

- **Pay No Attention to That Man Behind the Curtain: Exposing and Challenging Government Hacking for Surveillance**
 -
-

Contents

Introduction	02
Government Hacking for Surveillance: 10 Necessary Safeguards	03
Q&A	04
Hacking Safeguards In Context	10
Argentina	10
Uganda	11
Chile	13
Colombia	16
Mexico	18
Ethiopia	20
Conclusion	22

Introduction

Privacy and security are both essential to protecting individuals, including their autonomy and dignity.

Undermining privacy undermines the security of individuals, their devices and the broader infrastructure. People need privacy to freely secure themselves, their information, and fully enjoy other rights.

In turn, the systems that constitute our modern infrastructure, whether commercial or governmental, must be secure and aid in securing privacy. Ensuring that our devices, networks and services are secure is a constant challenge. Security requires multiple actors – particularly security researchers, industry and the government – to commit significant resources and cooperate with each other. Technological systems must support and enhance privacy, not undermine it. Laws or practices must not compel individuals or organisations to undermine their security or the security they provide to the users who place their trust in them.

Unfortunately, commitment to security is lacking across the world. Instead, poorly drafted cyber security and cyber crime laws focus on monitoring and criminalising online behaviour and increasing state surveillance powers rather than addressing the root problems of insecure systems. Too often there is a lack of threat modelling and assessment done by organisations prior to the development and deployment of systems. There is too little attention paid to how all systems contain vulnerabilities and that good security ethos is about identifying as many and ensuring equitable disclosure and patching. This lack of attention to root security problems is particularly worrying in relation to critical infrastructure. These gaps leave countries, and in turn, people's data, vulnerable to attacks and data breaches, and governments unprepared to respond to them. The results of this environment that we are building may be catastrophic for privacy and security and results in a loss in trust and stifled innovation.¹

In Privacy International's experience of challenging government surveillance, we have observed that governments tend to presume that insecurity is acceptable if it enables their surveillance goals. This is unacceptable. Governments around the world have argued for undermining encryption, demanded companies build mechanisms to permit government circumvention of existing protections, and even asked for the removal altogether of certain security mechanisms. These demands leave the security of devices, networks, and services at risk. They are the opposite of cyber security. A growing number of governments around the world are also embracing hacking to facilitate their surveillance activities. When governments hack for surveillance

¹ See Privacy International and partner work on cyber security here: <https://www.privacyinternational.org/topics/cyber-security>

purposes, they again seek to prioritise insecurity, undermining the security we so desperately need.

Because government hacking for surveillance purposes entails unique and extensive interferences with privacy and other fundamental rights and poses significant risks to the security of devices and networks, Privacy International questions whether it can ever be a legitimate component of state surveillance. Even where governments hack in connection with legitimate surveillance 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.

Government Hacking for Surveillance: 10 Necessary Safeguards

Privacy International has produced a set of 10 Hacking Safeguards,² designed to help interested parties assess government hacking in light of applicable international human rights law as well as the security implications of this surveillance practice. We must prioritise the security of systems and data. We hope that our Hacking Safeguards will help spur public debate about the scope and nature of government hacking powers and their privacy and security implications.

As part of a series published by Privacy International,³ the purpose of this briefing is to highlight examples of government hacking for surveillance that we, our partner organisations, and others have investigated in Argentina, Chile, Colombia, Ethiopia, Mexico and Uganda and analyse them alongside the Hacking Safeguards. These examples put into context a complicated issue and demonstrate how far governments are from what is required under international human rights law with regards to their hacking activities. It also illustrates the challenge civil society has in highlighting the importance of defensive security to offensive minded governments. We also attempt to answer some frequently asked questions about hacking and its implications for security.

We encourage interested parties to share any examples of government hacking for surveillance with Privacy International, along with corresponding legislation, if any exists.

The Hacking 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.

² Privacy International, *Government Hacking and Surveillance: 10 Necessary Safeguards*, 2017 <https://privacyinternational.org/type-resource/hacking-necessary-safeguards>

³ See further publications at <https://privacyinternational.org/topics/cyber-security>

Q & A

What is hacking?

The term “hacking” is difficult to define. Hacking is essentially an attempt to understand a system better than it understands itself, and then nudging it to do what the hacker wants. For the Hacking 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.

Is all hacking bad?

No. Hacking often has negative associations in the public sphere, where it is often connected with cyber crime, such as the theft of money or personal information. But hacking can benefit security. Computer systems are complex, and almost with certainty, contain vulnerabilities. Hacking is essential to identifying vulnerabilities, testing them by developing exploits, and sharing these results, which is critical for improving security and incident response. Hacking can therefore help us improve and strengthen the systems that are essential to our lives, and increasingly as they govern our lives.

What capabilities do governments need to hack?

Surveillance is increasingly conducted in secret. Unsurprisingly, therefore, many governments shroud their hacking powers and capabilities in secrecy. Hacking is fundamentally about causing technologies to act in a manner the manufacturer, owner or user did not intend or foresee. In the surveillance context, it is a method for gaining access to a system and therefore to information about its users. Hacking can include interference with systems in the government’s physical custody as well as remote interference with systems.

A common feature of hacking is the exploitation of weaknesses in software and hardware, which may be used by millions of people.⁴ For example, governments may use such preexisting vulnerabilities to remotely install malware on a system, without the affirmative participation of the user. However, hacking may also involve taking advantage of people to interfere with their systems. ‘Phishing’, for example, is a common social engineering technique whereby an adversary impersonates a reputable person or organisation. Phishing attacks typically take the form of an email or text message, which may contain a link or attachment infected with malware. In both instances, the effects of installing malware may permit the government to conduct a number of different forms of surveillance. They may access all the data stored on the system; covertly turn on a device’s microphone, camera, and GPS-based locator technology; capture continuous screenshots of the hacked device or see anything input and/or output from that device, including login details and passwords, internet browsing histories, and documents and communications the user never intended to disseminate. Hacking also permits the manipulation of data on a system, such as deleting, adding, or corrupting data.

