Mozilla

To the Honourable Members of the Science & Technology Committee of the House of Commons,

Thank you for this opportunity to provide comment and input on the draft Investigatory Powers Bill.

1. Introduction

1.1 Mozilla's mission is to promote openness, innovation, and opportunity on the Web. We produce the Firefox Web browser and Firefox OS mobile ecosystem, together adopted by half a billion individual Internet users around the world. Mozilla is also a non-profit foundation that educates and empowers Internet users to be the Web's makers, not just its consumers. To accomplish this, Mozilla functions as a global community of technologists, thinkers, and builders -- including many contributors and developers in the United Kingdom -- who work together to keep the Internet alive and accessible. We are legally registered in the UK, maintain an office in London, and around 100 of our employees live here. Additionally, every year we bring thousands of people to the Greenwich Peninsula for the Mozilla Festival, a weekend-long celebration of making and building on the Web.

1.2 The open Internet relies on technological and legal design decisions to ensure its continued vitality. Unfortunately, the legislation before you would undermine that framework, and represents a serious threat to open source software, online commerce, and user privacy, security, and trust. A comprehensive revision of the Investigatory Powers Bill is necessary to protect the Internet and its users.

1.3 The bill proposes a broad and dangerous set of surveillance mandates and authorities that threaten privacy and security online. Keeping Internet users safe does not have to cost them their privacy, nor the integrity of communications infrastructure. We believe the current legislation falls far short of striking the right balance.

1.4 In particular, we have serious concerns regarding:

- Requirements to undermine encryption that pose a severe threat to trust online and to the effectiveness of the Internet as an engine for our economy and society;
- Bulk equipment interference authorities that could be used to violate the integrity of our products and harm our relationship with our users;
- Limitations on disclosure that impact our open philosophy and in practice are unworkable for an open source company;

- Bulk interception capabilities that would compromise the privacy of communications; and
- Data retention mandates that create unnecessary risk for businesses and users.

1.5 Government collection and retention of user data impact trust and openness online. This makes it critical to have a clear and public understanding of the means and limits of surveillance activities - a set of surveillance rules of the road.

1.6 The following three principles, derived from the Mozilla Manifesto, attempt to identify those means and limits. They offer a "Mozilla way of thinking" about the complex landscape of government surveillance and law enforcement access. We do not propose a comprehensive list of good or bad government practices, but rather describe the kinds of activities in this space that would protect the underpinnings and integrity of the Web.

- User Security: Mozilla Manifesto Principle #4 states "Individuals' security and privacy on the Internet are fundamental and must not be treated as optional." Governments should act to bolster user security, not to weaken it. Strong and reliable encryption is a key tool in improving user security. Security and privacy go hand-in-hand; you cannot have one without the other.
- Minimal Impact: Mozilla Manifesto Principle #2 states that the Internet is a global public resource. Government surveillance decisions should take into account global implications for trust and security online by focusing activities on those with minimal impact.
- Transparency and Accountability: Mozilla Manifesto Principle #8 calls for transparent community-based accountability as the basis for user trust. Because surveillance activities generally are (and inherently must be, to some degree) conducted in secret, independent oversight bodies must be effectively empowered and must communicate with and on behalf of the public to ensure democratic accountability.

1.7 In several respects, the Investigatory Powers bill does not adequately reflect these three principles, and consequently gives cause for great concern.

2. Obligations to weaken the security of our products

2.1 The draft Bill permits encryption backdoor mandates through the obligations imposed by a "maintenance of capability order," which may include an obligation to "remove the electronic protection applied by a relevant operator to any communications or data."[1] In practice, this provision could be used to force companies to undermine the encryption protecting user communications -- for example, for users of Hello, our encrypted in-browser video conferencing service -- unacceptably placing their private data at risk. Moreover, the possibility that companies might be forced to weaken encryption on products would erode user trust in those products, harming the continued success of online commerce. This has a potentially huge impact on the Internet: Firefox encrypts 100 billion individual Web data transfers for our users every day.

