed: "When fairly open-ended grounds such as national security are invoked as the reason to monitor personal data and correspondence . . . [t]heir application should be authorized solely when there is a definite risk to the protected interests, and when that harm is greater than society's general interest in maintaining the rights to privacy and the free expression of thought and the circulation of information."[25]

Implementation Notes

- This safeguard provides that government authorities must establish, at a minimum, a series of factors prior to carrying out a "hacking measure." The use of the phrase "hacking measure" serves to emphasise that the government must subject specific steps in a hacking operation to separate judicial authorisation processes. The need to chain authorisations in this manner results from the complications in demonstrating necessity and proportionality in the hacking context.
  - In certain circumstances, government authorities may lack information regarding the identity of the target person and/or relating to the target system of that person. (This scenario is distinguishable from one in which the government lacks a target altogether and seeks authorisation for a hacking measure to "fish" for targets, which would fail the necessity requirement.) This information can be elusive, for example, where a target person uses technology, such as a virtual private network ("VPN"), to protect their anonymity or secure their information. In such circumstances, certain identifying details about the person and/or system may first require interfering with the system to obtain that information. (For that reason, the safeguard provides that government authorities must establish "[t]o the greatest extent possible," the identity of the target person and "uniquely identifying details" of the target system).
  - Modern systems allow multiple users (or multiple user profiles, which can correspond to one or more users). Government authorities may therefore find it difficult to pinpoint with accuracy the target person, even if it has targeted a particular system. Modern systems also permit users to store many different kinds of intimate information or to communicate in many different ways, which can present challenges to minimising access to and collection of information.
  - By subjecting specific steps in a hacking operation to separate judicial authorisation processes, government authorities may be able to resolve some of these necessity and proportionality challenges. For example,

[25] IACHR Special Rapporteur for Freedom of Expression Report, supra, at paras. 161-62.

where they lack information regarding the target person and/or relating to the target system, they may first seek authorisation to interfere with the system for the limited purpose of determining this information. They may then use those details to form the basis of a subsequent application for authorisation to interfere with the system to access and collect data on the target system. Or for example, where government authorities seek to target a particular system but lack details allowing it to minimise access to and collection of relevant and material information, they may first seek authorisation to interfere with the system for the limited purpose of determining information that would allow for such minimisation (e.g. to determine what services are running on the system).

- Government authorities should also subject different forms of surveillance through hacking to separate judicial authorisation processes. For example, they cannot seek a single authorisation to access stored data and to conduct real-time surveillance through a microphone or camera. Because each purpose raises distinct privacy and security concerns, they should be subject to distinct necessity and proportionality analyses.

- In (1)(a), this safeguard provides that government authorities must establish a "high degree of probability" that "a serious crime or act(s) amounting to a specific, serious threat to national security has been or will be carried out".
  - The "high degree of probability" standard comes from the International Principles on the Application of Human Rights to Communications Surveillance ("Necessary and Proportionate Principles").[26]
  - Under international human rights law, "serious crime" and "national security" may constitute legitimate aims pursuant to the principle of necessity.[27] International human rights authorities have not strictly defined "serious crime."[28] But pursuant to the principle of legality, "serious crime" must be defined with sufficient clarity and precision so that the public can foresee the circumstances in which the government may hack. Moreover, given the privacy and security risks posed by government hacking, the definition of serious crime in this context should be particularly narrow.
  - "National security" can be particular prone to overly broad interpretations by the government.[29] The U.N. Siracusa Principles on

[26] Principle 5, Necessary and Proportionate Principles. Privacy International helped coordinate the drafting process for the Necessary and Proportionate Principles. The language "high degree of probability" emerged during that process as an attempt to bridge the "probable cause" standard in the United States with the "reasonable suspicion" standard common in other jurisdictions.

[27] See, e.g., Article 8(2), ECHR ("There shall be no interference by a public authority with the exercise of his right except such as is . . . necessary in a democratic society in the interests of national security, . . . for the prevention of disorder or crime . . . ."); U.N. Human Rights Committee, Concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland, U.N. Doc. CCPR/C/GBR/CO/7, 17 Aug. 2015, para. 24 ("The State Party Should . . . ensur[e] that access to communications data is limited to the extent strictly necessary for prosecution of the most serious crimes . . . .").

[28] See, e.g., Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Concern over the Acquisition and Implementation of Surveillance Programs by States of the Hemisphere, Press Release R80/15, 21 July 2015 ("[A]ccording to international standards, the use of programs or systems for the surveillance of private communications . . . must be strictly limited to the needs to meet compelling objectives such as the investigation of serious crime as defined in legislation.") (emphasis added).

[29] See, e.g., Zakharov, supra, at para. 248 ("It is significant that [the law governing interception of communications] does not give any indication of the circumstances under which an individual's

the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights ("Siracusa Principles") provides guidance on the proper scope of "national security": "National security may be invoked to justify measures limiting certain rights only when they are taken to protect the existence of the nation or its territorial integrity or political independence against force or threat of force." The Siracusa Principles further provide that national security "cannot be invoked as a reason for imposing limitations to prevent merely local or relatively isolated threats to law and order" or "as a pretext for imposing vague or arbitrary limitations."[30]

- In (4), this safeguard provides that government authorities must include information on the "method, extent and duration of the proposed hacking measure." Hacking comprises a range of ever-evolving techniques, many of which are technically complex. For judicial authorities to evaluate the necessity and proportionality of a proposed hacking measure, they must be able to assess whether what the government proposes to do at the technical level corresponds to its stated purpose in undertaking the hacking measure. The technical details related to the proposed hacking measure are therefore critical to the necessity and proportionality analysis.
- In (7), this safeguard provides that government authorities must include a security assessment "so as to enable an assessment of the proportionality of the proposed hacking measure against its security implications." As discussed in the legal commentary to the "Security and Integrity of Systems" safeguard, the exercise of the right to privacy is linked to the security of the devices, networks and services individuals rely on to communicate with each other. Thus, the security implications of a hacking measure are relevant to an assessment of the proportionality of the proposed interference with the right to privacy. In addition, as discussed in the implementation notes to the "Security and Integrity of Systems" safeguard, government hacking for surveillance poses novel and grave threats to security. These threats further demand that government authorities seeking to carry out a hacking measure – and judicial authorities determining whether to authorise such a measure – explicitly consider the security implications as part of the proportionality analysis. The requirement in (4), which provides that government authorities include information on the "method, extent and duration of the proposed hacking measure," buttresses the requirement in (7). These technical details facilitate the security assessment by requiring the government to explicitly indicate how it intends to interfere with a target system.

