In the European Court of Human Rights
Application No. 46259/16

BETWEEN:-

Privacy International and others

Applicant

v.

the United Kingdom

Respondent Government

THIRD-PARTY INTERVENTION

ARTICLE 19: Global Campaign for Free Expression and The Electronic Frontier Foundation

---

I. Introduction

1. This third-party intervention is submitted on behalf of ARTICLE 19: Global Campaign for Free Expression (ARTICLE 19) and the Electronic Frontier Foundation (EFF, jointly Interveners).

2. ARTICLE 19 is an independent human rights organisation that works around the world to protect and promote the right to freedom of expression and the right to freedom of information. ARTICLE 19 monitors threats to freedom of expression in different regions of the world, as well as national and global trends and develops long-term strategies to address them and advocates for the implementation of the highest standards of freedom of expression, nationally and globally.

3. The Electronic Frontier Foundation is a non-profit legal and policy organization that safeguards freedom of expression and privacy in the digital world. EFF regularly files amicus curiae or intervener briefs in court cases of consequence regarding freedom of expression. Drawing on the expertise of its attorneys and staff technologists, EFF's briefs seek to educate courts about Internet technologies and the broader consequences of laws and decisions affecting those technologies.

4. The Interveners welcome the opportunity to intervene as third parties in this case, by the leave of the President of the Court, which was granted on 15 July 2019 pursuant to Rule 44 (3) of the Rules of Court. These submissions do not address the facts or merits of the applicant's case.

5. The Interveners believe that this case provides the Court with the opportunity to rule for the first time on the compatibility of government interference with computer systems or equipment – colloquially known as "government hacking" – with the rights to privacy and freedom of expression. The UK is renowned for its intelligence capabilities and the way in which it regulates surveillance is often replicated around the world. Hence, the present case will set an important precedent on the developing standards of surveillance at the international, regional and domestic levels. In these submissions, the Interveners address the following:

   (i) the various known forms of government equipment interference techniques, especially the range of equipment interference tools available to the Government of the United Kingdom (the UK) and technical issues arising from their use; and

   (ii) the impact of equipment interference on fundamental human rights, in particular the rights to freedom of expression and privacy, most notably, through analysis of the "chilling effect" of the equipment interference on fundamental rights.

II. Equipment interference techniques

a) Defining features of "equipment interference"

6. Equipment interference (EI), also known as computer network exploitation (CNE), covers a range of techniques that may be used to obtain communications, equipment data or other information from equipment (software, data, a computer system, network, or other electronic device) without the permission of the person or organisations responsible for that equipment.[1] EI can be carried out remotely or through physical interaction with the equipment in question. The complexity of EI operations varies: it encompasses a broad array of activities and methods. It can involve situations where physical access or access credentials are required, such as covertly downloading data from a subject's mobile device when it is left unattended, or using someone's login credentials to gain access to data held on a computer (including names and IP addresses as well as sensitive information such as the location, age, gender, marital status, income, ethnicity, sexual orientation, education and family of the user.)[2] On a more technologically complex level, it may involve exploiting existing vulnerabilities in software to gain control of devices or networks to remotely extract material or monitor the user of the device.[3] Recent government hacking conducted in the USA by the Federal Bureau of Information (FBI) is an apt illustration of the vast reach of EI.[4] The FBI used a controversial form of malware that named a "Network Investigative Technique," relying on a single U.S. warrant, allowing the FBI to hack over 87,000 computers

[1] See, e.g. Center for Internet and Society, Security Risks of Government Hacking, September 2018; Access Now, A Human Rights Response to Government Hacking, September 2016.
[2] See Home Office, Equipment Interference: Draft Code of Practice, December 2017.
[3] *Ibid.*
[4] The FBI used this technique to identify visitors to the child pornography website Playpen, being accessed through the Tor network, which protects the anonymity of browsers. See e.g. M. Rumold, Playpen: the Story of the FBI's Unprecedented and Illegal hacking Operation, EFF Deeplinks Blog, 15 September 2016.

