PRIVACY INTERNATIONAL

Intervention before the Federal Constitutional Court in the case 2 BvR 1850/18

September 2019

Table of Contents

SUMMARY 2

INTRODUCTION 3

I. THE USE OF STATE TROJANS CAN THREATEN THE ESSENCE OF THE RIGHTS TO PRIVACY AND DATA PROTECTION UNDER INTERNATIONAL AND EUROPEAN HUMAN RIGHTS LAW, IF NOT PROPERLY CONSTRAINED 5

II. THE USE OF STATE TROJANS VIOLATES STATES' OBLIGATIONS TO EFFECTIVELY GUARANTEE THE SECURITY AND INTEGRITY OF IT SYSTEMS 8

III. THE USE OF STATE TROJANS SHOULD NOT VIOLATE THE PRINCIPLES OF NECESSITY AND PROPORTIONALITY UNDER BOTH INTERNATIONAL AND EUROPEAN LAW12

A. STATE TROJANS MUST BE LIMITED TO WHAT IS STRICTLY NECESSARY FOR THE PURPOSES OF PROSECUTING CRIME 12

B. STATE TROJANS RELY ON THE STOCKPILING OF SYSTEM VULNERABILITIES, WHOSE RISK FOR INDIVIDUALS' RIGHTS CANNOT BE PROPORTIONATE TO THE BENEFIT SOUGHT IN A SINGLE CRIMINAL INVESTIGATION 15

CONCLUSIONS 18

Summary

Privacy International would like to provide this statement in the case of 2 BvR 1850/18 before the Federal Constitutional Court regarding the use of so-called "state trojans" as a standard measure in criminal investigation proceedings.

Privacy International is a non-profit, nongovernmental organization based in London dedicated to defending the right to privacy around the world. Established in 1990, Privacy International undertakes research and investigations into state and corporate surveillance with a focus on the technologies that enable these practices.

Privacy International has litigated or intervened in cases implicating the right to privacy in the courts of Europe, including the European Court of Human Rights and the Court of Justice of the European Union, and various nations, including the United Kingdom (UK), France, Hungary, the United States of America (US), Colombia, South Africa and South Korea. To ensure universal respect for the right to privacy, Privacy International advocates for strong national, regional and international laws that protect privacy. It is frequently called upon to give expert evidence to Parliamentary and Governmental committees around the world on privacy issues and has advised, and reported to, among others, the Council of Europe, the European Parliament, the Organisation of Economic Co-operation and Development, and the United Nations. It also strengthens the capacity of partner organizations in developing countries to do the same.

Focusing on the privacy and security concerns raised by the government use of state trojans, this statement puts forward the following submissions:

I. The use of state trojans threatens the essence of the rights to privacy and data protection under international and European human rights law;

II. The use of state trojans violates states' obligations to effectively guarantee the security and integrity of IT systems;

III. The use of state trojans may be incompatible with the principles of necessity and proportionality under both international and European law.

Introduction

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.[1] System refers both to any combination of hardware and software or a component thereof. This statement addresses a particular form of hacking, namely the state use of trojans, in accordance with paragraphs 100a and 100b of the German Code of Criminal Procedure (StPO).

As a form of government surveillance, state trojans present unique and grave threats to privacy and security. It has the potential to be far more intrusive than any other surveillance technique, permitting the government to remotely and surreptitiously access personal devices and all the intimate information they store.[2] It also permits the government to conduct novel forms of real-time surveillance, by covertly turning on a device's microphone, camera, or GPS-based locator technology, or by capturing continuous screenshots or seeing anything input into and output from the device.[3] The use of trojans allows governments to manipulate data on devices, by deleting, corrupting or planting data; recovering data that has been deleted; or adding or editing code to alter or add capabilities, all while erasing any trace of the intrusion. These targets are not confined to devices. They can extend also to communications networks and their underlying infrastructure.