4. Judicial Authorisation

Prior to carrying out a hacking measure, government authorities must make an application, setting forth the necessity and proportionality of the proposed

communications may be intercepted on account of events or activities endangering . . . national, military, economic or ecological security. It leaves the authorities an almost unlimited degree of discretion in determining which events or acts constitute such a threat and whether that threat is serious enough to justify secret surveillance, thereby creating possibilities for abuse.").

[30] U.N. Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights, U.N. Doc. E/CN.4/1985/4, 1985, paras. 29-31.

measure to an impartial and independent judicial authority, who shall determine whether to approve such measure and oversee its implementation. The judicial authority must be able to consult persons with technical expertise in the relevant technologies, who may assist the judicial authority in understanding how the proposed measure will affect the target system and systems generally, as well as data on the target system and systems generally. The judicial authority must also be able to consult persons with expertise in privacy and human rights, who may assist the judicial authority in understanding how the proposed measure will interfere with the rights of the target person and other persons.

Legal Commentary

- International human rights law requires that any interference with the right to privacy "be attended by adequate procedural safeguards to protect against abuse." These safeguards "generally include independent prior authorization and/or subsequent independent review." In particular, when it comes to "targeted surveillance programmes . . . [j]udicial involvement that meets international standards is an important safeguard." [31] The U.N. Human Rights Committee has recently extended this safeguard to the hacking context, observing that States undertaking "hacking of digital devices" should "provid[e] for judicial involvement in the authorization of such measures in all cases."[32]
    - The ECtHR has indicated that prior independent authorisation – preferably judicial – is a minimum safeguard to protect the right to privacy, particularly in the surveillance context. It has noted that "[i]n a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure."[33] It has further held that judges require access to

[31] 2014 Report of the U.N. Special Rapporteur on Counter Terrorism, supra, at paras. 45-46; see also U.N. Human Rights Committee, Concluding Observations on the Fifth Periodic Report of France, U.N. Doc. CCPR/C/FRA/CO/5, 17 Aug. 2015, para. 12 ("[The State Party] should also ensure the effectiveness and independence of a monitoring system for surveillance activities, in particular by making provision for the judiciary to take part in the authorization and monitoring of surveillance measures."); U.N. Human Rights Committee, Seventh Periodic Report of the United Kingdom, supra, at para. 24 ("The State Party should . . . [e]nsure that robust oversight systems over surveillance, interception and intelligence-sharing of personal communications activities are in place, including by providing for judicial involvement in the authorization of such measures in all cases . . . ."); U.N. Human Rights Committee, Concluding Observations on the Sixth Periodic Report of Canada, U.N. Doc CCPR/C/CAN/CO/6, 13 Aug. 2015, para. 10 ("The State Party should . . . [p]rovide for judicial involvement in the authorization of surveillance measures . . . ."); OHCHR Report on the Right to Privacy in the Digital Age, supra, at para. 38 ("Judicial involvement that meets international standards relating to independence, impartiality and transparency can help to make it more likely that the overall statutory regime will meet the minimum standards that international human rights law requires."); 2013 Report of the U.N. Special Rapporteur on Freedom of Expression, supra, at para. 81 ("Legislation must stipulate that State surveillance of communications must only occur under the most exceptional circumstances and exclusively under the supervision of an independent judicial authority.").

[32] U.N. Human Rights Committee, Concluding Observations on the Sixth Periodic Report of Italy, U.N. Doc. CCPR/C/ITA/CO/6, 28 Mar. 2017, para. 37.

[33] Zakharov, supra, at para. 233 (citing Klass and Others v. Germany, European Court of Human Rights, App. No. 5029/71, 6 Sept. 1978, paras. 55-56); see also Szabó, supra, at para. 77 ("[I]n this field, control by an independent body, normally a judge with special expertise, should be the rule and substitute solutions the exception, warranting close scrutiny.").

the "relevant information" necessary for them to adequately assess the request for surveillance.[34]

- The IACtHR has held that the right to privacy, enshrined in Article 11 ACHR, gives way "when there is a well-substantiated search warrant issued by a competent judicial authority, spelling out the reasons for the measure being adopted and specifying the place to be searched and the objects that will be seized."[35]
- The IACHR Special Rapporteur for Freedom of Expression has observed that "decisions to undertake surveillance activities that invade the privacy of individuals must be authorized by independent judicial authorities, who must state why the measure is appropriate for the accomplishment of the objectives pursued in the specific case; whether it is sufficiently restricted so as not to infringe upon the right in question more than necessary; and whether it is proportionate in relation to the interests pursued."[36]

Implementation Notes

- This safeguard provides that the judicial authority "must be able to consult persons with technical expertise in the relevant technologies" as well as "persons with expertise in privacy and human rights." The U.N. High Commissioner for Human Rights has recognised that prior judicial authorisation "should not be viewed as a panacea" and that "in several countries, judicial warranting or review of the digital surveillance activities of intelligence and/or law enforcement agencies have amounted effectively to an exercise in rubber-stamping." The Commissioner has noted therefore "[t]he utility of independent advice, monitoring and/or review to help to ensure strict scrutiny of measures imposed under a statutory surveillance regime."[37]
  - The first category of "independent advice" is technical expertise. As discussed in the implementation notes for the "Necessity and Proportionality" safeguard, hacking comprises a range of ever-evolving techniques, many of which are technically complex. Moreover, for judicial authorities to evaluate the necessity and proportionality of a proposed hacking measure, they must be able to assess whether what the government proposes to do at the technical level corresponds to its stated purpose in undertaking the hacking measure. And yet, judicial authorities cannot be expected to understand the technical aspects of a proposed hacking measure without recourse to technical expertise. Access to technical expertise is therefore critical for judicial authorities to sufficiently consider the necessity and proportionality of a particular hacking measure.

[34] Zakharov, supra, at para. 261 (observing that the State's "judicial scrutiny" was "limited in scope" because "materials containing information about . . . the organisation and tactics of operational-search measures may not be submitted to the judge and are therefore excluded from the court's scope of review" and that "the failure to disclose the relevant information to the courts deprives them of the power to assess whether there is a sufficient factual basis to suspect the person in respect of whom operational-search measures are requested . . . .").

[35] Garcia v. Peru, Inter-American Commission of Human Rights, Case 11.006, Report No. 1/95, 17 Feb. 1995.

[36] IACHR Special Rapporteur for Freedom of Expression Report, supra, at para. 165.

[37] OHCHR Report on the Right to Privacy in the Digital Age, supra, at para. 38.