in 120 countries and territories.[5] To date, the FBI still has not revealed the full technical details of how the Network Investigative Technique operated. Court filings reveal that it relied on a vulnerability in the Tor Browser, a widely used tool for preserving anonymity during web browsing, which allowed the FBI to remotely execute a payload that sent details about target computers back to the government. However, in certain cases, the U.S. Department of Justice has opted to dismiss criminal prosecutions where defence counsel has sought further details of the technique.[6]

7. The nature and scale of EI renders it a "far more intrusive" tool than any other "single surveillance technique currently deployed by the intelligence services."[7] Thus, by virtue of its defining characteristic, government hacking or EI can be distinguished from other existing forms of surveillance technology due to the ability of governments to utilize this power "remotely, surreptitiously, across jurisdictions, and at scale."[8] Further, because "a single hack can target many people, even those who are incidental or unrelated to a government investigation or operation,"[9] the use of EI implicates the rights to privacy, freedom of speech, and other human rights of individuals on a much greater scale than a traditional law enforcement investigation.

b) EI techniques available to the UK Government

8. There are several "creative and ever-evolving methods" to obtain different types of information.[10] Many intelligence or law enforcement agencies deploy malware, a "specialized software that allows whoever deploys it to take control of or extract information from a target device."[11] Depending on what function the malware has been coded to perform, it can enable law enforcement agencies to record a large and diverse quantity of information such as logging every key-stroke that a user types, turning on microphones and cameras to capture video and audio from the room that the device is in, monitoring every website that a user visits including seeing the personal contents of email and other online communications, accessing all files stored on the device, and obtaining information to ascertain the owner of a device. Further, malware often relies on known vulnerabilities within products and software, and when these vulnerabilities are fixed attackers will move on to a new exploit. The most common techniques through which malware can be deployed and that may be used by governments, depending on circumstances and technological details, include the following:[12]

    - Social engineering or "phishing," which involves sending an email or other message to the target (usually impersonating someone with whom the target is

[5] Privacy International, Privacy International's Work on Hacking, 10 February 2017.
[6] M. Nunez, BI Drops All Charges in Child Porn Case to Keep Sketchy Spying Methods Secret, Gizmodo, 6 March 2017.
[7] Privacy International & Open Rights Group, Draft Equipment Interference Code of Practice Submission, 20 March 2015.
[8] Privacy International, Written Submissions in *Association Confraternelle De La Presse Judicaire and 11 Other Applications v. France*, December 2017, para 12.
[9] *Ibid.*
[10] Draft Code of Practice, *op.cit.*
[11] *Ibid.*
[12] *C.f. e.g.* Privacy International & Open Rights Group, *op.cit.*

familiar or a trusted person) that contains a link or attachment infected with malware;[13]

- "Watering hole" attack, which facilitates the deployment of malware on a target's device (and on devices belonging to non-targets) without their awareness that any software is being downloaded or installed, typically by "installing custom code on a website that will infect with malware any device that visits that website;"[14]

- "Man in the middle attack," (or "machine in the middle attack"), which may use an Internet service provider to deploy malware in the course of a target's access to an unrelated and uninvolved site or service. As a result, "the attack interrupts or gets in the middle of a request by the target device to access internet content." This form of attack can also involve modifications to software as it is being downloaded by the target.[15]

- Direct remote access attack, involving the takeover or search of a target device by communicating with it directly, without any kind of intermediation by a web site or download;

- "Supply-chain attack," which targets a third-party in order to ultimately access information on the target device or account. This could involve hacking a software developer or publisher, compelling a software developer or publisher to publish malware, or physically intercepting devices that are being manufactured or shipped in order to infect those devices with malware;

- Surreptitious access or surreptitious entry attacks, involving physical access to devices themselves. This physical access could occur during law enforcement's search of a home or office, and could involve planting physical bugs inside the device or taking advantage of physical access to tamper with the software installed on it.[16]

9. There is a lack of transparency about the EI/CNE programmes in use by the UK intelligence services. Some information is available from the Snowden surveillance files; these include:

[13] An example of a successful and highly disruptive phishing attack is outlined in the U.S. indictment of 12 Russian military intelligence agents accused of obtaining the contents of emails belonging to officials of a national political party during the 2016 U.S. presidential election; Indictment, *US v. Viktor Borisovich Netyksho, et. al.*, Case No. 1:18-cr-00215-ABJ, D.D.C., 13 July 2018.