Governments can develop these capabilities ‘in house’ or they can purchase them ‘off the shelf’ from surveillance technology companies. The tools and methods we are aware of in Africa and Latin America mostly concern the latter. Leaked company documents have played a major role in bringing transparency to the issue, particularly companies selling spyware, a collective term for hacking capabilities which include remote access tools and malware.⁵

For many, the first time it was known that a government was in fact hacking for surveillance purposes was via leaked or found documents. Evidence of these tools and methods come from additional sources, such as documents obtained through the course of our own research and investigations, or through research and public reporting by journalists and other civil society organisations, including the partners in our International Network.⁶

During the 2011 Arab Spring in Egypt, activists recovered half shredded and burned archives from the abandoned headquarters of the Egyptian Security Service. Among these they found documents and contracts relating to the purchase of FinFisher, a hacking tool which allowed remote access to a target’s device, developed and sold by the UK company Gamma International.⁷ This discovery sparked multiple civil

4 For further background on hacking, please see Privacy International’s submission on the Equipment Interference Code of Practice, 20 March 2015. Available from: https://www.privacyinternational.org/sites/default/files/PI%20and%20ORG%20Submission%20-%20Draft%20Equipment%20Interference%20Code%2020%20Mar%202015_0.pdf

5 In 2016, Privacy International launched the Surveillance Industry Index, the world’s largest publicly available educational resource of data and documents of its kind on the surveillance industry, and an accompanying report charting the growth of the industry and its current reach <https://privacyinternational.org/blog/1236/privacy-international-launches-surveillance-industry-index-and-new-accompanying-report>

6 See information on Privacy International’s Network: <https://privacyinternational.org/partners>

7 Karen McVeigh, The Guardian, British firm offered spying software to Egyptian regime – documents, 28 April 2011 <https://www.theguardian.com/technology/2011/apr/28/egypt-spying-software-gamma-finfisher>

society investigations into Gamma International and other companies which were selling hacking capabilities to repressive regimes with a poor human rights record. In 2013, Privacy International filed a complaint with the OECD National Contact Points regarding the sale of spyware by UK company Gamma International and another surveillance company Trovicor,⁸ headquartered in Germany, to Bahraini government actors. These sales were revealed by documents published anonymously online.⁹ In 2014, leading civil society research organisation Citizen Lab published research into countries that had purchased FinFisher, and also found evidence of the spyware on laptops belonging to activists.

In 2015, the Italian spyware company Hacking Team's systems were hacked and a cache of contracts and emails published online. In the following months, civil society and journalists pored over the documents to discover which governments had purchased spyware, how much they had spent, and to glean clues of what it would be used for and who it would target. This led to a variety of actions and consequences we outline in this paper, which also led to the development of the Hacking Safeguards.

What's the problem? The government is hacking to catch bad guys, right?

The examples we and others have collected demonstrate hacking is often not used to facilitate legitimate surveillance activities. States with terrible human rights records known to have purchased hacking capabilities have been proven to target human rights defenders, journalists, political opponents, protesters and dissidents, including those in exile outside the country. In Uganda, the explicit aim of the hacking operation codenamed "Fungua Macho" was to crush a protest movement objecting to rising prices.¹⁰ In Mexico, hacking powers were used to spy on public health advocates involved in a high profile "soda tax" campaign working to combat obesity.¹¹ In Colombia, the military used hacking to spy on those involved in peace negotiations with FARC, placing the whole process in jeopardy.¹²

Even where governments use hacking to facilitate legitimate surveillance activities, its privacy and security implications means governments may never be able to demonstrate that hacking as a form of surveillance is compatible with international human rights law. Where governments seek to authorise hacking powers within that context, they must both engage in a robust public debate about their necessity and

8 Privacy International et al vs. Gamma International, 1 February 2013 https://www.oecdwatch.org/cases/Case_286

9 Adriana Edmeades, Open Democracy, How Bahrain Spies on British Soil, 4 November 2014 <https://www.opendemocracy.net/opensecurity/adriana-edmeades/how-bahrain-spies-on-british-soil>

10 Musaaazi Namit, Aljazeera Uganda walk-to-work protests kick up dust, 18 April 2011 <http://www.aljazeera.com/indepth/features/2011/04/201142831330647345.html>

11 Azam Ahmed and Nicole Perlroth, Using Texts as Lures, Government Spyware Targets Mexican Journalists and Their Families, 19 June 2017 <https://www.nytimes.com/2017/06/19/world/americas/mexico-spyware-anticrime.html>

12 Associated Press in Bogota, The Guardian, Army cyberspies monitored Colombian peace negotiators, magazine reports, 4 February 2014 <https://www.theguardian.com/world/2014/feb/04/colombia-farc-peace-talk-negotiators-spied-on-magazine-reports>

proportionality and further assess those powers against the Hacking Safeguards.

What are the concerns about hacking from a privacy perspective?

As discussed above, hacking permits governments remote access to systems and therefore potentially to all the data stored on those systems. 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. Moreover, hacking permits governments to conduct novel forms of real-time surveillance, such as covertly turning on a device's microphone, camera, or GPS-based locator technology. Finally, hacking permits governments to manipulate data in a variety of ways.

The privacy intrusions of hacking are enormously amplified should a government interfere with communications networks and their underlying infrastructure. A single hack can affect many people, including those who are incidental or unrelated to a government investigation or operation. But 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. For example, GCHQ, the UK's signals intelligence agency, hacked Belgacom, Belgium's largest telecommunications provider, in 2013.¹³ Hacking directed at networks could be for conducting surveillance against specific individuals, groups or countries, or across numerous jurisdictions.

What are the concerns about hacking 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 seeks vulnerabilities not to secure systems through testing and coordinated disclosure, but to exploit them to facilitate a surveillance objective. This activity has the potential to undermine the security not only of targeted systems but also of other unrelated systems. As we rely increasingly on the internet and connect more and more of our physical world to it, this risk increases.

The right to privacy does not feature in my country's constitution/laws. Do the Hacking Safeguards still apply?