- The second category of "independent advice" is expertise in privacy and human rights. A dominant feature of judicial authorisation processes in the surveillance context is that they are ex parte. International human rights authorities have expressed concern that these processes fail to effectively represent the interests of the proposed targets of surveillance. Thus, the U.N. High Commissioner for Human Rights has, in lamenting judicial "rubber stamping," noted "particular interest in the creation of 'public interest advocacy' positions within surveillance authorization processes."[38] And the Council of Europe Commissioner for Human Rights has called on States to "[c]onsider the introduction of security-cleared public interest advocates into surveillance authorisation processes . . . to represent the would-be targets of surveillance."[39]

5. Integrity of Information

Government authorities must not add, alter or delete data on the target system, except to the extent technically necessary to carry out the authorised hacking measure. They must maintain an independently verifiable audit trail to record their hacking activities, including any necessary additions, alterations or deletions. Where government authorities rely on data obtained through an authorised hacking measure, they must disclose the method, extent and duration of the hacking measure and their audit trail so that the target person can understand the nature of the data obtained and investigate additions, alterations or deletions to information or breaches of the chain of custody, as appropriate.

Legal Commentary

- Where government authorities intend to use information obtained through surveillance in legal proceedings against a person, maintaining the integrity of that information is essential to ensuring its integrity – and later admissibility – as evidence.[40] It is therefore closely tied to the protection of the due process and fair trial rights of the person(s) subject to surveillance. Thus, the U.N. Special Rapporteur on the Freedom of Expression has noted that hacking, which "not only enable[s] a State to access devices, but also . . . to alter – inadvertently of purposefully – the information contained therein . . . threatens not only the right to privacy but also procedural fairness rights with respect to the use of such evidence in legal proceedings."[41]
- The U.N. Principles on the Effective Prevention and Investigation of Extra-legal, Arbitrary and Summary Executions ("Minnesota Protocol") provide one of the most detailed discussions on maintaining the integrity of evidence under international human rights law. The Protocol provides:

[38] Id.

[39] Commissioner for Human Rights, Council of Europe, Issue Paper on Democratic and Effective Oversight of National and Security Services, Commissioner's Recommendations, May 2015, para. 8 ("CoE Commissioner for Human Rights Issue Paper").

[40] See e.g., U.N. Office on Drugs and Crime, Current Practices in Electronic Surveillance in the Investigation of Serious and Organized Crime, 2009, pp. 21-25.

[41] 2013 Report of the U.N. Special Rapporteur on Freedom of Expression, supra, at para. 62.

> "Every stage of evidence recovery, storage, transportation and forensic analysis, from crime scene to court and through to the end of the judicial processes, should be effectively recorded to ensure its integrity as evidence. This is often referred to as the 'chain of evidence' or 'chain of custody'. Chain of custody is a legal, evidentiary concept requiring that any prospective item of evidence be conclusively documented in order to be eligible for admission as evidence in a legal proceeding. This includes the identity and sequence of all persons who possessed that item from the time of its acquisition by officials to its presentation in court. Any gaps in that chain of possession or custody can prevent the introduction of the item as evidence against a criminal defendant. Evidential material should be transported in a manner that protects it from manipulation, degradation and cross-contamination with other evidence. Each piece of evidence recovered . . . should be uniquely referenced and marked to ensure its identification from point of seizure to analysis and storage. To meet chain of evidence and integrity requirements, the transportation, tracking and storage of this evidence should include the investigator's details.
>
> Evidential material should be kept in an appropriate storage facility at all stages of the investigation. Storage facilities should be clean, secure, suitable for maintaining items in appropriate conditions, and protected against unauthorized entry and cross-contamination. Digital evidence should be collected, preserved and analysed in accordance with international best practice."[42]

Implementation Notes

- This safeguard prohibits government authorities from adding, altering or deleting data, "except to the extent technically necessary to carry out the authorised hacking measure." As discussed in the introduction to the safeguards, hacking permits the government to manipulate data on systems in a variety of ways, including by planting, corrupting or deleting data; sending data from the target system; or recovering data that has been deleted. At the same time, because hacking by definition involves interfering with a system, some manipulation of data may be technically necessary to carry out a proposed hacking measure.
- This safeguard requires government authorities to "maintain an independently verifiable audit trail to record their hacking activities." It remains open to debate whether an independently verifiable audit trail is technically feasible in the hacking context. Where governments have physical access to a target system, they typically preserve the integrity of digital evidence by creating a forensic image of the system and cryptographically hashing every file on the image.[43] Any alteration in the

[42] Office of the U.N. High Commissioner for Human Rights, The Minnesota Protocol on the Investigation of Potentially Unlawful Death: The Revised United Nations Manual on the Effective Prevention and Investigation of Extra-legal, Arbitrary and Summary Executions, 2016, paras. 65-66. The Protocol was revised in 2016 following a two-year process organized by the U.N. Special Rapporteur on Extrajudicial, Summary, or Arbitrary Executions and involving an international group of experts.

[43] A "hash" is a value returned by a "hash function," which takes an input of data of any size and creates an output value of a certain length. The hash is like a digital fingerprint of the data and hash functions are therefore used in cryptography to verify the integrity of a piece of data.

file will produce a different hash; hashes thus act to verify the integrity of each file. But hacking necessitates interference with a target system prior to any forensic imaging, making it difficult, perhaps impossible, to definitively prove that data on the target system is attributable to the actions of the target person as opposed to the government. The reliability of any forensic image is further undermined by the fact that data is constantly changing while a system is in use. Where governments choose, despite these technical realities, to authorise hacking operations, they must strive to record their hacking activities in as robust a manner as possible. This audit trail should include, *inter alia*, a detailed contemporaneous manual log of decisions and actions by authorised staff, computer activity logging, and screen captures of activity. All data related to the audit trail and data collected from the hacking measure must be stored securely and access must be limited to authorised staff.

- This safeguard further requires that when government authorities rely on data obtained through an authorised hacking measure, they must "disclose the method, extent and duration of the hacking measure" and the "audit trail." This information is necessary for the target person to independently evaluate whether the government's representations about the proposed hacking measure were complete and accurate when seeking authorisation to carry out the measure. It is also necessary for the target person to determine the extent of the government's interference with their system, including the data obtained from the system, and to verify the "chain of custody" (within the technical limitations described above). This information is therefore relevant to any defence by the target person in government proceedings against them that rely on data obtained through hacking.

6. Notification

Government authorities must notify the person(s) whose system(s) have been subject to interference pursuant to an authorised hacking measure, regardless of where the person(s) reside, that the authorities have interfered with such system(s). Government authorities must also notify affected software and hardware manufacturers and service providers, with details regarding the method, extent and duration of the hacking measure, including the specific configurations of the target system. Delay in notification is only justified where notification would seriously jeopardize the purpose for which the hacking measure was authorised or there is an imminent risk of danger to human life and authorisation to delay notification is granted by an impartial and independent judicial authority.