[14] The FBI used this type of attack to deploy the "Network Investigative Technique" in the Playpen cases; M. Rumold, Playpen, *op.cit.*

[15] This sort of attack is evidenced by CitizenLab's report of the use of Deep Packet Inspection devices to deliver nation-state malware in Turkey and in Syria. Users who attempted to download Microsoft Windows applications from official vendor websites, including Avast Antivirus, CCleaner, Opera, and 7-Zip, were silently redirected to malicious versions because they visited unsecured HTTP web links rather than the secure HTTPS versions. Attackers were able to exploit the unsecured HTTP link and redirect users to the malware. B. Marczak, et. al., Bad Traffic: Sandvine's PacketLogic Devices Used to Deploy Government Spyware in Turkey and Redirect Egyptian Users to Affiliate Ads?, CitizenLab, 9 March 2018.

[16] See, e.g., *United States v. Scarfo*, 180 F. Supp. 2d. 572 (D.N.J. 2001), describing FBI use of a keylogger installed through surreptitious entry.

- CAPTIVATEAUDIENCE, which is "used to take over a targeted computer's microphone and record conversations taking place near the device;"

- GUMFISH, which "covertly takes over a computer's webcam and takes photographs;"

- FOGGYBOTTOM, which "records logs of internet browsing histories, collecting login details and passwords for email accounts;" and

- SALVAGERABBIT, which "copies data from removable flash drives that connect to an infected computer." [17]

10. In addition, the Snowden surveillance files also disclose that the Government Communications Headquarters (GCHQ) has "developed extensive means of manipulating mobile devices – in particular iPhone and Android devices."[18] These "tools" permit the following: (i) "activation of a microphone and the taking of recordings without the user's consent," (ii) "precise identification of the geographical whereabouts of the user," (iii) "retrieval of any content from the phone," and (iv) "the avoidance of detection that the device has been compromised."[19]

11. While these methods are not explicitly mentioned in the UK's Investigatory Powers Act (IPA) 2016, the use of ambiguous terms such as "interference" and "interception" in the IPA 2016 itself leaves unclear whether the aforementioned pervasive means of EI (such as surreptitious entry or otherwise) are employed at present by UK law enforcement or intelligence agencies. Since the IPA 2016 "provides absolutely no detail as to the specific means and methods employed by security agencies in the course of Internet surveillance." [20] The Interveners submit that this ambiguity enhances the scope for abuse.

12. The concerns over transparency of the EI techniques employed by the UK Government can be highlighted by the comparison to the Computer Crime III Bill (the Dutch Bill) of the Netherlands. The Dutch Bill allows law enforcement agencies to "use a vulnerability in the IT system," "enter/intrude using a false identity or by brute force," or "use a Trojan to infect the device with malware."[21] This, therefore, permits Dutch authorities to undertake online searches, "including looking at the data and securing the data," intercepting "private information (streaming data), including capturing key strokes (including passwords) and real-time monitoring of data traffic (which may or may not include encryption)," "influence the data, by adjusting settings, turning on webcams/microphones, sabotaging or turning a device off," and deleting data.[22] While these are wide-ranging powers, the legality of which may be subject to challenge, the Dutch Bill serves as an interesting standard of comparison with the UK legislation on EI

[17] See, e.g. Liberty, Response to the Home Office Consultation on the Equipment Interference Code of Practice, March 2015, para 8.
[18] *Ibid.*, para 8(e).
[19] *Ibid.*
[20] Draft Code of Practice, *op.cit.*
[21] See, e.g. European Parliament, Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, Study for the LIBE Committee, 2017.
[22] *Ibid.*

because of its relative transparency. The scarce availability of information on the methods being employed by the UK law enforcement agencies inevitably culminates in grave transparency concerns,[23] particularly vis-à-vis the scope of abuse.

13. Taking into consideration the information gap, discussed above, it is respectfully submitted that the ambiguity surrounding the UK Government's use of EI tools, including on the specific techniques utilized by law enforcement or intelligence personnel, is severely problematic.

