IN THE EUROPEAN COURT OF HUMAN RIGHTS **App No. 46259/16**

PRIVACY INTERNATIONAL AND OTHERS

– v –

THE UNITED KINGDOM

THIRD PARTY INTERVENTION OF

THE ELECTRONIC PRIVACY INFORMATION CENTER ("EPIC")

Introduction

1. The Electronic Privacy Information Center ("EPIC") welcomes the opportunity to submit these written comments pursuant to leave granted on February 12, 2019, by the President of the First Section under Rule 44 § 3 of the Rules of the Court.

2. EPIC is a leading privacy and freedom of information organization in the United States. A public interest, non-profit research and educational organization in Washington, D.C., EPIC was established in 1994 to focus public attention on emerging privacy and civil liberties issues and to protect privacy, freedom of expression, and democratic values in the information age.[1] EPIC pursues a wide range of program activities including policy research, public education, conferences, litigation, publications, and advocacy. EPIC also works closely with a distinguished board of advisors, who are experts in law, technology and public policy and maintains one of the most popular privacy web sites in the world—epic.org. EPIC has participated as *amicus curiae* in close to one hundred cases in the United States, and previously served as third-party intervener with the European Court of Human Rights in *Big Brother Watch and Others v. the United Kingdom* (Applications nos. 58170/13, 62322/14 and 24960/15).[2]

3. *Privacy International and Others v. the United Kingdom* concerns a matter of essential importance to fundamental rights: whether the "computer hacking" techniques—including the surreptitious collection of information stored in a personal device that may be kept in a home or business—authorized under UK law, violate the European Convention on Human Rights. In accordance with Rule 44 § 5, these submissions do not address the facts or merits of the applicants' case. EPIC instead submits general concerns

[1] *See* EPIC, *About EPIC,* EPIC.org, https://epic.org/epic/about.html.
[2] *See* EPIC, *EPIC Amicus Curiae Briefs*, EPIC.org, https://epic.org/amicus/.

regarding this conduct by governments and the human rights issues implicated in this case. Specifically, EPIC provides context to the Court regarding (1) the scope and consequences of the government hacking, and (2) relevant recommendations of the U.S. President's Review Group, a high-level expert group, to limit the risks of these techniques. [3]

I. Government hacking creates unique risk to cybersecurity and individual rights

4. Government hacking comprises exploitation of software and hardware vulnerabilities, or the installation of malicious software, to gain access to data or control of a computer system.[4] Many nations make it a criminal offense to engage in computer hacking.[5] There is also an international convention on Cybercrime that seeks to coordinae the investigaitons and prosectuon of computer hacking.[6] Countries recognize a significant risk to public safety, economic activity, and national security arising from computer hacking. Increasingly, many nations view cybersecurity as a critical component of national security—western nations in Europe and America face asymmetric risks due to their highly connected commercial and municipal infrastructure, which creates a broad attack surface.[7]

5. Government attacks on private computer systems pose clear threats to cybersecurity, as well as for individual rights to privacy and free expression. For instance, hacking tools and vulnerabilities stockpiled by governments could be leaked or exfiltrated and then used by criminals to mount cyberattacks.[8] Hacking tools are routinely sold and deployed by malicious actors. And governments seek special access to private devices for investigatory purposes, they weaken essential security features and create new cybersecurity risks. [9]

---

[3] For details of the disclosures, *see* Barton Gellman & Ashkan Soltani, *NSA Collects Millions of E-mail Address Books Globally*, Wash. Post (Oct. 14, 2013), https://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html; Barton Gellman & Ashkan Soltani, *NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say*, Wash. Post (Oct. 20, 2013), http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

[4] Sven Herpig, Government Hacking: Global Challenges 3-4 (2017), http://cyber.haifa.ac.il/images/pdf/Government_Hacking_TCF.pdf/

[5] *See, e.g.*, 18 U.S.C. § 1030 ("Computer Fraud and Abuse Act") (criminal code of the United States).

[6] Council of Europe Convention on Cybercrime, Nov. 23, 2001, S. Treaty No. 108-11 (2003) (ratified Sept. 22, 2006).

[7] David E. Sanger, David D. Kirkpatrick and Nicole Perlroth, *The World Once Laughed at North Korean Cyberpower. No More*, N.Y. Times (Dec. 15, 2017), https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html

[8] *See., e.g.*, Scott Shane & Adam Goldman, *Suspect Identified in C.I.A. Leak Was Charged, but Not for the Breach,* N.Y. Times (May 16, 2018), https://www.nytimes.com/2018/05/15/us/cia-hacking-tools-leak.html.

