**App No. 46259/16**

**IN THE EUROPEAN COURT OF HUMAN RIGHTS**

**BETWEEN:**

| | |
|---|---|
| **PRIVACY INTERNATIONAL**<br>**AND OTHERS** | **Applicant** |
| **- v -** | |
| **THE UNITED KINGDOM** | **Respondent** |
| **MOZILLA CORPORATION** | **Third Party Intervener** |

# WRITTEN COMMENTS OF THIRD PARTY INTERVENER MOZILLA

## Preliminary

1. Mozilla Corporation ("Mozilla") submits these written comments pursuant to leave to intervene in Privacy Intl. v. UK, in support of the applicants' argument that the UK's legal framework for computer network exploitation ("CNE") breaches Articles 8 and 10 of the European Convention on Human Rights. Leave to intervene is granted by the Court by letter of 29 March 2019 and discontinuance of the adjournment of the proceedings by letter of 15 July 2019.
2. Mozilla is a wholly-owned subsidiary of the nonprofit Mozilla Foundation, based in the United States. Mozilla's mission is to ensure that the Internet is a global public resource, open and accessible to all. Today, hundreds of millions of people worldwide use Mozilla's openly developed, free and open source web browser, Firefox, to discover, experience, and connect to the web on computers, tablets, and mobile phones.
3. As the producer of one of the world's most popular web browsers, it is essential for Mozilla that vulnerabilities in Firefox are quickly identified and fixed; the integrity of our product, and the privacy, safety and security of our users depend on it.
4. CNE carried out by state agencies such as GCHQ can significantly intrude upon the privacy of the CNE's targets, and of people networked with them. As this and other courts have noted in the past, interference with privacy will often also chill freedom of expression and access to information. Mozilla, which is grateful to the Court for its permission to intervene in this case, does

not seek to expand on these points, as they are likely to be core to the Applicants' case.

5. Instead, Mozilla seeks to bring its experience with security and privacy to bear in this submission, to demonstrate to the Court other less immediate but no less significant harms—to the security and related privacy interests of wider society—that are created or perpetuated by governments pursuing CNE capabilities. Those risks are particularly acute due to CNE's inherent reliance on undisclosed vulnerabilities. A government's pursuit of CNE opportunities (whether targeted or bulk) relies on seeking out and secretly preserving software vulnerabilities.
6. Those vulnerabilities constitute impaired security in what is often very widely-used software. If left unfixed, such vulnerabilities are susceptible to exploitation by cybercriminals and other bad actors, putting at risk the privacy of communications and information of the people thereby affected.
7. Because of the dependency on vulnerabilities remaining secret, CNE as a tool of modern law enforcement and intelligence agencies carries unique risks to privacy and freedom of expression of wider society.

## **Background**

8. CNE relies on the covert discovery or introduction of vulnerabilities in software, computers, networks, or other systems. A vulnerability might, for example, allow a third party to send commands to a device telling it what to run, and enabling the third party to gain total control of the computer. The third party might be able to see what the user is doing, access all data on the computer, and even turn on the computer’s camera or microphone to watch and listen to the user. These vulnerabilities—and their concealment—can be exploited for state intelligence-gathering to obtain data or information, or for disruptive purposes; they can also be exploited by cybercriminals and malicious third parties.
9. Governments often have unique knowledge of vulnerabilities, and learn about vulnerabilities in many ways: through their own research and development, by purchasing them, through intelligence work, or by reports from third parties. Not only will they will often delay disclosure in order to support intelligence-gathering and government hacking, but many governments are believed to

make significant investment in the discovery, acquisition and “stockpiling” of software vulnerabilities, for intelligence purposes.

## Summary

10. Mozilla believes that individuals’ security and privacy on the internet are fundamental and must not be treated as optional. To this end, we believe further that governments can and should contribute to establishing greater cybersecurity for their citizens and their country’s businesses and organizations, and even for themselves. Yet state CNE significantly contributes to the prevalence of online technology vulnerabilities that are ripe for exploitation by cybercriminals and other bad actors and can result in serious privacy and security risks, and serious damage to citizens, enterprises, public services, and governments. As an advocate for individuals’ security, privacy, and freedom of expression and access to information online, Mozilla is concerned that CNE severely harms those fundamental interests. As a technology company that offers products impacted by CNE, Mozilla is further concerned that the use of CNE will violate the integrity of its products and harm its relationship with users. Mozilla exhorts governments, including the UK government, to minimize their use of CNE and to adopt robust vulnerability disclosure processes, thereby minimising interferences with individuals' fundamental rights perpetrated by others.

## State CNE puts individuals at risk by weakening device and internet security

11. Mozilla is profoundly concerned by the harmful impact of state CNE on end-user security and its inherent corollaries, privacy and freedom of expression and access to information online; as well as on the integrity of the Internet-connected infrastructure on which society has come to rely.