Legal Commentary

- International human rights authorities have recognised notification as an important procedural safeguard in protecting against abusive interference with the right to privacy.[44] This recognition is founded on the linkage

[44] 2013 Report of the U.N. Special Rapporteur on Freedom of Expression, supra, para. 82 ("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.").

between notification and access to "[e]ffective remedies for violations of privacy." Because "remedies must be known and accessible to anyone with an arguable claim that their rights have been violated . . . [n]otice (that either a general surveillance regime or specific surveillance measures are in place) . . . thus become[s a] critical issue[ ] in determining access to effective remedy."[45]

- The ECtHR has also tied notification "to the effectiveness of remedies before the courts and hence to the existence of effective safeguards against the abuse of monitoring powers." It has observed: "There is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively . . . ."[46] For that reason, the ECtHR has counselled that "as soon as notification can be made without jeopardising the purpose of the surveillance after its termination, information should be provided to the persons concerned."[47]
- The Council of Europe Human Rights Commissioner has also expressly supported for "a system of notification when a person has been the subject of surveillance."[48]

- The U.N. Special Rapporteur on Counter-Terrorism has observed that in some jurisdictions, "individuals must be notified when and how they are under surveillance, or as soon as possible after the fact" and that this right "must be ensured across borders by ensuring that legal regimes protect citizens and non-citizens alike."[49]
- The U.N. Human Rights Committee has recently extended the notification safeguard to the hacking context, observing that States undertaking "hacking of digital devices" should "afford[ ] 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."[50]

Implementation Notes

- This safeguard provides that government authorities must notify "person(s) whose system(s) have been subject to interference pursuant to an authorised hacking measure" that they "have interfered with

[45] OHCHR Report on the Right to Privacy in the Digital Age, supra, at para. 40.

[46] Zakharov, supra, at para. 234. The ECtHR did note an alternative to a notification requirement, whereby "any person who suspects that his or her communications are being or have been intercepted can apply to courts, so that the courts' jurisdiction does not depend on notification to the interception subject that there has been an interception of his communications." Id.

[47] Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, App. No. 62540/00, European Court of Human Rights, 28 June 2007, para. 90; see also Weber and Saravia, supra, at para. 135 ("The Court reiterates that the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies before the courts and hence to the existence of effective safeguards against the abuse of monitoring powers, since there is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively.").

[48] Commissioner for Human Rights, Council of Europe, Memorandum on Surveillance and Oversight Mechanisms in the United Kingdom, Comm DH(2016)20, May 2016, para. 25.

[49] 2009 Report of the U.N. Special Rapporteur on Counter Terrorism, supra, at para. 55.

[50] U.N. Human Rights Committee, Sixth Periodic Report of Italy, supra, at para. 37.

such system(s)." A government hacking measure can affect not only the target system but also other systems in a number of ways. For example, as discussed in the implementation notes to the "Necessity and Proportionality" safeguard, the government's hacking measure(s) may proliferate to systems beyond the target system. In addition, as discussed in those implementation notes, modern systems permit multiple users; a hacking measure targeted at a particular system may nevertheless interfere with the right to privacy of multiple users. Thus, government authorities must provide notification to all person(s) whose system(s) have been subject to interference pursuant to an authorised hacking measure.

    - Notification should include, *inter alia*, the date of entry and duration of the authorised hacking measure; whether data was or was not obtained pursuant to the measure; and whether irrelevant or immaterial data was obtained pursuant to the measure and the date of destruction of such data (pursuant to the "Destruction and Return of Data" safeguard).

- This safeguard also provides that government authorities must notify "person(s) whose system(s) have been subject to interference pursuant to an authorised hacking measure, regardless of where the person(s) reside." As discussed in the implementation notes to the "Necessity and Proportionality" safeguard, in certain circumstances, the government may lack information relating to the target system, which may include its location. Accordingly, government authorities might undertake a hacking measure in circumstances where the target system is located outside its jurisdiction. (Pursuant to the "Extraterritoriality" safeguard, government authorities must always comply with their international legal obligations when conducting an extraterritorial hacking measure.) In addition, a hacking measure deployed by government authorities may inadvertently proliferate to systems beyond the target system. That proliferation may interfere with system(s) outside of the jurisdiction of the government deploying the hacking measure. In these circumstances, government authorities must provide notification to the person(s) whose system(s) have been subject to interference, notwithstanding their location (unless otherwise provided for in the relevant legal mechanism relied upon for hacking extraterritorially).
- This safeguard further provides that government authorities must notify affected companies "with details regarding the method, extent and duration of the hacking measure, including the specific configurations of the target system." As discussed in the implementation notes to the "Security and Integrity of Systems" safeguard, government hacking measures may pose significant risks to the security of devices, networks and services, which are, by and large, designed, manufactured and sold by companies. Notifying affected companies of a hacking measure targeting its system(s) – and providing information regarding that measure, including the specific configurations of those system(s) – permits those companies to address the security implications of that measure. Companies may respond by protecting or mitigating against those risks, which may affect a large number of its users, many of whom may not be the target of the government's hacking measure.

7. Destruction and Return of Data

Government authorities must immediately destroy any irrelevant or immaterial data that is obtained pursuant to an authorised hacking measure. That destruction must be recorded in the independently verifiable audit trail of hacking activities. After government authorities have used data obtained through an authorised hacking measure for the purpose for which authorisation was given, they must return this data to the target person and destroy any other copies of the data.

Legal Commentary

The ECtHR has explicitly noted that the existence of a mechanism for the "destruction of personal data as soon as they [a]re no longer needed to achieve their statutory purpose, and for the verification at regular, fairly short intervals of whether the conditions for such destruction [a]re met" can "constitute[ ] an important element in reducing the effects of the interference with the secrecy of telecommunications to an unavoidable minimum."[51] The Court has also "deplore[d] the lack of a requirement to destroy immediately any data that are not relevant to the purpose for which they have been obtained."[52]

8. Oversight and Transparency

Government authorities must be transparent about the scope and use of their hacking powers and activities, and subject those powers and activities to independent oversight. They should regularly publish, at a minimum, information on the number of applications to authorise hacking approved and rejected; the identity of the applying government authorities; the offences specified in the applications; and the method, extent and duration of authorised hacking measures, including the specific configurations of target systems.

Legal Commentary: Oversight

- International human rights law requires that any interference with the right to privacy "be attended by adequate procedural safeguards to protect against abuse." These safeguards "generally include independent prior authorization and/or subsequent independent review."[53] The U.N. General Assembly has therefore called on States "[t]o establish or maintain existing

51 Weber & Saravia, supra, at para. 132; see also, Kennedy v. the United Kingdom, European Court of Human Rights, App. No. 26839/05, 18 May 2010, paras. 162, 164; see also Principle 13, Necessary & Proportionate Principles ("States should also enact laws providing that, after material obtained through Communications Surveillance has been used for the purpose for which information was given, the material must not be retained, but instead be destroyed or returned to those affected.").

