1. New America's Open Technology Institute (OTI) is pleased to submit the following comments to the Draft Investigatory Powers Bill Joint Committee regarding the Draft Investigatory Powers Bill.[1] New America's Open Technology Institute ("OTI") is a program of New America dedicated to technology policy and technology development in support of digital rights, social justice, and universal access to open communications networks. OTI, through its unique blend of policy expertise, technical capacity, and field-level engagement, seeks to promote a stronger and more open Internet to support stronger and more open communities. Digital Fourth Amendment policy and law is a particular area of interest for OTI, and the Institute testifies before the United States Congress regularly on issues of digital privacy and surveillance. New America is a non-profit civic enterprise dedicated to the renewal of American politics, prosperity, and purpose in the digital age through big ideas, technological innovation, next generation politics, and creative engagement with broad audiences.

2. We believe the measures proposed could create significant risks to privacy, security, and innovation, and should be approached with caution. Our comments focus on the bill's consideration of computer and network exploitation (CNE) as a response to "the loss of intelligence that may no longer be obtained through other techniques, such as interception, as a result of sophisticated encryption."[2] We believe that if CNE is to be used, it must be limited, and should only be authorized – if at all – in narrow circumstances with strong protections. Further, we believe that certain measures under consideration – specifically, use of CNE for bulk collection and adding new vulnerabilities in software updates – should be completely prohibited.

I. Encryption is a net positive for security of both private data and the network as a whole.

3. Encryption is a vital resource that protects the information of individuals, corporations and governments from a variety of criminals and others who would do harm. It has done so for over thirty years. As the Open Technology Institute noted in a policy paper on the history of encryption, in the 1980's "commercial demand for encryption products exploded," and in 1991 PGP – a major

[1] Secretary for the Home Department, *Draft Investigatory Powers Bill* (November 2015), *available at* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473770/Draft_Investigatory_Powers_Bill.pdf, *hereafter*, *Draft Investigatory Powers Bill*.
[2] *Draft Investigatory Powers Bill*, 16.

practical tool for end-to-end public key encryption of files and e-mail that is still popular today – was publically released.[3]

4. As end-to-end encryption of electronic communications has been available to the public for the last quarter century, neither the technology nor the challenges law enforcement may face regarding interception are novel. The most significant shift regarding encryption in recent years has been its growing value for average individuals and ordinary businesses as more and more data is stored and transmitted digitally, which is an argument against rather than for government interference in the technology.[4] Given that encryption is an indispensable tool that is widely available to and used by law-abiding individuals, companies, governments, and non-governmental organizations across the world to protect their security in an increasingly hostile digital ecosystem, the Investigatory Powers Bill should explicitly disclaim any effort to prohibit or interfere with the development or use of encryption.[5]

II. Any use of CNE should be narrowly tailored and only used a means of last resort.

5. Considering the expanded use of encryption and other security features by a wider variety of people and entities, governments may seek new methods to obtain evidence that they believe they can obtain in no other way. The draft bill clearly considers CNE to be one appropriate course in the face of these challenges. However, because CNE raises unique concerns regarding security, privacy, and accountability that are even more serious than those raised by traditional methods of interception, CNE – if used at all – should be subject to the highest legal standards and strictest checks and balances.

6. CNE is a threat to privacy because it is generally accomplished through unilateral and surreptitious action. When police use interception techniques that involve compelled assistance from a company, there is an independent party with the ability to object to surveillance that is overbroad or improper. CNE has no such third-party check on its use. In addition, by virtue of granting access to devices or networks that can transmit or store absolutely massive amounts of data unlike anything available in the physical world, CNE has the potential to return extraordinary troves of highly personal data to authorities on an unprecedented scale. The Supreme Court of the United States recently had to tackle the privacy implications of mobile phones, and said that "cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person… They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders,

---

[3] Danielle Kehl et al, New America's Open Technology Institute, *Doomed to Repeat History? Lessons From the Crypto Wars of the 1990's* (June 2015), *available at* https://static.newamerica.org/attachments/3407-doomed-to-repeat-history-lessons-from-the-crypto-wars-of-the-1990s/OTI_Crypto_Wars_History.abe6caa19cbc40de842e01c28a028418.pdf.

[4] For a comprehensive review of OTI's arguments against government mandates regarding encryption, please see *Read This Before You Rail Against Encryption*, New America Weekly, Nov. 19, 2015, *available at* https://www.newamerica.org/weekly/read-this-before-you-rail-against-encryption/.