### *The risks inherent in CNE are far-reaching*

12. By its nature, CNE will almost always affect more than the intended targets. CNE relies on vulnerabilities that potentially affect all users of a service or software, even if the CNE is intended for only a small number of individuals. In the case of widely used software, a CNE vulnerability stands to impact an enormous number of individuals. A vulnerability that affects Firefox, for example, could see the privacy and security of hundreds of millions of innocent people incidentally compromised, regardless of the intended scope of

the government's "exploit" (*i.e.,* a tool that takes advantage of the vulnerability for CNE purposes; also referred to herein as a "CNE tool"). The same is true for other broadly used software or hardware, whether browsers, operating systems, mobile phones, or the routers that send Internet traffic across the web.

13. This problem is compounded by ever-increasing device connectivity. As the "internet of things" expands, so does the potential use and impact of CNE. With the growth of smart cities, connected cars and connected homes, the reach of CNE and its associated risks increases correspondingly.

14. Furthermore, there is no practical way to guarantee that a vulnerability is used only within or outside certain jurisdictions. CNE may be directed to devices that are mobile or whose location cannot be reliably determined. In addition, the globalised nature of the Internet means that individuals in the UK frequently will be using services or storing material or data outside the UK. Moreover, software cannot be contained within one country's national borders.

*CNE can leave sensitive information, infrastructure and services open to abuse*

15. Not only is the scope of users affected by CNE vulnerabilities extremely broad; the information or systems that such vulnerabilities would permit access to are often extremely sensitive.

16. The current UK Equipment Interference Code of Practice gives examples of the kinds of information to which use of CNE could allow access: "*every keystroke entered by users*"; passwords; photographs; the location of meetings in calendar appointments; the content, sender and recipient of stored emails; and video surveillance footage.[1] That list will only increase as more and more devices are network-enabled.

17. As public and private infrastructure and services are increasingly managed remotely or accessed via the internet, web browsers such as Firefox assume an increasingly important role in ensuring secure, encrypted interactions with such systems. At the same time, because they act as gateways to highly private, sensitive or important online services such as email, healthcare networks, banking, and social security services, major web browsers such as

[1] UK Home Office, *Equipment Interference Code of Practice* (March 2018); available online at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf

Firefox, Google Chrome and Microsoft Edge can be attractive targets for state-sponsored CNE.

18. While such sensitive information, infrastructure and services may be the deliberate target of government CNE, they can logically also be accessed or interfered with by anyone else with knowledge of that same vulnerability (or even possession of the government's own CNE tools)—for example, cybercriminals and other malicious actors.

19. Indeed, a government puts its own systems and information at risk when it invests in CNE capabilities. This is borne out by examples of leaked exploits being used to attack government systems. (See below.)

*Software vulnerabilities and CNE exploits cannot be contained and are likely to come to light*

20. CNE tools rely on underlying vulnerabilities in the device or software code. These vulnerabilities as well as the related CNE tools can be (and are regularly) discovered and exploited by bad actors, and a government cannot guarantee that a vulnerability and associated exploit will remain known only to the government.

21. Assertions that risks to broader users can be limited by ensuring a vulnerability is never known outside the intelligence or law enforcement agencies using that vulnerability have been shown to be unrealistic and essentially impossible, even for the most well-resourced intelligence agencies.

22. Vulnerabilities used for CNE are typically revealed as a result of accidental release by or theft from government, or through independent discovery. The likelihood that any vulnerability ultimately will be revealed—with all the consequent security risks of disclosure—appears to be relatively high.

*Government release*

23. While for obvious reasons data is not available about government success rates in effectively securing CNE tools and related vulnerabilities, there have been multiple examples in recent years of these tools being inadvertently released in different ways. Government error has resulted in tools being left on public servers.[2] Exploits have been stolen from government servers.[3] In

[2] See, for example, https://www.reuters.com/article/us-cyber-nsa-tools-idUSKCN11S2MF

[3] See, for example, https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/; https://arstechnica.com/tech-policy/2018/09/nsa-employee-who-brought-hacking-tools-home-sentenced-to-66-months-in-prison/; and

some cases, exploits have been exposed by way of their use, for example by logging some action in a network file.[4]

*Independent discovery*

24. Vulnerabilities are also found through independent discovery, and research indicates that the rate of discovery may be fairly high. One study that looked at rate of rediscovery for software vulnerabilities (*i.e.*, the likelihood that two parties will independently discover the same vulnerability) estimated rediscovery at between 10 and 15 percent of the time, averaged across software sources.[5] This predicts that, for example, a vulnerability undisclosed by a state intelligence agency will be rediscovered up to 15% of the time (or more, depending on the software)—a high risk indeed, especially for products in use by tens or hundreds of millions of people.