[9] *See generally* Riana Pfefferkorn, Security Risks of Government Hacking (2018), https://cyberlaw.stanford.edu/files/publication/files/2018.09.04_Security_Risks_of_Government_Hacking_Whitepaper.pdf. For instance, the willingness by governments to pay for these

6. The risks of cascading effects inherent in stockpiling hacking technology became clear when some of the U.S. National Security Agency's most closely-guarded hacking tools were obtained by a group of hackers in 2016-2017; the group promptly dumped the material online.[10]

7. The hacking tools' release precipitated one of the largest cyberattacks in history. The attack, later attributed to North Korea,[11] relied on a Microsoft system vulnerability held by the NSA and impacted more than 200,000 computers in over 150 countries.[12] Referred to as "WannaCry," the self-propagating worm took the form of a ransomware attack: after encrypting the data of infected computers the perpetrators demand untraceable payment in order for users to regain access, under threat that the files will be destroyed.[13]

8. WannaCry affected Spanish mobile operator Telefónica, major car manufacturers, and Russian government ministries.[14] However, the effects on the UK National Health Service were most catastrophic,[15] The attack disconnected hospitals, diverting ambulances and disrupting surgeries, and causing an estimated 92 million pounds in economic damage.[16]

9. Though Microsoft had released a patch to the vulnerability two months prior to the attack, many systems had not yet updated their software to prevent the damage.[17] In fact, WannaCry was "attempting to infect thousands of systems a month" in the third-quarter of 2018.[18]

10. In the wake of the attack, Microsoft contended:

---

techniques stokes a growing exploit market, and hacking can impact civilians since cyber operations in an inter-connected world lack appropriate distinction. *Id.*

[10] Scott Shane, Nicole Perlroth, & David Sanger, *Security Breach and Spilled Secrets Have Shaken the N.S.A. to Its Core,* N.Y. Times (Nov. 12, 2017), https://www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html.

[11] Dustin Volz, *U.S. blames North Korea for 'WannaCry' cyber attack*, Reuters (Dec. 18, 2017), https://www.reuters.com/article/us-usa-cyber-northkorea-idUSKBN1ED00Q.

[12] Ian Sherr, *WannaCry ransomware: Everything you need to know*, CNet (May 19, 2017), https://www.cnet.com/news/wannacry-wannacrypt-uiwix-ransomware-everything-you-need-to-know/.

[13] Danny Palmer, *WannaCry ransomware crisis, one year on: Are we ready for the next global cyber attack?*, ZDNet (May 11, 2018), https://www.zdnet.com/article/wannacry-ransomware-crisis-one-year-on-are-we-ready-for-the-next-global-cyber-attack/. Some experts contend that the ransomware attack covered for a "more destructive intent," or was even the result of accidental release of the tool. *See* Ian Sherr, s*upra* note 12.

[14] Danny Palmer, *WannaCry ransomware crisis, one year on: Are we ready for the next global cyber attack?*, *supra* note 13.

[15] BBC, *NHS cyber-attack: GPs and hospitals hit by ransomware*, BBC (May 13, 2017), https://www.bbc.com/news/health-39899646.

[16] Matthew Field, *WannaCry cyber attack cost the NHS £92m as 19,000 appointments cancelled,* Telegraph (Oct. 11, 2018), https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/.

[17] Danny Palmer, *Why WannaCry ransomware is still a threat to your PC*, ZDNet (Nov. 13, 2018), https://www.zdnet.com/article/why-wannacry-ransomware-is-still-a-threat-to-your-pc/.

[18] *Id*.

[T]his attack provides yet another example of why the stockpiling of vulnerabilities by governments is such a problem. This is an emerging pattern in 2017…. Repeatedly, exploits in the hands of governments have leaked into the public domain and caused widespread damage. An equivalent scenario with conventional weapons would be the U.S. military having some of its Tomahawk missiles stolen. And this most recent attack represents a completely unintended but disconcerting link between the two most serious forms of cybersecurity threats in the world today – nation-state action and organized criminal action.

The governments of the world should treat this attack as a wake-up call.[19]

11. Nations' desire to deploy hacking techniques in investigations also encourages efforts to weaken essential security features such as encryption.