[5] Home Secretary Theresa May has stated that the bill "will not ban encryption or do anything to undermine the security of people's data.". *See*, The Associated Press, *Apple Boss Cook Says He'll Resist UK Government Spy Law Plan*, Nov 11, 2015, *available at* http://bigstory.ap.org/article/c176a081b3d9418e90aa788a52495fd7/apple-boss-cook-says-hell-resist-uk-government-spy-law-plan. However, some commentators fear that particular provisions of the bill would do just that. *See*, Alex Hern, The Guardian, *Tech Firms Warn Snooper's Charter Could End Strong Encryption in Britain*, Nov 9, 2015, *available at* http://www.theguardian.com/technology/2015/nov/09/tech-firms-snoopers-charter-end-strong-encryption-britain-ip-bill.

libraries, diaries, albums, televisions, maps, or newspapers."[6] Even our smallest devices contain huge amounts of personal data, yet the CNE contemplated in the bill would yield much more, authorizing access to much larger systems and networks used by countless ordinary people.

7. CNE also raises security concerns because it necessarily involves the use of some sort of vulnerability in the software of the target's device, software that may also be used by thousands or even millions of others. Unfortunately, vulnerabilities don't care who uses them. Any vulnerability used by government in compliance with the law can also be used by bad actors for malicious purposes, be they identity thieves, fraudsters, corporate spies, or foreign intelligence operatives. Government should be in the business of making networks and devices more secure, and telling software vendors about the vulnerabilities it knows of so that they can be patched. Frequent reliance on CNE would undermine its motivation to do so and thereby leave those widespread vulnerabilities open to malicious actors. Furthermore, if the security of the government's storage or transmission of such stockpiled vulnerabilities were compromised, the government's use of CNE could even alert criminals and spies to vulnerabilities of which they were previously unaware.

8. Because of all these concerns, OTI has previously concluded when commenting on this issue in the United States that with CNE, "we are faced with a digital surveillance technique that is substantially more invasive than the analog electronic surveillance techniques of the past."[7] If used at all, checks should exist to ensure that CNE is at most a measure of last resort, and that it does not become a commonly relied-upon investigative technique. CNE should therefore only be deployed with judicial authorization based on a strong factual showing, and only after the government has demonstrated that less intrusive means of obtaining the information have been exhausted. That authorization should also be coupled with strict time limits defining the duration of the surveillance and requiring minimization of data that is not responsive to the government's stated need as particularly described in the authorization.

9. Even with all of these checks, the use of CNE still carries a unique range of serious privacy and security risks that distinguish it from traditional surveillance and may make any use at all unreasonable. These risks include the privacy risk to non-suspects who share the target computer or network; the risk that the government's CNE software may spread to non-target computers or networks; the possibility, in cases of botnet investigations or so-called "watering hole" attacks, that thousands or even millions of computers may be infected; and the risk that the software used to remotely access any of those computers or networks may end up causing damage, either by altering or deleting data or creating brand new security vulnerabilities that may be exploited by others.[8] All of these risks are amplified even further when the CNE is intended to enable bulk surveillance.

---

[6] *Riley v. California*, 573 U.S. __ (2014).

[7] Testimony of Kevin Bankston on Proposed Amendments to Rule 41 of the Federal Rules of Criminal Procedure, before the Judicial Conference Advisory Committee on Criminal Rules, at 3, Nov. 5, 2014, available at https://www.newamerica.org/downloads/OTI_Rule_41_Testimony_11-05-14_final.pdf.

[8] See id. at 5-6.

III. Bulk CNE would be profoundly dangerous to both privacy and security, and should be prohibited.

10. Use of CNE against a large group of subjects is never appropriate, and would have severe harms for both privacy and security.

11. Bulk surveillance is in itself a controversial practice. By its nature this method does not distinguish between suspected bad actors and individuals with no connection to wrongdoing. Activities that involve such disproportionate impacts on privacy are unnecessary and unacceptable. In addition, debate in recent years has conclusively debunked the theory that bulk collection will provide unique value simply because it provides the government with more data, while also demonstrating the significant privacy risk posed by such collection.[9]

12. Additionally, while we do not believe that bulk collection is necessary or called for, bulk collection of communications metadata (which is explicitly referenced in the draft bill[10]) does not require the use of CNE. Communications metadata cannot be fully encrypted in the same manner as content or data at rest; in order for a third party to route data, information about the sender and recipient must be available. Such information, therefore, can generally be obtained from telecommunications providers when necessary and with the proper oversight.