25. This may be due in part to the wide range of groups, independent of software and hardware companies, that drive efforts to find these vulnerabilities and exploits.

    - Other states will often seek to add to their own CNE arsenals;
    - Governments, universities and other organizations frequently fund security research efforts, such as audits of widely used software.  The European Commission, for example, operates a large "bug bounty" program as part of the EU-FOSSA 2 project.[6]
    - There is a thriving shadowy market in the sale or licensing of such exploits to different audiences, such as criminal or hacker groups that might use a vulnerability for illicit purposes.

26. The more popular and important software becomes, the more likely there will be independent discovery of vulnerabilities in that software, given concentration of efforts on "high value" targets. In addition, vulnerabilities in "open source" software (*i.e.*, for which the software source code is publicly available and open for inspection by all), such as Firefox, may be even more likely to come out through independent discovery.

https://www.theregister.co.uk/2017/04/14/latest_shadow_brokers_data_dump/.

[4] See, for example, https://www.theregister.co.uk/2019/05/07/equation_group_tools/

[5]https://www.belfercenter.org/sites/default/files/files/publication/Vulnerability%20Rediscovery%20%28belfer-revision%29.pdf

[6] https://ec.europa.eu/digital-single-market/en/news/eu-bug-bounty-programme-open-source-software-gives-awards-eur-25000

*When a vulnerability or exploit is publicly revealed without notice to the affected developer or vendor, security risks increase exponentially*

27. When details of a CNE tool and/or the underlying vulnerability become public, the risk to users' privacy and security as well as the integrity of government and business operations increases dramatically. Companies face a race against time to fix their products before publicly known vulnerabilities are used by malicious actors to attack the broader user base.

28. WannaCry, a worldwide ransomware attack that broke in 2017, is a prominent example of the real harm that can occur when a government withholds disclosure of a vulnerability in order to exploit it for intelligence purposes. The attack made use of a stolen CNE tool leaked over a month earlier that was believed to have been developed by the U.S. National Security Agency based on a vulnerability in Microsoft Windows systems.[7] It is estimated to have had over 200,000 victims in 150 countries in the first weekend of its existence[8]—including National Health Service hospitals across England and Scotland, and the Russian Interior Ministry, among others[9]—and continues to cause damage even today. The leaked exploit was later used by the Russian government, for example, in the so-called "NotPetya" attack, which was intended for Ukraine but ended up incapacitating some of the world's largest businesses, including Russia's itself.[10] And it was again used this past May in an attack on the U.S. city of Baltimore, infecting thousands of computers and shutting down or disrupting email services, health alerts, and more.[11] This example shows how efforts of even the most sophisticated and well-resourced governments of the world to hold knowledge of vulnerabilities and CNE tools in secret can result in substantial harm, including to members of the very regimes that harbor and develop them.

29. Another example of withheld knowledge about widely used software becoming inadvertently known, to the detriment of user security and privacy, involves the Firefox open codebase, which Mozilla believes may have been the target of intrusive state CNE activity. The Firefox codebase is regularly

[7] https://arstechnica.com/information-technology/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet/

[8] https://www.abc.net.au/news/2017-05-15/ransomware-attack-to-hit-victims-in-australia-government-says/8526346

[9] https://www.cbsnews.com/news/hospitals-across-britain-hit-by-ransomware-cyberattack/

[10] https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[11] https://www.nytimes.com/2019/05/25/us/nsa-hacking-tool-baltimore.html

reused and adapted for different products which include the Tor Browser, a web browser that allows anonymous browsing and has been promoted as a key tool for journalists and political dissidents living under oppressive regimes.[12] In November 2016 Mozilla became aware of an independently discovered Firefox vulnerability and related exploit allowing attackers to collect user IP and MAC addresses, thereby effectively deanonymizing users of Tor.[13] The fact that the exploit worked in essentially the same way as the "network investigative technique" used by the U.S. FBI to deanonymize Tor users[14] gave rise to speculation that it was created by a law enforcement agency.[15] Mozilla had limited time to fix the Firefox code before the vulnerability and exploit were publicly revealed and available for widespread nefarious use.