52 Zakharov, supra, at para. 255.

53 2014 Report of the U.N. Special Rapporteur on Counter Terrorism, supra, at para. 45; see also U.N. Human Rights Committee, Seventh Periodic Report of the United Kingdom, supra, at para. 24 (recommending the State Party "[e]nsure that robust oversight systems over surveillance, interception and intelligence-sharing of personal communications activities are in place, including by . . . considering the establishment of strong and independent oversight mandates with a view to preventing abuses"); U.N. Human Rights Committee, Sixth Periodic Report of Canada, supra, at para. 10 (expressing concern "about the lack of adequate and effective oversight mechanisms to review activities of security and intelligence agencies and the lack of resources and power of existing mechanisms to monitor such activities" and recommending the State Party "[e]stablish oversight mechanisms over security and intelligence agencies that are effective and adequate and provide them appropriate powers as well as sufficient resources to carry out their mandate").

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."[54]

- The U.N. Special Rapporteur on Counter Terrorism has explained that "[s]urveillance systems require effective oversight to minimize harms and abuses." The Special Rapporteur noted that "[i]n many States, parliaments and independent bodies have been charged with conducting reviews of surveillance policies and procedures, and on occasion have been offered the opportunity for pre-legislative review . . . aided by the use of sunset and review clauses in legislation." The Special Rapporteur recommended that "[s]trong independent oversight mandates . . . be established to review policies and practices, in order to ensure that there is strong oversight of the use of intrusive surveillance techniques and the processing of personal information." The Special Rapporteur condemned "secret surveillance system[s] . . . not under the review of an effective oversight body."[55]
- The U.N. High Commissioner for Human Rights has noted "[t]he utility of independent advice, monitoring and/or review to help ensure strict scrutiny of measures imposed under a statutory surveillance regime has been highlighted positively in relevant jurisprudence." The High Commissioner also observed that "Parliamentary committees . . . can play an important role" although "they may also lack the independence, resources or willingness to discover abuse, and may be subject to regulatory capture." The High Commissioner further noted that "[j]urisprudence at the regional level has emphasized the utility of an entirely independent oversight body, particularly to monitor the execution of approved surveillance measures."[56]
    - The ECtHR has condemned a "system of secret surveillance" where no official "is required to regularly report to an independent body or to the general public on the overall operation of the system or on the measures applied in individual cases."[57] The Court has further condemned regimes that do not set out in law "the manner in which [oversight mechanisms] may supervise" surveillance, such as through "publicly available regulations or instructions describing the scope of their review, the conditions under which it may be carried out, the procedures for reviewing the surveillance measures or for remedying the breaches detected." With respect to the independence requirement, the Court takes "into account the manner of appointment and the legal status of the members of the supervisory body" and has previously found "sufficiently independent the bodies composed of members of parliament of both the majority and the opposition, or of persons qualified to hold judicial office, appointed either by parliament or by

[54] 2016 U.N. General Assembly Resolution on the Right to Privacy in the Digital Age, supra, at para. 5(d); see also U.N. General Assembly Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/RES/69/166, 18 Dec. 2014, para. 4 ("2014 U.N. General Assembly Resolution on the Right to Privacy in the Digital Age"); 2013 Report of the U.N. Special Rapporteur on Freedom of Expression, supra, at para. 93 ("States should establish independent oversight mechanisms capable to ensure transparency and accountability of State surveillance mechanisms.").

[55] 2009 Report of the U.N. Special Rapporteur on Counter Terrorism, supra, at paras. 51, 56, 62.

[56] OHCHR Report on the Right to Privacy in the Digital Age, supra, at para. 38.

[57] Ekimdzhiev, supra, at paras. 87-88.

the Prime Minister." With respect to the "powers and competences" of the supervisory body, the Court has noted that "it is essential that the supervisory body has access to all relevant documents, including closed materials and that all those involved in interception activities have a duty to disclose to it any material it requires."[58]

- The Council of Europe Commissioner for Human Rights has also recommended that states "[e]stablish or designate one or more bodies that are fully independent from the executive and the security services to oversee all aspects of security service regulations, policies, operations and administration." In particular, the Commissioner emphasised that "where security services engage in [hacking], these activities are subject to the same level of external oversight as is required for surveillance measures that have equivalent human rights implications."[59]
- The European Commission for Democracy through Law has observed that "[t]wo very significant stages in the signals intelligence process where safeguards must apply are the authorization and follow-up (oversight) processes" and noted that "the latter must be performed by an independent, external body is clear from the ECtHR's case law."[60]

Legal Commentary: Transparency

- The U.N. General Assembly has recognised that one of the purposes of oversight is to "ensur[e] transparency, as appropriate . . . for State surveillance of communications, their interception and the collection of personal data."[61]
- The U.N. Special Rapporteur on Counter Terrorism has observed that "[t]he principle of transparency and integrity requires openness and communication about surveillance practices." The Special Rapporteur also noted that "[o]pen debate and scrutiny is essential to understanding the advantages and limitations of surveillance techniques, so that the public may develop an understanding of the necessity and lawfulness of surveillance."[62]
- The U.N. Special Rapporteur on Freedom of Expression has indicated that "States should be completely transparent about the use and scope of communications surveillance techniques and powers" by publishing "at minimum, aggregate information on the number of requests approved and rejected, a disaggregation of the requests by service provider and by

58 Zakharov, supra, at paras. 276, 278, 281.

59 CoE Commissioner for Human Rights Issue Paper, supra, at paras. 1, 7.

60 European Commission for Democracy through Law (Venice Commission), Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Agencies, Study No. 719/2013 CDLAD(2015)006, 7 Apr. 2015, para. 20.

61 2016 U.N. General Assembly Resolution on the Right to Privacy in the Digital Age, supra, at para. 5(d); see also 2014 U.N. General Assembly Resolution on the Right to Privacy in the Digital Age, supra, at para. 4.