Yes. Even if privacy is not explicitly protected in domestic laws, most States have signed up to international or regional obligations that do protect privacy. This could

13 Ryan Gallagher, The Intercept, How U.K. spies hacked a European ally and got away with it, 17 February 2018 <https://theintercept.com/2018/02/17/gchq-belgacom-investigation-europe-hack/>

be through the UN International Covenant on Civil and Political Rights (ICCPR), or regional instruments such as the American Convention on Human Rights, the Arab Charter on Human Rights or the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms.

Where will I find laws governing hacking in my country?

Very few countries have explicitly legislated for government hacking for surveillance purposes and those that have are largely concentrated in Europe. An extensive analysis on the use and legality of Hacking Team software by governments in Latin America by Derechos Digitales, one of Privacy International's partners in Chile, found its use to be largely without legal basis in the whole region.¹⁴

In some instances, governments have interpreted existing surveillance legislation to authorise hacking. But government hacking powers, if they are to be authorised, must be subject to a regulatory framework tailored to its unique privacy and security implications, which the Hacking 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. In other instances, legal provisions addressing government hacking are hard to find, scattered in other legislative instruments, such as a criminal code or cyber security law. In those instances, they may be worded so mysteriously that they are hard to interpret. Indeed, governments rarely use the word 'hacking' to describe their hacking powers. In the US, for example, the government has described hacking as "network investigative techniques" and "computer network exploitation", among other terms. And in the UK, for instance, the government's power to hack is referred to as "equipment interference".

My government says that hacking is legislated for as part of the existing communications surveillance legal framework. Is this OK?

No. As discussed above, it is not acceptable to use existing legislation governing surveillance to justify hacking powers. As hacking for surveillance purposes results in novel and grave implications for both privacy and security, it is not clear that it is compatible with international human rights law. If governments insist on authorising hacking for surveillance, they must enact a regulatory framework with safeguards designed to address its unique implications. This is one of the central themes of the Hacking Safeguards, and is explored in depth in this briefing.

What are Privacy International's Hacking Safeguards? Why are they needed?

A growing number of governments around the world are embracing hacking to

¹⁴ Lorenzo Franceschi-Bicchierai, Motherboard, Hacking Team's 'Illegal' Latin American Empire, 18 April 2016 https://motherboard.vice.com/en_us/article/gv5v8q/hacking-team-illegal-latin-american-empire

facilitate their surveillance activities. And yet, many deploy this capability in secret and without a clear basis in law.

The Hacking Safeguards were adapted, in part, from The International Principles on the Application of Human Rights to Communications Surveillance (also known as the “Necessary and Proportionate Principles” or “13 Principles”) launched in 2013. A joint initiative from civil society, industry and technology experts, the 13 Principles were developed to demonstrate how existing human rights law applied to new methods of digital surveillance of individuals.¹⁵ Over 400 organisations, experts and Parliamentary groups signed on to support the 13 Principles, as well as 300,000 individuals globally.¹⁶

The 13 Principles described how modern communications surveillance activities must be subject to safeguards and oversight, which are established under international human rights law. While the 13 Principles serve as a useful framework for approaching government hacking powers, the novel privacy and security implications of those powers required a further adaptation of the principles established under international human rights law. Nevertheless, like the 13 Principles, the Hacking Safeguards emphasise the core principles of legality, necessity and proportionality of any government powers that interfere with the right to privacy.

For the purposes of the briefing, Privacy International focuses predominantly on the first safeguard, which addresses the legality of government hacking powers. As outlined in each of the examples below, governments are hacking in secret and without a clear legal basis. In the first instance, the legality requirement ensures that there exists a public debate on the very need for these powers. Where governments subsequently establish a legal basis for those powers, that basis further ensures that the purpose and scope of those powers are clear and accessible to the public. Where relevant, Privacy International also discusses the relevance of the other Hacking Safeguards to specific examples. In particular, the examples below reveal the necessity that governments carry out an assessment of how hacking for surveillance may affect the security and integrity of systems and data, as part of any necessity and proportionate analysis.

The ten safeguards explore:¹⁷

1. Legality
2. Security and Integrity of Systems
3. Necessity and Proportionality
4. Judicial Authorisation
5. Integrity of Information
6. Notification
7. Destruction and Return of Data
8. Oversight and Transparency
9. Extraterritoriality
10. Effective Remedy

¹⁵ <https://necessaryandproportionate.org/principles>

¹⁶ <https://necessaryandproportionate.org/sign>

¹⁷ Privacy International, Government Hacking and Surveillance: 10 Necessary Safeguards, 2017
<https://privacyinternational.org/type-resource/hacking-necessary-safeguards>

Hacking Safeguards In Context

Argentina

Emails leaked from Hacking Team in July 2015 contained exchanges with Argentine companies that claimed to have ties with state agencies, but a transaction could not be proved from these emails. However, political figures such as deceased prosecutor Alberto Nisman and journalist Jorge Lanata were known to have been targeted with spyware in 2014. In December 2015, Citizen Lab documented an extensive malware, phishing, and disinformation campaign that was likely state sponsored in several Latin American countries, including Argentina.¹⁸

There is discussion as to whether the amendments proposed in 2016 to Argentina's Criminal Procedure Code broaden government surveillance powers to include hacking.¹⁹ The amendments presented for open consultation included the introduction of special methods of investigation, including remote surveillance of computer equipment, and surveillance through image capturing, localisation, and monitoring. The proponents of the bill argued that the techniques are justified by the need to react appropriately and flexibly to the difficult task of combatting transnational criminal activity.

Critics said the bill failed to provide a definition of hacking, merely referring to the use of "software which enables or facilitates remote access," as well as the lack of necessary information as to the relevant authority responsible for carrying out such activities.²⁰ In the end, the bill was not passed, however several of its provisions ended up being addressed in individual laws, except the chapter on electronic surveillance.