At the same time, the use of state trojans has the potential to undermine the security of targeted devices, networks or infrastructure, and potentially even the internet as a whole. Computer systems are complex and, almost with certainty, contain vulnerabilities that third parties can exploit to compromise their security. Government use of state trojans often depends on exploiting vulnerabilities in systems to facilitate a surveillance objective. Government hacking may also involve manipulating people to interfere with their own systems. These latter techniques prey on user trust, the loss of which can undermine the security of systems and the internet.

---

[1] Privacy International, 'Government Hacking' available at https://privacyinternational.org/topics/government-hacking.

[2] See U.S. District Court, Western District of New York, Privacy International and Others v. Federal Bureau of Investigation and Others (Case No. 18-cv-1488) available at: https://privacyinternational.org/sites/default/files/2019-01/pi_v._fbi_-_hacking_foia_-_complaint_-_as_filed.pdf, paras 5-6.

[3] Investigatory Powers Tribunal (IPT), *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs*, Witness Statement of Eric King (5 October 2015) available at: https://privacyinternational.org/sites/default/files/2018-03/2015.10.05%20Witness_Statement_Of_Eric_King.pdf, 11-12.

A growing number of governments around the world are embracing a series of hacking measures, such as state trojans, to facilitate their surveillance activities.[4] 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 doing so without sufficient safeguards and oversight necessary to minimise the privacy and security implications of hacking.

In 2017, the German Code of Criminal Procedure (StPO) was amended to allow investigating authorities to "impinge" upon information technology systems in order to collect data from them.[5] This, in turn, would require the installation of software that reads data and transmits it to law enforcement authorities extracting it from the device of the person being targeted by surveillance technology. Such software is generally referred to as "state trojans".[6]

[4] See, for example, UK Investigatory Powers Act 2016, Part 5 (Equipment interference); U.S. Federal Rules of Criminal Procedure, Rule 41, and also Privacy International, 'Whose World Is This? US and UK Government Hacking' (July 2016) available at: https://privacyinternational.org/feature/1691/whose-world-us-and-uk-government-hacking; Article 15 of the Federal Law of the Russian Federation on the Federal Security Service Act (no. 40-FZ) 1995 ("[L]egal entities in the Russian Federation providing . . . electronic communications services of all types . . . shall be under obligation, at the request of federal security service organs, to include in the apparatus additional hardware and software and create other conditions required . . . to implement operational/technical measures").

[5] See §100a(1) and §100b of the German Code of Criminal Procedure, as amended by the Act of 17 August 2017, Bundesgesetzblatt 2017 I, 3202.

[6] Sven Herpig and Julia Schuetze, 'Umfassende Cyber-Sicherheitspolitik für Deutschland' (Stiftung Neue Verantwortung, 6 October 2017) available at: https://www.stiftung-nv.de/de/publikation/umfassende-cyber-sicherheitspolitik-fuer-deutschland.

I. The use of state trojans can threaten the essence of the rights to privacy and data protection under international and European human rights law, if not properly constrained

Human rights instruments that guarantee the right to privacy and the protection of individuals' personal data may sometimes permit interferences with these rights so long as those abide by certain principles, such as legality, necessity and proportionality, and do not interfere with the "*core*" or "*essence*" of those rights.[7]

The U.N. Special Rapporteur for Counterterrorism has emphasized that "*in no case may the restrictions be applied or invoked in a manner that would impair the essence of a Covenant right.*"[8] 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.*"[9]

Article 8 of the European Convention on Human Rights (hereinafter, ECHR) provides that "*[e]veryone has the right to respect for his private and family life, his home and his correspondence*". The European Court of Human Rights (hereinafter, ECtHR) has held that measures, such as covert surveillance for the purposes of detecting or preventing crime, fall within the ambit of Article 8 of the Convention and has underlined that restrictions imposed upon this right should not unacceptably weaken the protection afforded by this right.[10] In *Christine Goodwin v. the United Kingdom*,[11] the ECtHR noted:

> Nonetheless, the very essence of the Convention is respect for human dignity and human freedom. Under Article 8 of the Convention in particular, where

---

[7] See, in particular, International Covenant on Civil and Political Rights, Article 17(1) ("*No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation*"); Convention for the Protection of Human Rights and Fundamental Freedoms, Article 8(2) ("*There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society…*"); Charter of Fundamental Rights of the European Union, Article 52(1) ("*Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others*").