III. The impact of EI techniques on fundamental human rights

a) Impact of the use of EI techniques on privacy and freedom of expression

14. There are several privacy and freedom of expression related concerns stemming from the use of EI techniques by governments across the globe. These apply to the UK, exacerbated by the lack of transparency over the techniques used by the UK intelligence services**.** These wide-ranging implications for privacy have been acknowledged by the UN High Commissioner for Human Rights, in his 2014 report in which he highlighted that "any capture of communications data is potentially an interference with privacy and, further, that the collection and retention of communications data amounts to an interference with privacy whether or not those data are subsequently consulted or used. Even the mere possibility of communications information being captured creates an interference with privacy, with a potential chilling effect on rights, including those to free expression and association."[24]

15. The Special Rapporteur on freedom of opinion and expression expressed similar concerns in his 2016 report, in which he states that "surveillance may create a chilling effect on the online expression of ordinary citizens, who may self-censor for fear of being constantly tracked. Surveillance exerts a disproportionate impact on the freedom of expression of a wide range of vulnerable groups, including racial, religious, ethnic, gender and sexual minorities, members of certain political parties, civil society, human rights defenders, professionals such as journalists, lawyers and trade unionists, victims of violence and abuse, and children." [25] In other words, "those with a legitimate and lawful interest in expressing dissent may feel watched or monitored to such an extent that they are deterred from attending protests and other gatherings, again emphasising the disproportionate impact of bulk powers."[26]

16. Due to the very nature of EI techniques, privacy and freedom of expression incursions are a very real threat not just for a particular target or user but potentially for an entire group, family or community.[27] Since EI tools are inherently "designed

[23] *Ibid.*
[24] Report of the Office of the UN High Commissioner for Human Rights, A/HRC/27/37, 30 June 2014, para 20.
[25] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/32/38, 11 May 2016.
[26] Liberty, Response to the Home Office, *op.cit.*, p. 4.
[27] International Federation of Library Associations and Institutions, The right to privacy in the digital age, 12 March 2015, p. 1.

to allow an unauthorized person to control another's computer," a "security hole" is created, which is subject to exploitation by any individual or organization with relevant technical expertise.[28] Resultantly, all "passwords, encryption keys and personal files can be collected and copied, either to further other intelligence aims or for a criminal purpose, depending on who has found the vulnerability in the target's system."[29]

17. In this regard, the Interveners highlight that the UN Special Rapporteur on freedom of expression has emphasized the "extremely disturbing" impact of these forms of surveillance technology: "Offensive intrusion software such as Trojans… constitute such serious challenges to traditional notions of surveillance that they cannot be reconciled with existing laws on surveillance and access to private information. These are not just new methods for conducting surveillance; they are new forms of surveillance."[30] The Interveners share the concerns expressed by the Special Rapporteur, particularly with regard to threats to privacy and procedural fairness rights, in the context of the use of evidence obtained through the use of EI techniques, in legal proceedings.[31] The potential for intentional alteration of data, which raises concerns vis-à-vis the "integrity of evidence obtained from the target device," enhances the scope for violations of the right to fair trial (as guaranteed by Article 6 of the European Convention on Human Rights), for instance where "covert modifications of the system and the planting of data and network logs could lead to misrepresentations of activity and perversions of justice."[32]

18. Several reports show that the use of EI techniques severely impede the ability of journalists to conduct research and investigations, and to publish their work to specific or general audiences or lead to self-censorship.[33] This can then inhibit the important functions that the media plays in maintaining transparency and accountability of the State.[34] For example:

    - In 2016, researcher Elizabeth Stoycheff published an influential study on the impact on government surveillance on social media users. [35] Those participating in the study were informed of NSA monitoring and shown a fictional Facebook post regarding U.S. airstrikes against ISIS, after which they were asked about their willingness to comment, share and like the post, or create a new post about the same topic. They were also questioned on whether they supported or opposed U.S. airstrikes, what they thought most other Americans believed about the airstrikes, and whether surveillance is necessary for national security. The study concluded that "the government's online