In April 2018, two Senators introduced a new bill to incorporate to the Criminal Procedural Code all the provisions that were passed in previous years in separate laws, but the bill also introduced once again provisions on electronic surveillance, such as a remote access to devices, the use of location tracking, and eavesdropping techniques, to name the most concerning; unlike the other provisions, the chapter on surveillance was never enshrined by any law. ADC, a civil society organisation in Argentina, raised concerns about the lack of a comprehensive and public debate on the matters addressed, since the introduction of government hacking and other

18 Freedom House, Argentina Freedom on the Net, 2017 <https://freedomhouse.org/report/freedom-net/2017/argentina> ; Citizen Lab, Packrat Seven Years of a South American Threat Actor, 2015 <https://citizenlab.ca/2015/12/packrat-report/>

19 <https://www.justicia2020.gob.ar/noticias/proyecto-reforma-al-codigo-procesal-penal-federal-ingreso-al-senado-la-nacion/>

20 See, State of Privacy, Argentina, 2017 <https://privacyinternational.org/state-privacy/57/state-privacy-argentina> and Freedom House, Freedom on the Net 2017 <https://freedomhouse.org/report/freedom-net/2017/argentina>

surveillance techniques have clear consequences on people's right to privacy.²¹ When the bill was considered by the plenary of the Senate, several opposition senators brought up the lack of a robust debate around the incorporation of such surveillance techniques. Finally, the proponents of the bill introduced a modification to remove the whole chapter on surveillance and the bill was passed by the Senate without it. Nevertheless, the authors of the bill stated that they would pursue the incorporation of surveillance techniques in the near future,²² making modifications to the original text and introducing checks and balances.²³

By placing new hacking powers in the Criminal Procedure Code, those powers failed to meet the principle of legality as outlined in the first Hacking Safeguard as they are not "*explicitly*" prescribed in a framework "*tailored to hacking's unique privacy and security implications*". Moreover, due to the confusion surrounding the meaning and scope of the amendments, they are not "*sufficiently clear and precise to enable persons to foresee [their] application and the extent of the interference.*"²⁴

The first Hacking Safeguard requires that hacking powers, like other surveillance powers, have a clear legal basis. 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.*" Legality is also closely tied to the concept of "*arbitrary interference,*" the idea being that the exercise of a secret power carries the inherent risk of its arbitrary application.²⁵

Uganda

In 2015, Privacy International published an investigation, *For God and My President: State Surveillance in Uganda*,²⁶ exposing a secret government surveillance operation that targeted a domestic protest movement highlighting the spiraling cost of living. The surveillance operation was made possible by the government's purchase of FinFisher, intrusion malware developed and sold by the UK based company Gamma.²⁷ The operation itself was carried out in absence of a rigorous legal framework governing communications surveillance in general, and particularly without an explicit framework governing hacking.

21 ADC, #ReformaEspía: Nuevas técnicas de vigilancia para la investigación penal, 2018 <https://adcdigital.org.ar/wp-content/uploads/2018/04/AnalisisReformaEspiaCPPF.pdf>

22 Página 12, Una media sanción que excluyó la vigilancia electrónica, 2018 <https://www.pagina12.com.ar/110681-una-media-sancion-que-excluyo-la-vigilancia-electronica>

23 Página 12, La vigilancia y las escuchas tendrán un plazo de treinta días, 2018 <https://www.pagina12.com.ar/109876-la-vigilancia-y-las-escuchas-tendran-un-plazo-de-treinta-dia>

24 Hacking Safeguard 1: Legality <https://privacyinternational.org/safeguards/85/hacking-safeguard-1-legality>

25 See the legal commentary to the first hacking safeguard on legality <https://privacyinternational.org/advocacy-briefing/1057/hacking-safeguards-and-legal-commentary#1>

26 Privacy International, *For God and My President: State Surveillance In Uganda*, October 2015 https://privacyinternational.org/sites/default/files/2017-12/Uganda_Report_1.pdf

27 The Chieftaincy of Military Intelligence (CMI) purchased FinFisher surveillance malware in December 2011 from Gamma International GmbH (Germany), according to documents obtained by Privacy International. See also, Nick Hopkins and Jake Morris, BBC, UK firm's surveillance kit 'used to crush Uganda opposition', 15 October 2015 <http://www.bbc.co.uk/news/uk-34529237>

According to documents acquired by Privacy International, the explicit aim of the operation, codenamed Fungua Macho ('open your eyes' in Swahili), was to crush the Walk to Work²⁸ protest movement by obtaining personal information on the protesters that could be used to silence and blackmail them. The operation also aimed to spy on the Forum for Democratic Change (FDC) opposition party, media houses, parliamentarians and intelligence insiders by infecting personal communication devices with the intrusion malware.

The government denied these allegations and Privacy International duly responded laying out the evidence we had obtained, which amounted to pages of official and verified documents. At the time, we added:

*"Furthermore, The Regulation of Interception of Communications Act (2010) does not regulate the use of intrusion malware like FinFisher. Rather, the law only covers interception of communications, as conducted through Uganda's service provider networks. The use of FinFisher amounts to "hacking" an individual's device. The Fungua Macho operation—which appears to have been completed without any reference to judicial oversight or warrants—was thus not within the realm of law."*²⁹

Thus, to the extent that the Ugandan government has been hacking while relying on the powers contained in the Regulation of Interception of Communications Act, such activities would fail the principle of legality. That principle, as articulated in the first Hacking Safeguard requires that:

"government hacking powers must be explicitly prescribed by law and limited to those strictly and demonstrably necessary to achieve a legitimate aim."

As the Legal Commentary to this safeguard further explains:

"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."

In the 2016 Uganda Universal Periodic Review³⁰ submitted to the UN Human Rights Council, Privacy International recommended that the government:

28 Musaazi Namit, Aljazeera Uganda walk-to-work protests kick up dust, 18th April 2011 <http://www.aljazeera.com/indepth/features/2011/04/201142831330647345.html>

29 Privacy International, Ugandan Government Deployed FinFisher Spyware To 'Crush' Opposition, Track Elected Officials and Media In Secret Operation During Post-Election Protests, Documents Reveal, 15 October 2015 <https://privacyinternational.org/node/694>

30 Uganda Universal Periodic Review (2016) https://privacyinternational.org/sites/default/files/2017-12/uganda_upr2016.pdf

“Ensure that the Parliament conducts an inquiry into the use of intrusion software to assess their compliance with Uganda’s domestic and international human rights obligations and make publicly available any findings related to the above inquiry;”

And:

“Halt all procurement of intrusion malware and other hacking tools pending the results of the Parliamentary inquiry and ensure there are appropriate controls to prevent the use of private surveillance industry products to facilitate human rights abuses”

Unfortunately, neither recommendation was referenced in the government’s response and the law remains unchanged.