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

[9] OHCHR, *The Right to Privacy in the Digital Age* (A/HRC/27/37, 30 June 2014), para. 23; see also ECtHR, *Zakharov v. Russia* (App. No. 47143/06, 4 December 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*").

[10] ECtHR, *S. and Marper v. the United Kingdom*, App. Nos. 30562/04 and 30566/04, 4 December 2008, para 112.

[11] ECtHR, *Christine Goodwin v. the United Kingdom*, App. No. 28957/95, 11 July 2002

> the notion of personal autonomy is an important principle underlying the interpretation of its guarantees, protection is given to the personal sphere of each individual.[12]

Similarly, Article 7 and Article 8 of the Charter of Fundamental Rights of the EU (hereinafter, CFREU) guarantee the right to privacy and the right to protection of personal data, respectively. Article 52 para. 1 of the CFREU states that limitations on rights and freedoms recognised by the Charter must "*respect the essence of those rights and freedoms*". In *Digital Rights Ireland*,[13] the CJEU examined the compatibility of Directive 2006/24/EC (Data Retention Directive),[14] which provided for the retention of and access to traffic and location data for the purposes of preventing, detecting and prosecuting serious crime, with Articles 7 and 8 of the Charter. Regarding the essence of the right to privacy, the Court noted:

> [E]ven though the retention of data required by Directive 2006/24 constitutes a particularly serious interference with those rights, it is not such as to adversely affect the essence of those rights given that […] the directive does not permit the acquisition of knowledge of the content of the electronic communications as such.[15]

In other words, what this reasoning suggests is that serious interferences that permit the acquisition of the content of electronic communications *could* be regarded as adversely affecting the essence of the right to privacy and of the right to the protection of personal data.

Today, an individual's devices, such as a phone and/or a computer, have replaced their photo albums, personal diaries and journals, letters and papers, phone books and much more.[16] The plethora of capabilities that consumer devices come with also include various plug-ins that allow individuals to store not only messages, emails,

---

[12] Ibid, para 90.

[13] Joined Cases C-293/12 and C-594-12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources & Others and Seitlinger and Others* [2014] ECR I-238.

[14] Directive (EC) 2006/24 of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L105/54 (Data Retention Directive).

[15] Joined Cases C-293/12 and C-594-12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources & Others and Seitlinger and Others* [2014] ECR I-238, para 39.

[16] In *Riley v. California*, in the Supreme Court of the United States, Chief Justice Roberts posits on the intrusiveness of gaining access to a modern telephone: "*a cell phone collects in one place many distinct types of information – an address, a note, a prescription, a bank statement, a video – that reveal much more in combination than any isolated record…The sum of an individual's private life can be reconstructed through a thousand photographs labelled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet.*"

voice recordings, videos and photos, but also credit card details, including mobile banking and mobile payment data,[17] passport (biometric) data,[18] passwords, virtual keys to digital locks[19] etc.

The use of state trojans permits governments' remote access to these systems, control of features like cameras, microphones and keyboards, and therefore potentially access to all of the data stored thereon.[20] Privacy International has uncovered that, in the UK, police are using highly intrusive technology to extract and store data from individual's phones. The technology, which has been rolled out nationally following its use by the Metropolitan Police Service during the London Olympics in 2012, gives the police the ability to obtain data from our phones than we cannot access ourselves and which we do not know exists.[21]

State trojans are therefore an extremely intrusive investigative technique, even when deployed against individual devices, because, as demonstrated above, they allow access to variety of sensitive personal data or to intimate aspects of one's private life.