62 2009 Report of the U.N. Special Rapporteur on Counter Terrorism, supra, at paras. 54-56; see also Escher et al. v. Brazil, Inter-American Court of Human Rights, Judgment (on Preliminary Objections, Merits, Reparations, and Costs), Concurring Opinion of Judge Sergio García Ramírez, Series C No. 200, 6 July 2009, para. 6 ("We reject the furtiveness with which the tyrant hides his intolerable arbitrariness. We condemn the secrecy that shrouds the symbols of authoritarianism. We censure opacity in the exercise of public authority. We demand – and we are achieving, step by step, based on the argument of human rights – transparency in the acts of Government and in the conduct of those who govern us.").

investigation and purpose." The Special Rapporteur further indicated that "States should provide individuals with sufficient information to enable them to fully comprehend the scope, nature, and application of the laws permitting communications surveillance."[63]

- The IACHR Special Rapporteur for Freedom of Expression has indicated that in the surveillance context, "[t]he principle of 'maximum disclosure' is applicable . . . and indeed governs all State acts: they are public and can only be kept secret from the public under the strictest circumstances, provided that this confidentiality is established by law, seeks to fulfil a legitimate aim under the American Convention, and is necessary in a democratic society." The Special Rapporteur proceeded to recommend that "States should disclose general information on the number of requests for interception and surveillance that have been approved and rejected, and should include as much information as possible, such as – for example – a breakdown of requests by service provider, type of investigation, time period covered by the investigations, etc."[64]

Implementation Notes

- This safeguard provides that government authorities must subject their hacking powers and activities to independent oversight. Independent oversight can take many forms. However, the U.N. Special Rapporteur on Counter Terrorism has recommended, in the intelligence context, that "[a]n effective system of . . . oversight includes at least one civilian institution that is independent of both the intelligence services and the executive." In terms of the coverage of the oversight mechanisms, the Special Rapporteur observed that they should consider "all aspects of the work of intelligence services, including their compliance with the law; the effectiveness and efficiency of their activities; their finances; and their administrative practices." The Special Rapporteur further recommended that oversight mechanisms should "have the power, resources and expertise to initiate and conduct their own investigations, as well as full and unhindered access to the information, officials and installations necessary to fulfil their mandates," and should "receive the full cooperation of intelligence services and law enforcement authorities in hearing witnesses, as well as obtaining documentation and other evidence."[65] In addition, the Special Rapporteur further indicated that oversight mechanisms should "publish (annual) reports describing [their] activities and findings" and "as appropriate, incidental reports describing specific investigations."[66] Finally, for the reasons explained in the implementation notes to the "Judicial Authorisation" safeguard, oversight mechanisms must be able to consult persons with technical expertise in the relevant technologies as well as persons with expertise in privacy and human rights.

[63] 2013 Report of the U.N. Special Rapporteur on Freedom of Expression, supra, at paras. 91-92.

[64] IACHR Special Rapporteur for Freedom of Expression Report, supra, at paras. 166, 168.

[65] U.N. Human Rights Council, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight, U.N. Doc. A/HRC/14/46, 17 May 2010, Practices 6-7.

[66] Hans Born and Aidan Wills eds., Geneva Centre for the Democratic Control of Armed Forces, Overseeing Intelligence Services: A Toolkit, 2012, p. 84.

- This safeguard further provides that government authorities should publish certain information, at a minimum, related to their applications for authorisation of hacking measures. Government authorities should also consider publishing additional information that will enable the public to assess, as fully as possible, the privacy and security implications of their hacking operations. This information might include, for example, the number of systems beyond the target system affected by authorised hacking measures and the damage caused to those system(s) and/or data.

9. Extraterritoriality

When conducting an extraterritorial hacking measure, government authorities must always comply with their international legal obligations, including the principles of sovereignty and non-intervention, which express limitations on the exercise of extraterritorial jurisdiction. Government authorities must not use hacking to circumvent other legal mechanisms – such as mutual legal assistance treaties or other consent-based mechanisms – for obtaining data located outside their territory. These mechanisms must be clearly documented, publicly available, and subject to guarantees of procedural and substantive fairness.

Legal Commentary

- Under international human rights law, a state's human rights obligations extend to all individuals subject to its jurisdiction.[67] Those obligations therefore extend "to anyone within the power or effective control of that State . . . , even if not situated within the territory of the State . . . ."[68] In the surveillance context, the Office of the U.N. High Commissioner for Human Rights has explained that a state's human rights obligations may be engaged "if that surveillance involves the State's exercise of power or effective control in relation to digital communications infrastructure, wherever found, for example through direct tapping or penetration of that interference."[69] The U.N. Human Rights Committee has also indicated that a state's human rights obligations are engaged when it undertakes "surveillance activities within and outside its territory"[70] and that "measures should be taken to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity, regardless of the nationality or location of the individuals whose

[67] Art. 2(1), ICCPR ("Each State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant . . . ."); Art. 1(1) ACHR ("The States Parties to this Convention undertake to respect the rights and freedoms recognized herein and to ensure to all persons subject to their jurisdiction the free and full exercise of those rights and freedoms . . . .); Art. 1, ECHR ("The High Contracting Parties shall secure to everyone within their jurisdiction the rights and freedoms defined in Section I of this Convention.).

[68] U.N. Human Rights Committee, General Comment No. 31, supra, at para. 10.

[69] OHCHR Report on the Right to Privacy in the Digital Age, supra, at para. 34; see also 2014 Report of the U.N. Special Rapporteur on Counter Terrorism, supra, at para. 41 ("Even where states penetrate infrastructure located wholly outside their territorial jurisdiction the relevant authorities nevertheless remain bound by the State's obligations under the Covenant [on Civil and Political Rights].").

[70] U.N. Human Rights Committee, Concluding Observations on the Fifth Periodic Report of France, U.N. Doc. CCPR/C/FRA/CO/5, 17 Aug. 2015, para. 12.

communications are under direct surveillance."[71]

- International law also subjects a state to limitations on its authority to exercise extraterritorial jurisdiction.[72] Jurisdiction refers to "the authority of states to prescribe their law, to subject persons and things to adjudication in their courts . . . and to enforce their law."[73] Jurisdiction is inextricably linked to the principles of sovereignty and territoriality: "Jurisdiction is an aspect of sovereignty, it is coextensive with and, indeed, incidental to, but also limited by, the State's sovereignty. . . . '[I]t is an essential attribute of the sovereignty of this realm, as of all sovereign independent States, that it should possess jurisdiction over all persons and things within its territorial limits and in all cases, civil and criminal, arising within these limits.' If a State assumed jurisdiction outside the limits of its sovereignty, it would come into conflict with other States which need not suffer any encroachment upon their own sovereignty . . . . Such a system . . . divides the world into compartments within each of which a sovereign State has jurisdiction."[74]
- The scope of a state's extraterritorial jurisdictional competence depends on the type of jurisdiction exercised by the state. A state can exercise three types of jurisdiction: (1) prescriptive ("*i.e.* to make its law applicable to the activities, relations, or status of persons, or the interests of persons in things"), (2) adjudicative ("i.e. to subject persons or things to the process of its courts"), or (3) enforcement ("i.e. to induce or compel compliance . . . with its laws or regulations").[75]
- Enforcement jurisdiction is generally constrained by territory.[76] Thus, "a state cannot investigate a crime, arrest a suspect, or enforce its judgment or judicial processes in another state's territory without the latter state's permission."[77] This jurisdictional constraint – *i.e.* the requirement of consent

[71] U.N. Human Rights Committee, Seventh Periodic Report of the United Kingdom, supra, at para. 24; see also U.N. Human Rights Committee, Concluding Observations of the Fourth Periodic Report of the United States of America, U.N. Doc. CCPR/C/USA/CO/4, 23 Apr. 2014, para. 22.