Chile

In 2015, the Hacking Team leaks revealed the Chilean government’s hacking capabilities. They revealed that the Investigations Police of Chile (PDI) had purchased two systems: “Galileo” and “Phantom”. The PDI initially denied the purchases, and stressed that prior judicial authorisation was required under Chilean law to conduct hacking for surveillance. But the purchases were later confirmed. According to analysis by Derechos Digitales,³¹:

“...in order to comply with the requirements of the Legality Principle [in the 13 Principles], it is necessary to comply with Article 9 of the Chilean Criminal Procedure Code which requires judicial authority for the interference of fundamental rights. However, the use of malware is not specifically authorised in the wording of the code, thus its legality is conditioned to what is sought with its use according to applicable regulations such as the Intelligence Act, the Terrorist Law, and the Drug Act. Government entities specifically stated that “Phantom” would be used only for the purpose of pursuing drug trafficking and organised crime.”

The analysis continues:

“The PDI defends its use of “Phantom” arguing a need to modernise its capabilities in order to “investigate organized crime, international terrorism, and drug trafficking on a large scale.” These justifications are written according to Law 19,974 on intelligence systems [Intelligence Act, 2004]. Article 24 provides “special procedures for collecting information” to sources that are closed to the public—they are exclusively limited to intelligence and counterintelligence activities that aim to safeguard national security and protect Chile and its people from terrorism, organized crime, and drug trafficking “and include” intervening on computer systems and networks (section III, paragraph b) and any other technological systems for transmission, storage or processing communications or information (section III, paragraph d). Since such operations are carried out by the police and under judicial authorisation, this form of computer system

31 Derechos Digitales, State Communications Surveillance and the Protection of Fundamental Rights in Chile, July 2016. See Section 2.2.3 Targeted Surveillance: Malware <https://necessaryandproportionate.org/country-reports/chile>

“intervention” (use of malware) would be carried out according to this law.”

Nevertheless, the PDI’s use of hacking for surveillance purposes still fails the principle of legality. Pursuant to that principle, as articulated in the Hacking Safeguards, government hacking powers must be *“explicitly prescribed by law”* and as outlined in the examples of Uganda and Argentina above, governments cannot simply interpret an existing framework, which authorises other surveillance activities, to authorise hacking. Therefore, invoking other laws such as the Criminal Procedure Code is insufficient.

In addition, using a prior law that was passed in order to investigate organised crime, international terrorism, and drug trafficking to authorise hacking means that the government was not required to assess the potential risks and damage to the security and integrity of the target system and data (or other systems and data), as outlined in Hacking Safeguard Two. This type of assessment is necessary for governments to meet the principles of necessity and proportionality when hacking, as outlined in Hacking Safeguard Three.

The Chilean government claimed that the use of hacking for surveillance was legitimate due to the need for prior judicial authorisation:

“The Control Committee of Intelligence of the House of Representatives cited both directors of the PDI and ANI asking them to explain the purchase of the software. While it is not possible to find records of that meeting, the President of the Committee Deputy Saffirio noted after the session, “with the explanation given [in the session], it is certain that strict controls exist within the PDI, which allows them to operate these systems (Phantom) with a prior judicial authorisation.”

While prior judicial authorisation is a necessary safeguard to authorise surveillance activities, including hacking, as outlined in Hacking Safeguard Four, it is not enough by itself to ensure hacking activities comply with international human rights law. Moreover, the judicial authorisation process itself will look different in the hacking context, requiring the judicial authority to assess the unique privacy and security implications of hacking. Hacking Safeguard Three: Necessity and Proportionality includes some of the unique pieces of information that an application for judicial authorisation to hack must include:

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

1. *A high degree of probability that:*
 - 1.1 *A serious crime or act(s) amounting to a specific, serious threat to national security has been or will be carried out;*
 - 1.2 *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;*
 - 1.3 *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.”*

In addition, the judicial authorisation process for hacking in Chile falls short in other ways. Judges, for example, do not have access to independent technical expertise to sufficiently consider the necessity and proportionality of a particular hacking measure. Moreover, Chile lacks an independent oversight mechanism. Therefore, the judicial authorisation process in Chile cannot be considered an adequate legal safeguard as required by international human rights law when any interference with the right to privacy occurs.

Nevertheless, a bizarre hacking controversy continues to unfold in Chile. In 2017, the Chilean uniformed police (Carabineros) conducted an operation called “Operación Huracán”, which resulted in the raid and detention of eight people under charges of rural violence and terrorism.³² This operation relied heavily on the interception of Whatsapp and Telegram conversations from the detained persons,³³ allegedly using hacking capabilities.

This operation was supposedly authorised pursuant to the Intelligence Act (2004), through a special warrant directly requested by the intelligence unit of the Carabineros. However, in October 2017 the Chilean Supreme Court ordered the release of these eight persons, ruling that the evidence failed to demonstrate their participation in the alleged crimes.³⁴

In January 2018, there was a dramatic plot twist in the story: New information emerged showing that the Carabineros Intelligence Unit never actually intercepted communications nor hacked any device for extractive surveillance purposes, and the

32 <http://www.biobiochile.cl/noticias/nacional/chile/2017/09/25/operacion-huracan-6-meses-de-diligencias-que-terminaron-con-8-detenidos-por-atentados.shtm>

33 <http://impresa.elmercurio.com/Pages/NewsDetail.aspx?dt=2017-09-26&dtB=26-09-2017%200:00:00&PaginaId=2&bodyid=3>

34 <http://www2.latercera.com/noticia/suprema-ordena-liberar-detenidos-operacion-huracan/>

judicial hacking order was used as a cover to plant evidence on the detainees' phones.³⁵

Nevertheless, the fact that the Carabineros claimed it did conduct a hacking operation indicates they believe themselves to have this power, even though they seemingly did not use it in this instance. The legal basis for these powers seems again to be the Intelligence Act, which we have already outlined above as insufficient to meet the principle of legality required under international human rights law and as set out in our Hacking Safeguards.