When a state trojan is deployed against an individual's device, it can achieve results that are at least as intrusive as if the targeted individual were to have his house bugged, his home searched, his communications intercepted, and a tracking device fitted to his person. Due to the unprecedented seriousness of this intrusion, and in order to ensure that they do not violate the essence of the rights, measures involving state trojans need to be deployed only in cases that deal with serious crime or act(s) amounting to a specific, serious threat to national security. In particular, investigating authorities need to make sure that such measures are limited to what is strictly

[17] See, for example, Visa, "Kontaktloses Bezahlen mit Visa", available at: https://www.visa.de/bezahlen-mit-visa/genutzte-technologien/kontaktloses-bezahlen-mit-visa.html.
[18] See, for example, Mobile QuickClear, available at: https://mobilepassport.us/#quickclear.
[19] See, for example, Nuki, "Eintreten in die Smart Home Welt mit Nuki deinem smarten Türschloss für Zuhause", available at: https://nuki.io/de/.
[20] Investigatory Powers Tribunal (IPT), *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs*, Witness Statement of Eric King (5 October 2015) available at: https://privacyinternational.org/sites/default/files/2018-03/2015.10.05%20Witness_Statement_Of_Eric_King.pdf, 10-11. See also, Der Spiegel, "How the NSA Accesses Smartphone Data" (9 September 2013), available at: https://www.spiegel.de/international/world/how-the-nsa-spies-on-smartphones-including-the-blackberry-a-921161.html.
[21] Privacy International, "Digital stop and search: how the UK police can secretly download everything from your mobile phone" (March 2018) available at: https://privacyinternational.org/sites/default/files/2018-03/Digital%20Stop%20and%20Search%20Report.pdf.

necessary, by, for example, specifying to the greatest extent possible the identity of the persons or the details of the target system (see point III.a. below).[22]

II. The use of state trojans violates states' obligations to effectively guarantee the security and integrity of IT systems

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 measures such as state trojans are relevant to an assessment of the scope and nature of that measure's interference with the right to privacy.

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*".[23] 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.[24]

The Special Rapporteur has also explained the relationship 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*,"[25] 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.*"[26] 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*

---

[22] See Privacy International, Hacking Safeguards and Legal Commentary (June 2018), available at: https://privacyinternational.org/advocacy-briefing/1057/hacking-safeguards-and-legal-commentary#3.

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

[24] Ibid.

[25] Report of the U.N. Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (A/HRC/29/32, 22 May 2015), para 6.

[26] Ibid.

products and services."[27] The Special Rapporteur concluded that "*States should avoid all measures that weaken the security that individuals may enjoy online.*"[28]

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*"[29] as well as in facilitating "*State surveillance*,"[30] including by "*respond[ing] to requirements that digital networks and communications infrastructure be designed to enable intrusion by the State.*"[31] 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*"[32] and to "*ensure that the private sector is able to carry out its functions independently in a manner that promotes individuals' human rights.*"[33] The Special Rapporteur concluded that "*States must refrain from forcing the privacy sector to implement measures compromising the privacy [and] security . . . of communications services.*"[34]

Fundamentally speaking, the use of state trojans is about causing technologies to act in a manner the manufacturer, owner or user did not intend or did not foresee. A single hack can affect many people, including those who are incidental or unrelated to a government investigation or operation. In other words, state trojans are about exploring – often in a creative fashion – vulnerabilities in computer security.[35]

The Federal Constitutional Court has recognised a right in confidentiality and integrity of information technology systems. In *BVerfG, 27.02.2008 - 1 BvR 370/07* and *1 BvR 595/07*, the Court clarified:

---

[27] Ibid, para 11.
[28] Ibid, para 60.
[29] Report of the U.N. Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (A/HRC/23/40, 17 April 2013), paras 72-74.
[30] Ibid.
[31] Ibid.
[32] Ibid, paras 76-77.
[33] Ibid,
[34] Ibid, para 96 (citing Office of the U.N. High Commissioner for Human Rights, Guiding Principles on Business and Human Rights, 2011); *see also* Report of the U.N. Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (A/HRC/29/32, 22 May 2015), para 28.
[35] See U.S. District Court, Central District of California (Eastern Division), In the matter of the search of an apple iPhone seized during the execution of a search warrant on a black Lexus is300, California license plate 35KGD203, Brief of Amici Curiae Privacy International and Human Rights Watch Available at: https://privacyinternational.org/sites/default/files/2018-03/Amicus%20Brief%20-%20PI%20and%20HRW.pdf, 6-7.