[28] Privacy International & Open Rights Group submission, *op.cit.*
[29] *Ibid.*
[30] Report of the Special rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, A/HRC/23/40, 17 April 2013, para 62.
[31] *Ibid.*
[32] Privacy International & Open Rights Group submission, *op.cit.*
[33] See, e.g. Privacy International, Two sides of the same coin – the right to privacy and freedom of expression, 2 February 2018; or Association for Progressive Communications, The right to freedom of expression and the use of encryption and anonymity in digital communications, Submission to the UN Special Rapporteur on the Right to Freedom of Opinion and Expression, February 2015, p. 11.
[34] *C.f.* Privacy International, Two sides of the same coin, *op.cit.*
[35] E. Stoycheff, Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of the NSA Internet Monitoring, Journal of Mass Communication Quarterly, 93(2), 296-311.

surveillance programs may threaten the disclosure of minority views and contribute to the reinforcement of majority opinion."[36]

- Similar conclusions were made in the CitizensLab report about Ahmed Mansoor, an internationally recognized human rights defender residing in the United Arab Emirates, who was targeted through Pegasus in 2016.[37]

- A 2018 Report by The Citizen Lab documented the use of Pegasus spyware against journalists and civic media in the UK, Mexico and Canada, in which it confirmed the targeting of at least eight Mexican journalists through the use of Pegasus.[38] In some cases, targets also included family members, such as the case of a journalist Carmen Aristegui, whose minor child was targeted while at boarding school in the USA.[39] Journalists quoted in the report claimed that once journalists and their sources realized they could be listened to without their knowledge, this would lead to self-censorship.[40] Hence the Report concluded that the use of Pegasus and other spyware to target journalists has had a chilling effect on reporting, grounded in fears that activities may be monitored."[41]

- Notably, Pegasus' spyware was reportedly used by Saudi Arabia to track Jamal Khashoggi;[42] and after his brutal murder, it was revealed that one of his associates, a Saudi dissident based in Canada, had Pegasus malware installed on his cell-phone.[43]

- In 2018, EFF and Lookout published a report uncovering a global malware espionage campaign that targeted military personnel, activists, journalists, and lawyers.[44] Through a phishing email, the campaign encouraged people to visit a fake app-store and download fake versions of Signal and WhatsApp carrying malware to Android phones. The research revealed that the Lebanese General Directorate of General Security (GDGS) may have been behind the attack, and that the attack obtained "hundreds of gigabytes of data exfiltrated from thousands of victims, spanning 21+ countries in North America, Europe, the Middle East, and Asia." Further, the attack used FinFisher/FinSpy malware, software that is developed by the British company the Gamma Group, and sold

---

[36] *Ibid.*
[37] *See, e.g.* Citizen Lab, The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender, August 2016.
[38] Pegasus refers to a "sophisticated tool for spying on mobile phones": it is "designed to allow an operator to monitor targets' iPhone or Android devices". In fact, "Pegasus allows an operator to read text messages (including encrypted messages), examine photos, and track a phone's location," in addition to its ability to "silently enable microphones and cameras." While Pegasus "is exclusively sold to governments for the purposes of fighting terror and investigating crime," its use demonstrates that it is actively misused "by repressive governments to spy on human rights defenders, journalists and others who they may deem as threats to their power." See The Citizen Lab, Reckless VI, 27 November 2018.
[39] *Ibid.*
[40] *Ibid.*
[41] *Ibid.*
[42] *C.f.* Amnesty International, Israel: Amnesty and New York University in legal action to prevent spyware attacks, 13 May 2019; or CNN, How a hacked phone may have led killers to Khashoggi, 20 January 2019.
[43] See, e.g. Al Jazeera, Targeted by a Text: Investigating how an Israeli cyber-weapons technology is being used by governments to spy on civilians. 14 May 2019; B. Marczak, et. al., The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil, The Citizen Lab, 1 October 2018.
[44] EFF & Lookout, Dark Caracal: Cyber-espionage at a Global Scale, January 2018.

to law enforcement and intelligence around the world, including Turkmenistan, Brunei, and Bahrain.[45]

- In March 2019, the CitizensLab, ARTICLE 19 Mexico and Central America, and Mexican digital rights group R3D published the report documenting that Griselda Triana, a journalist and the wife of a murdered journalist Javier Valdez, was targeted with Pegasus spyware following his assassination in 2017. The report concluded that this was a part of official abuse by the Mexican Government and raised concerns about this pattern in relation to Mexican journalists were also frequent targets of physical violence and killings.[46]