12. Encryption allows individuals to authenticate transactions and safeguard data, protecting a digitized global economy.[20] Encryption prevents crime, protecting "*billions of people every day against countless threats—be they street criminals trying to steal our phones and laptops, computer criminals trying to defraud us, corporate spies trying to obtain our companies' most valuable trade secrets*."[21]

13. Encrypted communications also support freedom of expression—protecting human rights defenders, journalists, and vulnerable communities from harm, and subverting unlawful censorship by states.[22] "*Encryption and anonymity, separately or together, create a zone of privacy to protect opinion and belief*," Special Rapporteur on the freedom of expression has explained.[23]

14. As security expert Bruce Schneier notes, while good digital security requires more than encryption, it is "*a critical component of security"*:

Strong encryption means unbreakable encryption. Any weakness in encryption will be exploited -- by hackers, by criminals and by foreign governments. Many of the hacks that make the news can be attributed to weak or -- even worse -- nonexistent encryption.[24]

---

[19] Brad Smith, *The need for urgent collective action to keep people safe online: Lessons from last week's cyberattack*, Microsoft (May 14, 2017), https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/.

[20] Coalition comments regarding the Parliamentary Joint Committee on Intelligence and Security (PJCIS) review of the Telecommunication and Other Legislation Amendment (Assistance and Access) Bill 2018 1 (October 11, 2018), https://newamericadotorg.s3.amazonaws.com/documents/Coalition_Comments_on_Australia_Assistance_and_Access_Bill_2018_10-11-18.pdf [hereinafter Coalition Comments Assistance and Access Law].

[21] *Id.* at 1—2.

[22] *Id.* at 1.

[23] U.N. Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *Report on the use of Encryption and Anonymity in Digital Communications*, ¶ 12, U.N. Doc. A/HRC/29/32 (May 22, 2015).

[24] Bruce Schneier, *The Importance of Strong Encryption to Security*, Schneier on Security (Feb. 25, 2016), https://www.schneier.com/blog/archives/2016/02/the_importance_.html.

15. Nonetheless, governments have long called for encryption workarounds.[25] But these back doors, just as other hacking tools, are prime targets for theft. Any vulnerability created to provide exceptional government access is equally available to malicious actors once discovered.

16. The quintessential call for exceptional access in the U.S. gave rise to the 2016 *Apple v. FBI* litigation.[26] Apple had provided the Federal Bureau of Investigation with all data that it possessed for the accounts of criminal suspects in a high-profile investigation,[27] but the FBI also demanded access to encrypted data stored on two devices.[28] Because Apple itself had no technological capacity to access the encrypted data—maintained only on the user's device —the company could not produce the data. Yet the FBI sought a court order requiring Apple to develop techniques that would allow FBI to break the password protection on the devices and obtain access to the encrypted data. [29]

17. When Apple refused, the FBI sued. EPIC filed an *amicus brief* for the federal court, explaining the "security features in dispute in this case were adopted to protect consumers from crime."[30]

18. EPIC furthered explained, that the practical consequences of acceding to the FBI request would have made millions of iPhones around the world susceptible to attack by criminal hackers. In fact, the strong safety features that Apple had adopted (and defended in the FBI case) were precisely to minimize the risks associated with unlawful hacking.[31]

19. Connected consumer technologies, like cell phones, are a primary target for criminals and identity thieves, as EPIC explained in the *Apple* case.[32] Device manufacturers devoted time and resources to develop strong security features seeking to outrun cybercriminals.[33] If the court ordered Apple "to develop techniques that deactivate the core security features on the iPhone, every iPhone user and every individual whose personal data is stored on an iPhone could be impacted," EPIC concluded.[34]

---

[25] EPIC, *The Clipper Chip*, Epic.org, https://epic.org/crypto/clipper/.
[26] EPIC, *Apple v. FBI*, Epic.org, https://www.epic.org/amicus/crypto/apple/.
[27] Tim Cook, A Message to Our Customers, Apple (Feb. 16, 2016), https://www.apple.com/customer-letter/.
[28] Government's Ex Parte Application for Order Compelling Apple Inc. To Assist Agents in Search, In the Matter of the Search of an Apple IPhone Seized During the Execution of a Search Warrant on a Black Lexis IS300, California License Plate 35KG203, No. 15-0451M (C.D. Cal. Feb. 16, 2016).
[29] Order Compelling Apple, Inc. to Assist in Search, In the Matter of the Search Warrant of an Apple IPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. 15-0451M (C.D. Cal. Feb. 16, 2016).
[30] Brief for Amicus Curiae Electronic Privacy Information Center (EPIC) and Eight Consumer Privacy Organizations at 6, In the Matter of the Search of an Apple IPhone Seized During the Execution of a Search Warrant on a Black Lexis IS300, California License Plate 35KG203, No. 15-0451M (C.D. Cal. Mar. 22, 2016), https://www.epic.org/amicus/crypto/apple/EPIC-Corrected-Amicus-Brief.pdf
[31] *Id*. at 10—12.
[32] *Id*. at 6.
[33] *Id*. at 10—12
[34] *Id*. at 4.