> The fundamental right to guarantee the integrity and confidentiality of information technology systems, on the other hand, must be applied if the authorisation to interfere covers systems which alone or in their technical networks may contain personal data of the data subject to such an extent and variety that access to the system makes it possible to gain an insight into essential parts of a person's lifestyle or even to obtain a meaningful picture of his or her personality. Such a possibility exists, for example, when accessing personal computers, regardless of whether they are permanently installed or mobile. Not only when used for private purposes, but also when used for business purposes, personal characteristics or preferences can regularly be inferred from the user behaviour. The specific protection of fundamental rights also extends, for example, to mobile telephones or electronic diaries, which have a wide range of functions and can record and store personal data of various kinds.[36]

The ECHR does not only impose obligations on states to abstain from interfering with individuals' rights. It also imposes positive obligations on public authorities to secure the rights enshrined in the Convention, including the right to privacy.[37] The European Court of Human Rights has held that the "*protection of personal data […] is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention*".[38]

EU law imposes similar obligations on member states to guarantee the security and integrity of information systems. Specifically, Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016[39] establishes rules for the processing of personal data, also in the context of a criminal investigation.[40] The Directive, which

---

[36] BVerfG, Urteil des Ersten Senats vom 27. Februar 2008, 1BvR370/071 und BvR 595/07, Ziff. 20.

[37] See, for example, *K.U. v. Finland*, App. No. 2872/02, 2 December 2008, para 42.

[38] *I v. Finland*, App. No. 20511/03, 17 July 2008, para 38.

[39] Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

[40] For the interplay between privacy and data protection, and how government hacking may also interfere with data protection rights, see EU Agency for Fundamental Rights (FRA), Handbook on European data protection law (2018 Edition) available at: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf, 20; Juliane Kokott and Christoph Sobotta, 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR' International Data Privacy Law (Volume 3, Issue 4, November 2013) 222-228; CJEU, Joined Cases C-293/12 and C-594-12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources & Others and Seitlinger and Others* [2014] ECR I-238.

was transposed into German law,[41] underlines a series of obligations which could be can be summarised as ensuring the security, integrity and confidentiality of personal data by implementing relevant measures. Article 29 (Security of processing) paragraph 1 of the Directive reads:

> Member States shall provide for the controller and the processor, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, in particular as regards the processing of special categories of personal data referred to in Article 10.[42]

As we continue to integrate computer systems into the fabric of our lives, economies and societies, safeguarding the security of those systems becomes increasingly important. Contrary to these obligations, in order to deploy state trojans governments must induce security holes in the system that protect computers, telephones and networks.[43]

Taking into account the obligations of states to maintain the integrity and security of information systems, so that individuals can effectively exercise their fundamental

---

[41] Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU) Official publication: Bundesgesetzblatt 2017 1, 2097.

[42] These obligations are further clarified in paragraph 2, for example, which requires controllers, including relevant law enforcement authorities, to: *(a) deny unauthorised persons access to processing equipment used for processing ('equipment access control'); (b) prevent the unauthorised reading, copying, modification or removal of data media ('data media control'); (c) prevent the unauthorised input of personal data and the unauthorised inspection, modification or deletion of stored personal data ('storage control'); (f) ensure that it is possible to verify and establish the bodies to which personal data have been or may be transmitted or made available using data communication equipment ('communication control'); (h) prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media ('transport control'); (i) ensure that installed systems may, in the case of interruption, be restored ('recovery'); (j) ensure that the functions of the system perform, that the appearance of faults in the functions is reported ('reliability') and that stored personal data cannot be corrupted by means of a malfunctioning of the system ('integrity')* etc.