While still a developing story, as a product of this scandal, the Director General of Carabineros, the General in charge of the Intelligence unit and many other police officers have been denounced or fired, and the prosecution office is presenting charges against several officers for obstruction of justice.³⁶ But the people of Chile are due a public explanation of how this outrageous abuse of power happened, including the legal basis for the Intelligence Unit's hacking powers and what rules, if any, govern those powers. They are also due a public explanation of how the law will be amended to prevent such an abuse of power from happening again.

Colombia³⁷

Colombia's internal conflict began in the 1950s, impacting at least three generations of Colombians and making FARC the oldest guerrilla group in the world. The government's use of communications surveillance against FARC has been an integral part of the conflict, documented in a 2015 report by Privacy International.³⁸ It is known from the Hacking Team leaks that the Colombian police acquired the Remote Control System (RCS) called 'Galileo', spyware sold exclusively to governments by the company, as far back as 2012.³⁹ A 2014 investigation by Citizen Lab traced RCS back to Colombia and concluded that since 2012 it has been associated with attacks on journalists, activists and human rights defenders.⁴⁰ Around this time, a scandal involving government hacking shocked and galvanised Colombia's civil society and public. In early 2014, in the midst of peace talks taking place between the Colombian government and FARC, Semana Magazine uncovered⁴¹ a military hacking operation known as "Operación Andrómeda" targeted against the

35 <https://www.derechosdigitales.org/11890/la-mugre-y-la-furia-operacion-huracan-podria-haber-sido-un-montaje/>

36 <http://www.emol.com/noticias/Nacional/2018/03/22/899703/Fiscalia-formalizara-a-generales-r-Gonzalo-Blu-y-Teuber-por-caso-Huracan.html>

37 Further readings: <https://www.theguardian.com/world/2014/feb/04/colombia-farc-peace-talk-negotiators-spied-on-magazine-reports>, <https://karisma.org.co/risks-of-an-uncontrolled-state-surveillance-in-colombia/> US State Department, Colombia 2014 Human Rights Report <https://www.state.gov/documents/organization/236888.pdf>

38 Privacy International, Shadow State: Surveillance, Law and Order in Colombia, August 2015 https://privacyinternational.org/sites/default/files/2017-12/ShadowState_English.pdf

39 Privacy International, Fundación Karisma and Dejusticia. State of Privacy: Colombia, January 2018 <https://privacyinternational.org/state-privacy/58/state-privacy-colombia>

40 The Citizen Lab, 'Mapping Hacking Team's "Untraceable Spyware"', 17 February 2014. <https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware/>

41 Semana, ¿Alguien espío a los negociadores de La Habana? 2nd March 2014 <http://www.semana.com/nacion/articulo/alguien-espio-los-negociadores-de-la-habana/376076-3>

government negotiators of the peace talks and several other figures.⁴² Based on that information, the prosecution office presented charges against several military officers involved in these activities in early 2018.⁴³

The scandal involved not only hacking to obtain information about the negotiation of the peace talks, but also hacking against other undisclosed targets and the selling of classified information. Despite the criminal charges, the Colombian Ministry of Defense claims that the operation was conducted in accordance with the law, but with some security protocol flaws.⁴⁴ This indicates that the government, i.e. the Ministry of Defense, had approved surveillance against its own negotiators.

Concerns over the inadequacy of Colombia's surveillance framework, including with respect to government hacking, has been well documented by Privacy International and partners in recent years. As we wrote in 2017's submission to Colombia's Universal Periodic Review at the UN:

"According with article 269A of the Colombian criminal code, "hacking" ("Abusive access to an information system") is a criminal offense, and therefore, in the absence of any law explicitly regulating its use for surveillance purposes, it is a form of extra-legal surveillance that is illegal under Colombian law".⁴⁵

Because there is no law explicitly regulating the use of hacking for surveillance practices in Colombia, it is unclear how the Colombian Ministry of Defense can claim that its hacking operation was conducted in accordance with the law. In any event, Privacy International emphasises that even if such a legal framework were to exist, the Colombian government appears to have hacked the negotiators for reasons prohibited under international human rights law, which asserts:

"the muzzling of any advocacy of multi-party democracy, democratic tenets and human rights' is never a legitimate objective; in fact it undermines public engagement and debate in a matter that runs counter to the letter of Article 19 [ICCPR] and the object and purposes of the Covenant."⁴⁶

42 <https://www.theguardian.com/world/2014/feb/04/colombia-farc-peace-talk-negotiators-spied-on-magazine-reports>

43 <http://www.eltiempo.com/justicia/investigacion/pliego-de-cargos-a-militares-de-operacion-andromeda-167540> One of the involved hackers that was charged, Andrés Sepúlveda, is particularly famous and was profiled in Bloomberg in 2006 <https://www.bloomberg.com/features/2016-how-to-hack-an-election/>

44 <http://www.eltiempo.com/archivo/documento/CMS-15141236>

45 Stakeholder Report Universal Periodic Review 30th Session – Colombia, The Right to Privacy in Colombia. Submitted by Dejusticia, Fundación Karisma and Privacy International, September 2017 https://privacyinternational.org/sites/default/files/2018-03/UPR_The%20Right%20to%20Privacy%20in%20Colombia_2017.pdf

46 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.,

46 No. 16-7081, p. 15 (1 Nov. 2016), available at https://www EFF.org/files/2016/11/01/11.1.16_unitednations_human_rights_experts_amicus_brief.pdf (citing General Comment No. 34, supra, at 35) [hereinafter Brief of U.N. Human Rights Experts]. 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.

The Colombian government therefore cannot justify hacking activities as pursuant to a legitimate objective where they target those involved in a peace process aimed to bring about the end of a decades-long conflict.