## State CNE in the UK lacks essential legal and procedural safeguards; despite this, its use is growing

### *If vulnerabilities are used by government, they must be subject to robust, accountable and transparent vulnerability disclosure policies*

30. Governments have an important role to play in ensuring that individuals can use the Internet safely and privately; and in ensuring that infrastructure now being connected to the Internet is secure against attack.
31. The best way for governments to ensure the greatest security and privacy for the greatest number of people is to immediately disclose vulnerabilities that they learn about to the affected vendors. Where the government nonetheless wants to delay disclosure of a vulnerability for operational purposes, such a decision should be subject to robust, accountable, and transparent policies.[16]
32. The UK has a process for reviewing vulnerabilities that it learns about,[17] but the process remains shrouded in secrecy and is flawed in several respects:

[12] https://www.csoonline.com/article/3287653/what-is-the-tor-browser-how-it-works-and-how-it-can-help-you-protect-your-identity-online.html

[13] https://blog.mozilla.org/security/2016/11/30/fixing-an-svg-animation-vulnerability/

[14] https://regmedia.co.uk/2016/03/29/alfin.pdf

[15] https://www.lawfareblog.com/fbis-firefox-exploit

[16] See for example Centre for European Policy Studies, *Software Vulnerability Disclosure In Europe* (June 2018); available at https://www.ceps.eu/ceps-publications/software-vulnerability-disclosure-europe-technology-policies-and-legal-challenges/.

[17] GCHQ Equities Process (November 2018 / March 2019), available at https://www.gchq.gov.uk/information/equities-process.

(1) It is subject to broad exceptions whereby many vulnerabilities are not considered for responsible disclosure at all, for example where GCHQ does not expect the software vendor to fix the vulnerability.[18] This neglects to consider that persons using the insecure software would have been able to replace it with something more secure, had they been informed.

(2) It is operated without sufficient transparency and accountability. In this vein, it is also not known whether the GCHQ equities process is subject to strict time limits, as is the case for the U.S. government's equivalent, the Vulnerabilities Equities Process (VEP).[19]

(3) It could have broader representation from other governmental and non-governmental entities, helping to ensure that potential negative consequences of CNE are fully (and fairly) considered.

*Increasing use of CNE techniques by government agencies*

33. Attention to the security risks and intrusion to privacy posed by CNE is especially important now, due to the UK government's reportedly increasing use of CNE.

34. UK intelligence agencies, such as GCHQ, have made significant efforts in recent years to develop their CNE capabilities. In its 2016-2017 annual report, the UK Parliament Intelligence and Security Committee noted "*very substantial*" increases in "*GCHQ's allocation of effort to developing offensive cyber capabilities*".[20] According to that report, GCHQ boasted of a "*wide spectrum of successes*" and that "*We… actually over-achieved and delivered [almost double the number of] capabilities [we were aiming for ***].*"[21] The subsequent 2017-2018 annual report noted that a "*Computer Network Exploitation Scaling programme to move GCHQ projects towards a focus on*

[18] *Ibid.* , "Exceptions" ("*There are certain limited circumstances where vulnerabilities may not be subject to the Equities Process. (...) A second example, is where the software in question is no longer supported by the vendor (...)*")

[19] See Annex B of the 2017 Unclassified Vulnerabilities Equities Policy and Process for the United States Government: https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF

[20] UK Intelligence and Security Committee, *Annual Report 2016-2017*, at [108]. Available online at http://isc.independent.gov.uk/committee-reports/annual-reports

[21] *Ibid.*

*operations that are conducted on the internet using computer network exploitation techniques*" was a "*major project*" for the agency.[22]

35. GCHQ also proposes increased use of bulk CNE, which as with targeted CNE, relies on finding and stockpiling vulnerabilities in software on which millions of people may rely. In December 2018, the UK Home Office reported that GCHQ now intended to "*conduct a higher proportion of ongoing overseas focused operational activity using the bulk [equipment interference] regime than was originally envisaged*",[23] even though when the Investigatory Powers Act 2016 was passed, GCHQ had maintained that bulk CNE would be used only on an exceptional basis.

## Conclusion

36. CNE techniques carry an inherent risk of collateral damage to innocent users. These risks cannot be underestimated: CNE relies on software vulnerabilities that typically allow access to very sensitive information and/or disruption of important systems on which individuals and society rely.
37. The underlying vulnerabilities frequently come to light without having been disclosed by government to the organisations responsible for the affected software or hardware, allowing for exploitation by malicious actors and even other governments,[24] and potentially causing significant harm to individuals and businesses and local or national governments, even to the point of crippling vital infrastructure.
38. For the security and privacy of individuals worldwide, it is therefore essential that governments minimize use of CNE, and ensure sound practices for disclosure.

**ABIGAIL PHILLIPS**

**Mozilla Corporation**

**13 September 2019**

[22] UK Intelligence and Security Committee, *Annual Report 2017-2018*, p 19. Available online at http://isc.independent.gov.uk/committee-reports/annual-reports

[23] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/761147/Letter_from_the_Security_Minister_to_Dominic_Grieve_QC_MP_December_2018.pdf

[24] https://www.washingtonpost.com/world/national-security/us-set-to-declare-north-korea-carried-out-massive-wannacry-cyber-attack/2017/12/18/509deb1c-e446-11e7-a65d-1ac0fd7f097e_story.html ; https://www.theguardian.com/technology/2018/feb/15/uk-blames-russia-notpetya-cyber-attack-ukraine.