[43] See Investigatory Powers Tribunal (IPT), *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs*, Expert report of Professor Ross Anderson (30 September 2015) available at: https://privacyinternational.org/sites/default/files/2018-03/2015.09.30%20Anderson_IPT_Expert_Report_2015_Final.pdf, 17-19; Investigatory Powers Tribunal (IPT), *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs*, Witness Statement of Eric King (5 October 2015) available at: https://privacyinternational.org/sites/default/files/2018-03/2015.10.05%20Witness_Statement_Of_Eric_King.pdf, 22ff.

rights, inducing measures relying on state trojans that undermine the security of systems cannot be seen to be compatible with human rights law. State trojans, in such circumstances, contradict states' obligations to guarantee individuals' privacy and data protection, by implementing measures that would protect the security, integrity and confidentiality of information technology systems. By their very nature, state trojans require the exact opposite; a continuous undermining of security.

III. The use of state trojans should not violate the principles of necessity and proportionality under both international and European law

Due to their extremely intrusive nature and the serious security concerns they raise for individuals' privacy and data protection, government use of state trojans may struggle to be compatible with the principles of necessity and proportionality.

a. State trojans must be limited to what is strictly necessary for the purposes of prosecuting crime

Both international and EU human rights laws require that any interference with the right to privacy must be necessary and proportionate. 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.[44]

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'*."[45]

The ECtHR has also applied *strict* necessity to interferences with the right to privacy in the surveillance context. In *Szabó and Vissy v. Hungary*, the Court indicated that, given "*the potential of cutting-edge surveillance technologies to invade citizens' privacy*,":[46]

[44] U.N. Human Rights Council, Resolution on the Right to Privacy in the Digital Age (A/HRC/34/L.7/Rev.1, 22 March 2017), 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").

[45] CCPR, General Comment Nr. 34 (CCPR/C/GC/34, 12 September 2011), para. 35.

[46] ECtHR, *Szabó and Vissy v. Hungary* (App. No. 37138/14, 12 January 2016), para 73.

> 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.[47]

Similarly, in the context of data retention measures, the Court of Justice of the EU has held that, in order to be limited to what is strictly necessary, these measures must be subject to restrictions which "*circumscribe, in practice, the extent of that measure and, thus, the public affected*".[48]

As mentioned in point 1 above, state trojans can provide for a generalised, real-time access of investigating authorities not only to communications data and content of communications of an individual, but also to the most intimate aspects of their private lives, as authorities are able to in real time infiltrate a person's privacy by accessing uncommunicated photos, videos, diaries, notes and any other sensitive or non-sensitive data stored on their device, as well as covertly utilising microphones, cameras, GPS-tracking and other such functionalities.

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. For example, an IP address may relate to more than one person using the same network. This might inevitably result in investigating authorities accessing a plethora of information relating to the private life of people not under criminal investigation.[49]

In light of the considerations above, Privacy International strongly questions whether the use of state trojans can ever be made necessary and proportionate.

---

[47] Ibid.

[48] CJEU, Joined Cases C–203/15 and C–698/15 Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson [2016] ECR I–970, para 110.

[49] See, for example, Privacy International's submissions in U.S. Court of Appeals, U.S.A. v. Alex Levin (Nr. 16-1567, 10. Februar 2017) https://privacyinternational.org/sites/default/files/2018-10/2017.02.10_DOCKETED_Amicus_Brief.pdf. In this case, trojans were used by a law enforcement agencies to target large number sof people.

At the very least, use of state trojans should be considered as violating necessity, unless they are limited to what is strictly necessary. Specifically, prior to carrying out this hacking measure, government authorities must, at a minimum, establish:

(i) A high degree of probability that:

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

(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 the use of state trojans is the least intrusive option;

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

Privacy International has further articulated a full set of safeguards that must be attached to state hacking, if it is to be undertaken.[50]

[50] Privacy International, Hacking Safeguards and Legal Commentary (June 2018), available at: https://privacyinternational.org/advocacy-briefing/1057/hacking-safeguards-and-legal-commentary#3.

b. State trojans rely on the stockpiling of system vulnerabilities, whose risk for individuals' rights cannot be proportionate to the benefit sought in a single criminal investigation

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.*" [51] 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."*[52]