Mexico

In 2015, it was discovered that the Mexican government was also a client of Hacking Team.⁴⁶ In February 2017, an investigation by the Citizen Lab⁴⁸ revealed that spyware from Israeli firm NSO group was used in an operation targeting Mexican government food scientists and two public health advocates involved in a high profile “soda tax” campaign working to combat obesity. A journalist investigating official corruption, Rafael Cabrera, had also been targeted with the spyware.⁴⁹ Further details about targets were revealed by the Citizen Lab⁵⁰ and Mexican civil society group R3D,⁵¹ along with SocialTIC and Article 19 Mexico in June 2017. These included lawyers investigating the mass disappearance of students, an academic working against corruption, two influential journalists and an American representing victims of sexual abuse by the police.⁵²

In the first instance, these people could not be considered legitimate targets of surveillance. Therefore, the Mexican government hacking clearly falls foul of international human rights law.

Privacy International and R3D published a full analysis in 2017⁵³ and noted there does not appear to be a proper legal basis for the Mexican government to hack, even for legitimate surveillance purposes.

In June 2017, Privacy International and R3D wrote to the President of Mexico asking him to bring transparency to the issue and clarify the legal basis for hacking

47 See, Mexico State of Privacy, 2017 <https://www.privacyinternational.org/state-privacy/1006/state-privacy-mexico> Among the technologies purchased was Hacking Team’s Remote Control System “Da Vinci” product and other malware used to spy social networks and mail services including Facebook, Twitter and Gmail.

48 Citizen Lab, Bitter Sweet. Supporters of Mexico’s Soda Tax Targeted With NSO Exploit Links, 11 February 2017 <https://citizenlab.org/2017/02/bittersweet-nso-mexico-spyware/>

49 Nicole Perlroth, New York Times, iPhone Users Urged to Update Software After Security Flaws Are Found, 25 August, 2016 <https://www.nytimes.com/2016/08/26/technology/apple-software-vulnerability-ios-patch.html>

50 Citizen Lab, Reckless Redux: Senior Mexican Legislators and Politicians Targeted With NSO Spyware, 29 June 2019 <https://citizenlab.org/2017/06/more-mexican-nso-targets/>

51 R3D, #GobiernoEspia: vigilancia sistemática a periodistas y defensores de derechos humanos en México, 19 June 2017 <https://r3d.mx/2017/06/19/gobierno-espia/>

52 Azam Ahmed and Nicole Perlroth, Using Texts as Lures, Government Spyware Targets Mexican Journalists and Their Families, 19 June 2017 <https://www.nytimes.com/2017/06/19/world/americas/mexico-spyware-anticrime.html>

53 Privacy International briefing, International Human Rights Implications of Reported Mexican Government Hacking Targeting Journalists and Human Rights Defenders, 28 June 2017 <https://privacyinternational.org/sites/default/files/2017-12/Briefing%20on%20the%20International%20Human%20Rights%20Implications%20of%20Reported%20Mexican%20Government%20Hacking%20Targeting%20Journalists%20and%20Human%20Rights%20Defenders.pdf>

activities. The letter also asked the Attorney General's office to investigate the scope of hacking activities and the targeting of journalists, human rights defenders and activists with spyware.⁵⁴

In December 2017, the UN and IACHR Special Rapporteurs on Freedom of Expression jointly called on the Mexican government to establish an independent investigation into the use of the spyware, and to establish a legal framework to protect individuals from arbitrary and clandestine interference in their privacy.⁵⁵

To date, the government has failed to inform the public under which conditions these techniques would be used, for what purposes, by which entity and the legal basis of their deployment.

Privacy International and R3D's further analysis focused on the existing surveillance framework, and found it was *"unclear whether these activities even conform to the procedures and safeguards set forth in the Mexican surveillance framework."*⁵⁶ As we have learned from previous examples, justifying hacking for surveillance through existing surveillance frameworks is not compliant with international human rights law, as it violates the principle of legality.

In 2017, the Mexican Secretariat of the Interior (SEGOB) responded to our June letter, saying they had organised meetings to set out some action points in response to the various reports and analyses. Pursuant to international human rights law, government authorities must subject their surveillance powers and activities to *independent* oversight. An oversight body housed in the Ministry of the Interior would not be independent. Hacking Safeguard Eight addresses 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."

There have been efforts from other bodies to conduct oversight over the Mexican government. The INAI (National Institute of Transparency, Access to Information and Personal Data), began an investigation and in October 2017, ordered the government to turn over the contracts showing the acquisition of hacking capabilities. However, the government has been blocking and delaying these efforts.

54 <https://www.privacyinternational.org/sites/default/files/2017-12/PI-R3D%20Joint%20Letter.pdf>

55 Observaciones preliminares del Relator Especial de la ONU sobre la libertad de expresion y el Relator Especial sobre libertad de expresion de la CIDH después de su visita conjunta en México, 27 de noviembre- 4 de diciembre 2017

56 Privacy International briefing, International Human Rights Implications of Reported Mexican Government Hacking Targeting Journalists and Human Rights Defenders, 28 June 2017, P12 http://hchr.org.mx/images/doc_pub/ES-final-version-preliminary-observations.pdf

Ethiopia

The government of Ethiopia has a long history of purchasing spyware, and deploying it against civil society, both in Ethiopia and outside the country. Citizen Lab has published five sets of evidences since 2013 linking the government of Ethiopia to misuse of spyware against civil society actors. Targets were based in Canada, USA, Europe and elsewhere,⁵⁷ which demonstrates both the extraterritorial reach of commercial spyware and the circumvention of legal mechanisms, a clear contravention of international legal obligations.