20. EPIC further explained Smartphone theft was so widespread by 2012 that the Federal Communications Commission, in consultation with congressional leaders and state law enforcement agencies, developed strategies to curb the problems of "massive smartphone and data theft" and the resulting harms to consumers. [35]

21. The day before the court hearing was scheduled, the FBI asked to delay the hearing, and eventually dropped the case.[36] As a consequence, Apple was not forced to alter security features that safeguarded the personal data on millions of iPhones around the world.

22. Much less is known about government efforts to weaken security features for foreign intelligence purposes. However, documents in the Snowden disclosures suggest the U.S. Government sought to weaken a "pseudo random bit generator" algorithm Dual EC-DRBG.[37] This technology serves multiple purposes for strong encryption—for encryption "keys, random authentication challenges, initialization vectors, nonces, key-agreement schemes, generating prime numbers" other purposes.[38] The NSA advocated for industry and standards bodies to adopt Dual_EC_DRBG.[39] The National Institute of Standards Technology (NIST), an expert federal agency in charge of the development of cryptographic standards, eventually adopted the standard without knowledge of NSA's involvement.[40]

23. In 2015, a company called Juniper Networks revealed that hackers had been able to decrypt Virtual Private Network traffic by building upon the pre-existing security weakness in the pseudo random bit generator.[41]

II. A U.S. expert report proposed safeguards for public safety and to manage the risks of government hacking operations

In 2013, following the public revelations that the National Security Agency had developed techniques to exploit computer vulnerabilities, President Obama created a Review Group on Intelligence and Communications Technologies to assess whether the U.S. "*employs its technical collection capabilities in a manner that optimally protects our national security and advances our foreign policy while appropriately accounting for other policy considerations,*" such as privacy and civil liberties, risk of unauthorized

[35] FCC, Press Release, Chairman Genachowski Joins Senator Schumer, D.C. Mayor Gray, State Police Departments, and Wireless Carriers to Announce New Initiatives to Combat Massive Smartphone & Data Theft (Apr. 10, 2012).
[36] Government's Ex Parte Motion for a Continuance, In the Matter of the Search Warrant of an Apple IPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. 15-0451M (C.D. Cal. Feb. 22, 2016).
[37] Nicole Perlroth, Jeff Larson, & Scott Shane, *N.S.A. Able to Foil Basic Safeguards of Privacy on Web*, N.Y. Times (Sept. 5, 20130), https://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html.
[38] Bruce Schneier, *Did NSA Put A Secret Backdoor in New Encryption Standard?*, Wired (Nov. 15, 2013), https://www.wired.com/2007/11/securitymatters-1115/.
[39] Susan Landau, *On NSA's Subversion of NIST's Algorithm*, Lawfare (July 25, 2014), https://www.lawfareblog.com/nsas-subversion-nists-algorithm.
[40] *Id.*
[41] Riana Pfefferkorn, *supra* note 9, at 12—13.

disclosure, and protecting domestic and international trust.[42] The Group presented its recommendations later that year.[43]

24. The recommendations of the U.S. Review Group on Intelligence and Communications Technologies bear on determination of the present matter. The Review Group included leading experts on cybersecurity, privacy, fundamental rights, and the needs of the intelligence services.[44] The Review Group included a Presidential advisor on cybersecurity, a noted privacy scholar, a leading authority on the U.S. Constitution, , and the former acting director of the CIA. EPIC noted favorably the recommendations of the Review Group and urged implementation.[45]

25. First, Recommendation 29 (on encryption) of the U.S. Review Group states:

> *We recommend that, regarding encryption, the US Government should: (1) fully support and not undermine efforts to create encryption standards; (2) not in any way subvert, undermine, weaken, or make vulnerable generally available commercial software; and (3) increase the use of encryption and urge US companies to do so, in order to better protect data in transit, at rest, in the cloud, and in other storage.*[46]