13. Finally, use of CNE for bulk collection by definition requires exploitation of a vulnerability that impacts a wide population, and therefore represents a significant public security risk. As stated earlier, any vulnerability that governments can use can also be used by criminals or foreign governments, and one that targets a large number of people would be incredibly valuable to those other parties. Any time the government can engage in a bulk exploit, so might criminals, terrorists, or a foreign nations. Such a measure is bad policy, and can never "be necessary in the interests of national security."[11] Instead, governments that obtain vulnerabilities that can be used on such a massive scale should inform the vendor of the software in question and encourage them to fix the vulnerability.[12]

---

[9] For example, the United States recently outlawed domestic bulk collection after the ongoing telephony metadata bulk collection program was deemed to provide no unique security value. According to the Privacy and Civil Liberties Oversight Board, there was not "a single instance involving a threat to the U.S. in which the telephone records program made a concrete difference in the outcome of a counterterrorism investigation [and] … no instance in which the program directly contributed to the discovery of a previously unknown terrorist plot or the disruption of a terrorist attack." The Privacy and Civil Liberties Oversight Board, *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court*, (23 January 2014), 11, available at http://www.pclob.gov/SiteAssets/Pages/default/PCLOB-Report-on-the-Telephone-Records-Program.pdf. *See also, Liberty and Security in a Changing World, Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies,* The President's Review Group on Intelligence and Communications Technologies, Dec. 12, 2013, 104 *and* Bailey Cahall, David Sterman, Emily Schneider, and Peter Bergen, *Do NSA's Bulk Surveillance Programs Stop Terrorists?,* New America, Jan 13, 2014.

[10] *Draft Investigatory Powers Bill*, 20 ("Access to large volumes of data enables the security and intelligence agencies to piece together communications and other data and identify patterns of behaviour. This enables them to: Establish links between known subjects of interest, improving understanding of their behaviour and the connections they are making or the multiple communications methods they may be using").

[11] *Id*, at 21.

[12] *See*, Michael Daniel, *Heartbleed: Understanding When We Disclose Cyber Vulnerabilities*, White House Blog, Apr. 28, 2014 *available at* https://www.whitehouse.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities *and*

IV. Companies should never be forced to use update mechanisms to introduce vulnerabilities.

14. Government use of CNE should never consist of compelling a company to use a software update to introduce a vulnerability into an application or operating system. Use of software updates for CNE causes devices and software to be less secure. Such a method is even worse than leaving a known vulnerability unfixed, because rather than preserve an existing insecurity, it would involve government proactively weakening computer security, and increasing risk for consumers. And as with vulnerabilities left unfixed, vulnerabilities added through government action could be exploited by anyone who discovers them, including cyber criminals and other bad actors.

15. In addition to the direct security risks, this tactic would cause significant harm by discouraging good consumer behaviour. If it is possible that updates may actually make software less secure, individuals may decide they are better off leaving older versions of applications in place. Similarly, users may decide that automatic updates, which are widely viewed as vital for cybersecurity today, are more dangerous than not. Users should never question the legitimacy of software updates. Given cyber criminals' frequent use of older vulnerabilities for repeat attacks, and the importance of broad adoption of a patch when a mass vulnerability – such as Heartbleed – is discovered, it is critical that government does not discourage consumers from updating software.

16. Discouraging updates would cause problems beyond enhanced risk of cyber attack. Applications – especially those primarily designed for mobile use – are frequently updated to test or provide new features, and increase functionality. On average, the most popular iPhone applications are updated once every month.[13] If large numbers of users ignore updates out of concern that they include government mandated vulnerabilities, it will undermine general innovation and development.

17. Thus even if government does not pursue a policy of requiring vulnerabilities be included in updates, the mere legal authorization and possibility that such action could occur would have major repercussions. To avoid these harms, any authorization for government use of CNE should make clear that compelled inclusion of vulnerabilities in updates is not permitted.

18. We hope these comments will assist the Science and Technology Committee in its evaluation of the Draft Investigatory Powers Bill. Please contact OTI Senior Counsel Ross Schulman[14] if you have any questions.

---

[13] Hugh Kimura, SensorTower, *25 Top iOS Apps and Their Version Update Frequency* (15 April 2014), *available at* https://sensortower.com/blog/25-top-ios-apps-and-their-version-update-frequencies.

[14] Available by email at ross@opentechinstitute.org or by phone at +1 202-986-2700