In 2014 Tadesse Kersmo, an Ethiopian activist exiled in the UK, became concerned that his laptop may have been infected with malware after reading reports from Citizen Lab about the politically motivated spying conducted by the government of Ethiopia. Tadesse approached Privacy International and together with researchers from Citizen Lab, his laptop was examined. The laptop was infected with FinSpy⁵⁸ intrusion software and had been active in June 2012, after he arrived in the UK.⁵⁹

Domestically, Ethiopia's surveillance regime is broad and vague. A 2014 Human Rights Watch report into surveillance in Ethiopia found that: *"authorities face very few barriers in law and practice in use of surveillance powers, given the lack of privacy safeguards and independent oversight to prevent abuse. Unlike traditional forms of surveillance, the remote nature of these tactics also allows the government to extend these harms far beyond its borders."*⁶⁰

While Ethiopia fails on every level in the adequacy of its surveillance regime, and there is much to say about that in the Hacking Safeguards, due to the extraordinary cases of extraterritorial hacking, this section focuses on the extraterritorial implications of Ethiopia's hacking. As articulated in Hacking Safeguard 10:

"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

57 Citizen Lab, Commercial Spyware, The Multibillion Dollar Industry Built on an Ethical and Legal Quagmire, 6 December 2017 <https://citizenlab.ca/2017/12/legal-overview-ethiopian-dissidents-targeted-spyware/>; Citizen Lab, Champing at the Cyberbit: Ethiopian Dissidents Targeted with New Commercial Spyware, 6 December 2017 <https://citizenlab.ca/2017/12/champing-cyberbit-ethiopian-dissidents-targeted-commercial-spyware/>

58 Once downloaded onto a target's computer, FinSpy allows the operator of the Trojan to have total access to the computer. This means that it was possible to read Tadesse's email correspondence, even when encrypted, search the documents on his computer, monitor his web surfing, listen in on Skype calls he had with other members of Ginbot 7's executive committee, follow chat conversations, and even to remotely switch on the computer's webcam and microphone to extend surveillance beyond the computer to what was happening around it in the privacy of Tadesse's home.

59 Privacy International, Surveillance follows Ethiopian political refugee to the UK, 16 February 2014 <https://privacyinternational.org/blog/1199/surveillance-follows-ethiopian-political-refugee-uk>

60 Human Rights Watch (2014) They Know Everything We Do: Telecom and Internet Surveillance in Ethiopia <https://www.hrw.org/report/2014/03/25/they-know-everything-we-do/telecom-and-internet-surveillance-ethiopia>

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.”

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. This safeguard applies to hacking measures with extraterritorial effect, including measures that intentionally interfere with a target system located extraterritorially. Accordingly, Ron Deibert, Director of Citizen Lab, wrote in the wake of the latest publication of evidence:

“If a government wants to collect evidence on a person in another country, it is customary for it to make a formal legal request to other governments through a process like the Mutual Legal Assistance Treaties. Ethiopia appears to have sidestepped all of that. International norms would suggest a formal démarche to Ethiopia from the governments whose citizens it monitored without permission, but that may happen quietly if at all.”

In 2014, a legal challenge in the USA was brought by the Electronic Frontier Foundation (EFF) on behalf of an American citizen born in Ethiopia, known as Kidane, whose laptop was also infected with FinSpy. The allegation was that the Ethiopian government violated the US Wiretap Act. The court dismissed the case in 2016, which, as Deibert explains, *“establish[ed] a troubling precedent.”*

All this adds up to a lack of access to an effective remedy, as required under international human rights law and articulated in Hacking Safeguard 10: *“Persons who have been subject to unlawful government hacking, regardless of where they reside, must have access to an effective remedy.”*

The Legal commentary continues:

“...there are circumstances where a hacking measure may interfere with systems outside of the jurisdiction of the government deploying the measure. In those circumstances, all those subject to unlawful government hacking must have an effective remedy, notwithstanding their location.”

Conclusion

As many of the examples above demonstrate, states across Africa and Latin America are increasingly deploying hacking for surveillance purposes. It is unclear whether these activities can ever be compliant with international human rights law. Where governments nevertheless insist on deploying these powers, they must meet a series of minimum necessary safeguards as set out in international human rights law and that address the security implications of hacking.

The examples above further demonstrate that in most instances, governments have failed to articulate a clear basis in law for their hacking activities, as required by international human rights law. Applying our Hacking Safeguards means therefore that governments fall at the first hurdle by failing to meet the principle of legality. As stated at the outset, this is so important because at the heart of the principle of legality is the premise that placing “intrusive surveillance regimes on a statutory footing” subjects them to “public and parliamentary debate.” Legality is also closely tied to the concept of “arbitrary interference,” the idea being that the exercise of a secret power carries the inherent risk of its arbitrary application.⁶¹

Without a clear legal framework governing hacking, any hacking activities conducted by the government will violate international human rights law, notwithstanding the existence of other safeguards, such as prior judicial authorisation. Nevertheless, for illustrative purposes, we have also used the examples to discuss the application of additional principles enshrined in the Hacking Safeguards.

The briefing has demonstrated the difficulties in uncovering and challenging unlawful government hacking. The Hacking Safeguards are designed as a tool to assist civil society organisations: they provide a framework for challenges to focus on, and clear steps to hold governments to account. After these revelations, there has still been no official inquiries/judicial reviews or changes in the law in any of these countries. We hope the continued work of civil society organisations will change this status quo, and that the Hacking Safeguards will give stakeholders a tool to use in challenging hacking for government surveillance.

Privacy International is working to bring transparency to government hacking and to challenge its use through research, policy advocacy, and litigation. This entails:

- Understanding factually how governments hack; and
- Understanding legally how international human rights frameworks should apply to government hacking, exemplified by the Hacking Safeguards.

61 See the legal commentary to the first hacking safeguard on legality <https://privacyinternational.org/advocacy-briefing/1057/hacking-safeguards-and-legal-commentary#1>

We rely on our partners to report and investigate hacking, along with journalists and other civil society organisations. We also push governments for disclosure, often building on the research and investigations by others.

Other tools at our disposal are the use of freedom of information (FOI) requests and exerting pressure on oversight bodies. We're eager to partner with organisations in order to achieve this. We are happy to work together on FOI requests or to seek questions from oversight bodies. We are also happy to help organisations use and apply our safeguards within their jurisdictions

If you would like to work with us on this, get in touch by contacting PI Policy Officer Lucy Purdon (lucyp@privacyinternational.org) or PI Legal Officer Scarlet Kim (scarlet@privacyinternational.org).

**PRIVACY
INTERNATIONAL**

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