26. To effectuate Recommendation 29, the Review Group urged the NSA not to take specific steps that would undermine encryption:

- *NSA will not engineer vulnerabilities into the encryption algorithms that guard global commerce;*
- *The United States will not provide competitive advantage to US firms by the provision to those corporations of industrial espionage;*
- *NSA will not demand changes in any product by any vendor for the purpose of undermining the security or integrity of the product, or to ease NSA's clandestine collection of information by users of the product;*
- *and NSA will not hold encrypted communication as a way to avoid retention limits.*[47]

27. Second, Recommendation 30 (on vulnerability disclosure) states:

---

[42] Memorandum Reviewing Our Global Signals Intelligence Collection and Communications Technologies, 78 Fed. Reg. 49653 (Aug. 12, 2013).
[43] President's Review Group on Intelligence and Communications Technologies, Liberty and Security in a Changing World (2013), https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.
[44] *Id*. at 2
[45] EPIC, *Expert Panel Calls for End of NSA Bulk Data Collection* (Dec. 19, 2018), https://epic.org/2013/12/expert-panel-calls-for-end-of-.html, EPIC, *Presidential Review Scorecard*, https://www.epic.org/privacy/surveillance/prg-scorecard/.
[46] President's Review Group on Intelligence and Communications Technologies, *supra* note 43, at 216.
[47] *Id*. at 218.

We recommend that the National Security Council staff should manage an interagency process to review on a regular basis the activities of the US Government regarding attacks that exploit a previously unknown vulnerability in a computer application or system. These are often called "Zero Day" attacks because developers have had zero days to address and patch the vulnerability. US policy should generally move to ensure that Zero Days are quickly blocked, so that the underlying vulnerabilities are patched on US Government and other networks. In rare instances, US policy may briefly authorize using a Zero Day for high priority intelligence collection, following senior, interagency review involving all appropriate departments.[48]

28. In particular, the U.S. Review Group recognized that vulnerabilities in critical infrastructure should be addressed as soon as possible, and that "*for widely used code, it is in the national interest to eliminate software vulnerabilities rather than to use them for US intelligence collection*."[49]

29. The U.S. Review Group also recognized that only in exceptional cases "*when an urgent and significant national security priority can be addressed by the use of a Zero Day*" should the government use, instead of disclose, the exploit.[50] Such decision should be made only through a well-established process to assess the risk, deliberated at the highest levels of government.[51]

30. In fact, the U.S. began the process of establishing a vulnerabilities equities process (VEP) for intelligence agencies 2008.[52] However, the effort was completed in secret only at the urging of the Review Group. In 2017, the U.S. declassified the basic contours of its VEP—the composition of an interagency network and process for deliberation about whether to disclose a vulnerability as well as requirements for internal auditing.[53] While the policy has limitations—like internal executive branch accountability mechanisms that may lack true independence and a limited scope covering one type of vulnerabilities—publication of the VEP charter is a welcome first step toward transparency.[54] Following this model, United Kingdom recently disclosed the contents of its own, very similar VEP.[55]

Conclusion

31. Government hacking is unique among surveillance techniques. The practice entails a primary interference with systems or data, but also carries an inherent risk of cascading effects for digital security and the rights of privacy and freedom of expression.

32. Government hacking exploits vulnerabilities that should be corrected and fixed.

---

[48] *Id*. at 219.
[49] *Id*. at 219—20.
[50] *Id*. at 220.
[51] *Id*.
[52] EPIC, *Vulnerabilities Equities Process*, Epic.org, https://epic.org/privacy/cybersecurity/vep/.
[53] White House, Vulnerabilities Equities Policy and Process for the United States Government (2017), https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF.
[54] *Id*. at 4-5.
[55] GCHQ, *The Equities Process,* GCHQ.gov (Nov. 29, 2018), https://www.gchq.gov.uk/features/equities-process.

33. Government hacking incentivizes weaker technological safeguards.

34. An expert report from the U.S. proposed clear safeguards to protect public safety and manage the risks of government hacking operations.

35. EPIC respectfully urges the Court to consider these general principles in reviewing UK government hacking authorities against the standards of the Convention.

February 27, 2019

Respectfully submitted:

Marc Rotenberg, Executive Director
Alan J. Butler, Senior Counsel
Eleni Kyriakides, International Counsel
Electronic Privacy Information Center (EPIC)
1718 Connecticut Avenue, NW
Suite 200
Washington, DC 20009
USA
+1 (202) 483-1140