When determining whether an interference with the right to privacy was necessary in a democratic society, the European Court of Human Rights also examines whether the interference was proportionate to the aims pursued. This necessarily involves a balancing exercise between competing interests.[53] In that regard, "*national authorities enjoy a margin of appreciation, the scope of which will depend not only on the nature of the legitimate aim pursued but also on the particular nature of the interference involved*".[54]

In *S. and Marper v. the United Kingdom*,[55] the ECtHR dealt with the measure of DNA retention for the purposes of detecting and prosecuting crime. It noted:

> The Court observes that the protection afforded by Article 8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests. In the Court's view, the strong consensus existing among the Contracting States in this respect is of considerable importance and narrows the margin of appreciation left to the respondent State in the assessment of the permissible limits of the interference with private life in this sphere. The Court considers that any State claiming a pioneer role in the development of new technologies bears special responsibility for striking the right balance in this regard.[56]

---

[51] U.N., Report of the U.N. Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism (A/69/397, 23 September 2014), para 51.
[52] Ibid.
[53] ECtHR, *Z v. Finland* (App. No. 22009/93, 25 February 1997), para 94.
[54] ECtHR, *Leander v. Sweden* (App. No. 9248/81, 26 March 1987), para 59.
[55] ECtHR, S. and Marper v. the United Kingdom (App. Nos. 30562/04 and 30566/04, 4 December 2008).
[56] Ibid, para 112.

The use of state trojans relies on the exploitation of system vulnerabilities by investigating authorities, such as 0-day vulnerabilities. A 0-day vulnerability refers to a security flaw in software that is unknown to the vendor.[57] 0-day vulnerabilities get their name from the fact that, when identified, the computer user has had "0 days" to fix them before attackers can exploit the vulnerabilities. When researchers, white-hat hackers, and others discover vulnerabilities, they usually report the flaw to the company responsible for the security of the affected software.

When governments use 0-day vulnerabilities they face a dichotomy of sorts – should they stockpile or hoard 0-days in order to carry out a hacking measure which could potentially lead to a prosecution case or should they notify the vendor and ask them to fix the vulnerability for the public good? If authorities are allowed to exploit such gaps, they will more likely than not have an interest in building an "arsenal" of security gaps in order to be able to attack a target in the event of an investigation. This interest, in turn, will prevent them from notifying the affected manufacturer of IT systems, who can help close the security gap that has been discovered. If this happens, this means that the wider worldwide security risk would far outweigh the possible facilitation of prosecution in individual cases. [58]

Vulnerabilities are today being sold for six figure sums.[59] Governments have become some of the biggest developers and purchasers of information identifying 0-days.[60] In most cases, after buying 0-days, governments are reluctant to reveal them to software makers because the hole might then be repaired, curtailing government access. Governments therefore risk the security of their own citizens and businesses.[61]

---

[57] *See* Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (W. W. Norton & Company, 2015) ("Unpublished vulnerabilities are called 'zero-day' vulnerabilities; they're very vulnerable to attackers because no one is protected against them, and they can be used worldwide with impunity.").

[58] *See* Investigatory Powers Tribunal (IPT), *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs*, Expert report of Professor Ross Anderson (30 September 2015) available at: https://privacyinternational.org/sites/default/files/2018-03/2015.09.30%20Anderson_IPT_Expert_Report_2015_Final.pdf, 8.

[59] Ibid, 10.

[60] David E. Sanger, 'Obama Lets NSA Exploit Some Internet Flaws, Officials Say' (The New York Times, 12 April 2014) available at: https://www.nytimes.com/2014/04/13/us/politics/obama-lets-nsa-exploit-some-internet-flaws-officials-say.html?_r=1.

[61] Sean Gallagher, 'NSA secretly hijacked existing malware to spy on N. Korea, others' (ArsTechnica, 19 January 2015) available at: http://arstechnica.com/informationPtechnology/2015/01/nsa-secretly-hijacked-existing-malware-to-spy-on-n-korea-others.