[72] See American Law Institute, Restatement (Third) of Foreign Relations Law in the United States, 1987, §401.

[73] See id. at pt. IV, Introductory Note; see also Lassa Oppenheim, Oppenheim's International Law, Robert Jennings & Arthur Watts eds., 9th ed., 1992, p. 456; The Draft Convention on Research in International Law of the Harvard Law School, 29 American Journal of International Law 435, 467-69 (Supp. 1935).

[74] Frederick A. Mann, The Doctrine of Jurisdiction in International Law, 1964, p. 30. The principle of sovereignty – and therefore jurisdiction – is also "closely linked with the principle[ ] of . . . non-intervention," which "involves the right of every sovereign State to conduct its affairs without outside interference." Military and Paramilitary Activities in and against Nicaragua (Nicar. v. US), 1986 ICJ 14, para. 202 (27 June); see also Oppenheim, supra, at p. 428 (stating that the principle of nonintervention "is the corollary of every state's right to sovereignty, territorial integrity and political independence.")

[75] American Law Institute, Restatement (Third), supra, at §401; see also id. at cmt. a ("The limitations on a state's authority to subject foreign interests or activities to its laws differ from those that govern the state's jurisdiction to adjudicate, and [from] the limitations on a state's authority to enforce its law . . . .")

[76] See 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").

[77] International Bar Association, Report of the Task Force on Extraterritorial Jurisdiction, 2009, pp. 9-10 (citing S.S. Lotus, supra, at p. 18; Arrest Warrant of 11 April 2000 (Dem. Rep. Congo v. Belg.) 2002 I.C.J. 3, paras. 4, 49, 54); see also American Law Institute, Restatement (Third), supra, at §433(1)(a) ("A state's law enforcement officers may exercise their functions in the territory of another state only with the consent of the other state, given by duly authorized officials of that state.").

– is rooted in the principle of sovereignty, for any unilateral exercise of enforcement jurisdiction on another state's territory would violate that state's sovereignty by usurping its sovereign powers.[78]

- The territorial constraints on the exercise of enforcement jurisdiction apply to the hacking of devices located abroad. As a general matter, the principle of "State sovereignty and international norms and principles that flow from sovereignty apply to the conduct by States of [information and communications technology ("ICT")]-related activities and to their jurisdiction over ICT infrastructure within their territory."[79]
    - This principle is reflected in the Council of Europe's Convention on Cybercrime, which is an international treaty designed to articulate "a common criminal policy aimed at the protection of society through cybercrime."[80] The Convention drafters came to "the common understanding . . . that investigative activity of law enforcement authorities of a State Party in international communication networks or in computer systems located in the territory of another state may amount to a violation of territorial sovereignty of the state concerned, and therefore cannot be undertaken without prior consent of" that state.[81] Article 32 of the Convention reflects this understanding by permitting "trans-border access to stored computer data" only "with consent or where publicly available."[82]

Implementation Notes

- This safeguard provides that government authorities "must not use hacking to circumvent other legal mechanisms – such as mutual legal assistance treaties or other consent-based mechanisms – for obtaining data located outside their territory." States traditionally rely on consent-based mechanisms when exercising extraterritorial enforcement jurisdiction. The principal mechanism is a Mutual Legal Assistance Treaty ("MLAT"), a bilateral agreement containing procedures for obtaining and providing assistance in criminal matters. The U.N. Special Rapporteur on Freedom of Expression has observed that "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."[83] States must however refrain from circumventing the MLAT process and instead

[78] See S.S. Lotus, supra, at p. 18; Ian Brownlie, Principles of Public International Law, 8th ed., 2012, pp. 478-79; Michael Akehurst, Jurisdiction in International Law, 46 British Yearbook of International Law 145, 145-151 (1975).

[79] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, delivered to the General Assembly, U.N. Doc. A/70/174, 22 July 2015, ¶25; see also id. at para. 26(b) ("In their use of ICTs, States must observe, among other principles of international law, State sovereignty, sovereign equality . . . and non-intervention in the internal affairs of other States. Existing obligations under international law are applicable to State use of ICTs.").

[80] Council on Europe, Convention on Cybercrime pmbl., opened for signature 23 Nov. 2001, 2296 U.N.T.S. 167 (entered into force 1 July 2004).

[81] Henrik W.K. Kaspersen, Council of Europe, Cybercrime and Internet Jurisdiction, 2009, p. 26.

[82] Convention on Cybercrime, supra, at art. 32. An example where "data is not meant to be available" would be "if a law enforcement agency hacks into a suspected criminal's computer located in another State." In those circumstances, "it is exercising enforcement jurisdiction in that State and the activity requires the latter State's consent . . . ." Michael N. Schmitt, ed., Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2017, Rule 11, para. 14.

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

consider reforms to adapt the process to the digital age. Those reforms must be compliant with international law, including by ensuring international human rights standards govern any government surveillance activities undertaken extraterritorially.

- This safeguard applies to any hacking measure that has extraterritorial effect, including measures that intentionally interfere with a target system located extraterritorially, as well as measures that unintentionally interfere with systems located extraterritorially. A number of technologies operate to cloak the location of users when using the internet. In some cases, the technology deliberately protects the privacy of the user, for example, enabling journalists to communicate with vulnerable sources. In other instances, the technology masks the user as a by-product of its core service, such as securing communications. For example, many individuals and businesses rely on VPNs – which establish encrypted connections between the user's device and a trusted server that then appears as the source of any network activity – to send and receive sensitive data, such as financial or medical information or even for ordinary internet usage when connecting to potentially insecure networks, such as a public Wi-Fi hotspot. Government authorities who cannot determine the location of a target of a hacking measure should operate under the presumption that the target is located extraterritorially. The alternative – *i.e.* to presume that targets whose location are unknown are territorially located – risks disrupting the principle of sovereignty and violating the attendant prohibition on the unilateral exercise of extraterritorial enforcement jurisdiction. That disruption could, in turn, catalyse or escalate foreign relations conflict between states.

10. Effective Remedy

Persons who have been subject to unlawful government hacking, regardless of where they reside, must have access to an effective remedy.