19. Additionally, the chilling effect of the use of surveillance was demonstrated by the 2016 study, published in the Berkeley Technology Law Journal, that found a dramatic fall in monthly traffic to Wikipedia articles about terror groups and their techniques after the June 2013 disclosures of the U.S. domestic surveillance program by Edward Snowden.[47] The study looked at 48 Wikipedia articles that contained terrorism-related keywords and found that article views dropped by 30 percent after June 2013, which supports "the existence of an immediate and substantial chilling effect."[48]

b) Other Impact of EI techniques

20. The wide-reaching nature of EI techniques can have a particularly severe impact on groups at risk of discrimination, such as LGBTQI activists in countries where homosexuality is criminalised."[49] The victims of various forms of violence and abuse may be reluctant to report for fear of double victimization.[50] The impact of such equipment interference thus is not limited to the rights to privacy and freedom of expression but may also extend to impact the right to life, the right to equality and non-discrimination and other rights.

21. Other professions directly affected by equipment interference by the Government can be lawyers, who not only have a professional responsibility to maintain the confidentiality of information related to their clients but who also rely on the ability to exchange information freely with their clients in order to build trust and develop legal strategy. For example, the 2014 report of Human Rights Watch, which conducted interviews with 42 lawyers, confirmed that "as with journalists, lawyers increasingly feel under pressure to adopt strategies to avoid leaving a digital trail that could be monitored; some use burner phones, others seek out technologies they feel may be more secure, and others reported traveling more for in-person meetings."[51] The inevitable result of this is "the erosion of the right to counsel,"

[45] N. Perlroth, Software Meant to Fight Crime is Used to Spy on Dissidents, NY Times, 30 August 2012.
[46] See, e.g. CitizensLab, Reckless VIIWife of Journalist Slain in Cartel-Linked Killing Targeted with NSO Group's Spyware, 20 March 2019.
[47] J. Penney, Chilling Effects: Online Surveillance and Wikipedia Use, Berkeley Technology Law Journal, Vol. 31, No. 1, 2016, p. 117.
[48] *Ibid.*
[49] Global Information Society Watch, The Harms of Surveillance to Privacy, Expression and Association, 2014.
[50] 2016 Report of the Special Rapporteur on freedom of expression, *op.cit.*, para 24.
[51] Human Rights Watch, With Liberty to Monitor All, 28 July 2014.

which serves as a fundamental component of the right to a fair trial and due process, guaranteed in international, regional and domestic standards.[52]

22. The evidence also shows that even when the EI techniques are used against those engaged in criminal behavior, they are often disproportionate to stopping legitimate threats, resulting in unpatched software for millions of innocent users, overbroad surveillance, and other collateral effects.[53]

23. Importantly, it has been also documented that governments "stockpile" vulnerabilities found in computers and software for future exploitation.[54] Discoverers may sell the vulnerabilities they find to multiple buyers, and sometimes even multiple agencies within a single government.[55] Not only does this undermine the security of the device being exploited but the practice of "sitting on" zero-day exploits by governments rather than taking steps to fix and reduce the harm of those exploits can potentially damage the security of the Internet as a whole. Governments should not assume that they are the only ones who possess knowledge of a vulnerability, because in practice a single vulnerability may be exploited by malicious third parties, ranging from nation-state adversaries to simple thieves.

IV. Conclusion

24. The application of various EI techniques represents one of the greatest threats to fundamental rights in the digital age and has a real "chilling effect" on the rights to privacy and freedom of expression as well as other rights. The Interveners therefore suggest that the Court should carefully consider the technical implications of government use of these techniques on human rights, particularly in the absence of sufficient safeguards.

16 September 2019

Barbora Bukovska
Senior Director for Law and Policy
ARTICLE 19

Andrew Crocker
Senior Staff Attorney
Electronic Frontier Foundation

[52] *Ibid.*
[53] EFF, What to Do About Lawless Government Hacking and the Weakening of Digital Security, 1 August 2016.
[54] A. Greenberg, Former NSA Chief Defends Stockpiling Software Flaws for Spying, Wired, 7 May 2014.
[55] *Ibid.*