Unfortunately, each time intelligence services use a 0-day exploit, they also risk its discovery by criminals and other foreign agents who might use it against citizens.[62]

What recent cyberattacks have underlined is that hoarding system vulnerabilities might have onerous consequences for citizens globally. WannaCry, for example, was developed by hackers who effectively managed to exploit vulnerabilities stockpiled by the United States National Security Agency (NSA),[63] and seriously impacted European infrastructure operators in the sectors of health, energy, transport, finance and telecoms.[64]

Germany and the United Kingdom were among the first countries where the WannaCry malware attack was reported. According to the Berlin public prosecutor's office, the WannaCry attack resulted in a total of 450 Deutsche Bahn computers being affected.[65] In the United Kingdom, the WannaCry cyberattack had potentially serious implications for the National Health Service, leading to widespread disruption in at least 81 of 236 hospital trusts in England, with 19,000 medical appointments being cancelled, computers at 600 general practitioner surgeries being locked, and five hospitals having to divert ambulances elsewhere.[66] This potentially resulted in chaotic situations for patients, with sensitive personal data being encrypted or destroyed by the malware.[67]

The hoarding of system vulnerabilities by the state so that they can be used for deploying state trojans is disproportionate. Even when surveillance through state trojans is carried out in the context of legitimate aims, such as targeted criminal prosecutions, this cannot on its own outweigh the privacy and security interests of

---

[62] See Sven Herpig, 'A Framework for Government Hacking in Criminal Investigations' (Stiftung Neue Verantwortung, October 2018) available at: https://www.stiftung-nv.de/sites/default/files/framework_for_government_hacking_in_criminal_investigations.pdf.

[63] Linus Neumann, '"WannaCry"-Cyberattacke Die Lehren aus dem weltweit größten Angriff mit Erpressungssoftware' (Spiegel Online, 15 May 2017) available at: https://www.spiegel.de/netzwelt/web/wannacry-die-lehren-aus-dem-cyberangriff-a-1147589.html.

[64] EU Agency for Fundamental Rights (FRA), Fundamental Rights Report 2018 available at: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2_en.pdf, 161.

[65] Markus Böhm, 'Experten über "WannaCry"-Attacke: "Wir hatten noch Glück"' (16 May 2017) available at: https://www.spiegel.de/netzwelt/web/wannacry-450-bahn-computer-von-cyber-attacke-betroffen-a-1147921.html.

[66] UK, National Audit Office, Department of Health, Investigation: WannaCry cyber-attack and the NHS (Report by the Comptroller and Auditor General, 27 October 2017) available at: https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf.

[67] Zeit Online, 'WannaCry: Microsoft gibt US-Regierung Mitschuld an Hackerangriff' (15 May 2017) available at: https://www.zeit.de/digital/internet/2017-05/wannacry-microsoft-nsa-hackerangriff-usa-regierung.

individuals, whose sensitive personal data are rendered vulnerable to third-party exploitation.[68]

Conclusions

In all, state trojans present unique and grave threats to privacy and security. State trojans that rely on system vulnerabilities, or "0-days," should not be used unless those risks can be fully mitigated.

Because of their high level of intrusiveness, implementing measures that rely on state trojans threaten the essence of fundamental rights, such as the right to privacy and data protection.

Relying on state trojans that exploit security vulnerabilities also contradicts states' obligations to maintain the integrity and security of information systems, under both international and EU law standards.

The use of state trojans must be carefully examined under the principles of necessity and proportionality. Current state trojan technology makes it very difficult to limit an investigation to obtaining what is strictly necessary. Moreover, in balancing the state exploitation of vulnerabilities against the wider security risk to society, the use of vulnerabilities to facilitate state trojans cannot be proportionate, and would thus violate both international and European human rights standards.

30 September 2019

Privacy International
62 Britton Street
London EC1M 5UY
+44 (0) 20 3422 4321

[68] See also Sven Herpig, 'Schwachstellen- Management für mehr Sicherheit: Wie der Staat den Umgang mit Zero-Day-Schwachstellen regeln sollte' (Stiftung Neue Verantwortung, August 2018) available at: https://www.stiftung-nv.de/sites/default/files/vorschlag.schwachstellenmanagement.pdf.



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

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

UK Registered Charity No. 1147471