Legal Commentary

- International human rights law provides that states have an obligation to ensure an "effective remedy" for individuals whose rights they have violated.[84] This obligation extends to "individuals whose right to privacy has

[84] See Universal Declaration of Human Rights, U.N. General Assembly Resolution 217 (III) A, 10 Dec. 1948. art. 8 ("Everyone has the right to an effective remedy by the competent national tribunals for acts violating the fundamental rights granted him by the constitution or by law"); Art. 2(3), ICCPR ("Each State Party to the present Covenant undertakes: (a) To ensure that any person whose rights or freedoms as herein recognized are violated shall have an effective remedy, notwithstanding that the violation has been committed by persons acting in an official capacity; (b) To ensure that any person claiming such a remedy shall have his right thereto determined by competent judicial, administrative or legislative authorities, or by any other competent authority provided for by the legal system of the State, and to develop the possibilities of judicial remedy; (c) To ensure that the competent authorities shall enforce such remedies when granted."); Art. 25, ACHR ("1. Everyone has the right to simple and prompt recourse, or any other effective recourse, to a competent court or tribunal for protection against acts that violate his fundamental rights recognized by the constitution or laws of the state concerned or by this Convention, even though such violation may have been committed by persons acting in the course of their official duties; 2. The State Parties undertake: (a) to ensure that any person claiming such remedy shall have his rights determined by the competent authorities provided for by the legal system of the state; (b) to develop the possibilities of judicial remedy; and (c) to ensure that

been violated by unlawful or arbitrary surveillance."[85]

- The U.N. High Commissioner for Human Rights has observed that "[e]ffective remedies for violations of privacy through digital surveillance can . . . come in a variety of judicial, legislative or administrative forms." However, the High Commissioner noted that effective remedies "typically share certain characteristics": "First, those remedies must be known and accessible to anyone with an arguable claim that their rights have been violated. Notice (that either a general surveillance regime or specific surveillance measures are in place) and standing (to challenge such measures) thus become critical issues in determining access to effective remedy. . . Second, effective remedies will involve prompt, thorough and impartial investigation of alleged violations. This may be provided through the provision of an 'independent oversight body [. . .] governed by sufficient due process guarantees and judicial oversight, within the limitations permissible in a democratic society.' Third, 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."[86]
    - For a remedy to be effective, it must not only end ongoing violations, but also "counteract or make good any human rights harms that have occurred." The form that such remedy can take may include "apologies, restitution, rehabilitation, financial or non-financial compensation and punitive sanctions (whether criminal or administrative, such as fines), as well as the prevention of harm through, for example, injunctions or guarantees of non-repetition."[87]
- The U.N. Special Rapporteur on Counter Terrorism has similarly recommended: "[I]ndividuals should have the right to seek an effective

the competent authorities shall enforce such remedies when granted"); Article 13, ECHR ("Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity.").

85 2014 U.N. General Assembly Resolution on the Right to Privacy in the Digital Age, supra, at para. 4(e); U.N. Human Rights Committee, Concluding Observations on the Third Periodic Report of the Former Yugoslav Republic of Macedonia, U.N. Doc. CCPR/C/MKD/CO/3, 17 Aug. 2015, para. 23 ("[The State Party should] ensure that persons who are unlawfully monitored are systematically informed thereof and have access to adequate remedies."); U.N. Human Rights Committee, Seventh Periodic Report of the United Kingdom, supra, at para. 24 ("The State Party Should: . . . (e) Ensure that persons affected have access to effective remedies in cases of abuse.").

86 OHCHR Report on the Right to Privacy in the Digital Age, supra, at paras. 40-41 (citing U.N. and IACHR Special Rapporteurs on Freedom of Expression, Joint Declaration, supra; Segersted-Wiber and others v. Sweden, European Court of Human Rights, App. No. 62332/00, 6 June 2006; U.N. Human Rights Committee, General Comment No. 31, supra; U.N. Special Rapporteur on Counter-Terrorism, Compilation of Good Practices, supra; U.N. General Assembly Resolution on Basic Principles and Guidelines on the Right to a Remedy and Reparation for Victims of Gross Violations of International Human Rights Law and Serious Violations of International Humanitarian Law, U.N. Doc. No. A/RES/60/147, 16 Dec. 2005).

87 OHCHR, Guiding Principles on Business and Human Rights, supra, at p. 27. While these Principles address business-related human rights abuses, they are "grounded in recognition of . . . States' existing obligations to respect, protect and fulfil human rights and fundamental freedoms." Id. at 1; see also Chorzów Factory Case (Germany v. Poland), 1927 P.C.I.J. (Ser. A) No. 9, p. 21; International Law Commission, Draft Articles on the Responsibility of States for Intentionally Wrongful Acts, U.N. Doc. A/56/10, 2001, arts. 31, 34 and accompanying text.

remedy for any alleged violation of their online privacy rights. This requires a means by which affected individuals can submit a complaint to an independent mechanism that is capable of conducting a thorough and impartial review, with access to all relevant material and attended by adequate due process guarantees. Accountability mechanisms can take a variety of forms, but must have the power to order a binding remedy. States should not impose standing requirements that undermine the right to an effective remedy."[88]

- The U.N. Special Rapporteur on Freedom of Expression has emphasized the relationship between notification and access to an effective remedy: "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."[89]
    - The ECtHR has also recognised the relationship between notification and access to an effective remedy, noting that it will bear the factors of "the absence of notification and the lack of an effective possibility to request and obtain information about interceptions from the authorities . . . in mind when assessing the effectiveness of remedies available under [national] law." The Court concluded, in this circumstance, that the absence of both meant that the State Party did "not provide for effective remedies to a person who suspects that he or she has been subjected to secret surveillance." And "[b]y depriving the subject of [surveillance] of the effective possibility of challenging [surveillance] retrospectively," the Court found that the State Party had "eschew[ed] an important safeguard against the improper use of secret surveillance measures."[90]

Implementation Notes

This safeguard provides that those subject to unlawful government hacking must have access to an effective remedy "regardless of where they reside." As discussed in the implementation notes to the "Notification" safeguard, there are circumstances where a hacking measure may interfere with systems outside of the jurisdiction of the government deploying the measure. In these circumstances, all those subject to unlawful government hacking must have access to an effective remedy, notwithstanding their location.

88 2014 Report of the U.N. Special Rapporteur on Counter Terrorism, supra, at para. 61.

89 2013 Report of the U.N. Special Rapporteur on Freedom of Expression, supra, at para. 82.

90 Zakharov, supra, at paras. 291, 298; see also Szabó, supra, at para. 86 ("[T]he Court has held that the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies and hence to the existence of effective safeguards against the abuse of monitoring powers, since there is in principle little scope for any recourse by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their justification retrospectively. As soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, information should be provided to the persons concerned.").

Privacy International
62 Britton Street, London EC1M 5UY
United Kingdom

Phone +44 (0)20 3422 4321
www.privacyinternational.org
Twitter @privacyint

UK Registered Charity No. 1147471