2.2 Requirements that systems be modified to enable government access to encrypted data are a threat to users' security. The primary aim of computer security is to protect user data against any access not authorised by the user; allowing law enforcement access violates that design requirement and makes the system inherently weaker against the attacks that it is intended to defend against. Once systems are modified to enable law enforcement access by one government, vendors will be under enormous pressure to provide access to other governments. It will not be possible in practice to restrict access to only "friendly" actors. Moreover, the more government actors have access to monitoring capabilities, the greater the risk that non-governmental cyberattackers will obtain access. Endpoint law enforcement access requirements are also incompatible with Open Source and open systems because they conflict with users' right to know and control the software running on their own devices.

2.3 Encryption powers the security we need as a society for credit cards and commerce, patient data and medical information, proprietary business and legal discussions, and other important communications. As several leading cybersecurity experts articulated in a recent technical report, proposals to require a government backdoor into digital communications "are unworkable in practice, raise enormous legal and ethical questions, and would undo progress on security."[2]

3. Use of "equipment interference" impacting our company and our users

3.1 Similarly, compelling companies to modify their products to allow government access would deny UK businesses the ability to provide secure products and services to their customers, undermining trust and the success of UK businesses in the software and online service industries. For Mozilla, user trust is paramount, and any obligations introduced which would require us to undermine the security of the

[1] Section 189(4)(c), Maintenance of technical capability, Chapter 1, Part 9, Investigatory Powers Bill

[2] http://dspace.mit.edu/handle/1721.1/97690

products and services we build and distribute would pose a significant challenge to our operations in the UK.

3.2 In particular, we are concerned about the expansion of unsolicited "equipment interference," or effectively intrusion, capabilities proposed in the Bill including:

- systems intrusion capabilities for law enforcement and intelligence agencies providing the ability to gain direct access to, or otherwise tamper with, electronic devices to obtain communications, private information or equipment data;[3]
- bulk intrusion capabilities for intelligence agencies for acquiring the content of communications;[4]
- extra-territorial reach of intrusion capabilities to "conduct" and "persons" outside of the United Kingdom;[5] and
- an obligation on Communication Service Providers (CSPs) to assist in giving effect to intrusion requests.[6] These obligations would be imposed by the Secretary of State onto "relevant operators" or "relevant operators of a specified description," and would include, but would not be limited to:
    - (a) obligations to provide facilities or services of a specified description;
    - (b) obligations relating to apparatus owned or operated by a relevant operator;
    - (c) obligations relating to the removal of electronic protection applied by a relevant operator to any communications or data;
    - (d) obligations relating to the security of any postal or telecommunications services provided by a relevant operator;
    - (e) obligations relating to the handling or disclosure of any material or data.[7]

3.3 The bulk systems intrusion provisions in the Investigatory Powers bill could be used to compel a software developer, like Mozilla, to ship hostile software, essentially malware, to a user — or many users — without notice. As an open source project, this is problematic from both philosophical and practical perspectives.

3.4 All Mozilla products are open source[8] and free software.[9] Not only is our software available for download free of charge, but also any user has access to the

[3] Part 5, Equipment interference, Investigatory Powers Bill

[4] Part 2, Chapter 3, Investigatory Powers Bill

[5] Section 69, Extra-territorial application of Part 3, Investigatory Powers Bill

[6] Section 189, Maintenance of technical capability, Chapter 1, Part 9, Investigatory Powers Bill

[7] Section 184(4), Maintenance of technical capability, Chapter 1, Part 9, Investigatory Powers Bill

[8] http://www.opensource.org/docs/osd

source code, and may freely modify and redistribute it. This means that changes to our software are fundamentally public. Were we compelled to create a version of Firefox that was modified to permit surreptitious intrusion subject to a government order, the modifications could and would be discovered by the Mozilla community.

3.5 Furthermore, any user may use the source code we provide to “build” their own copy of the software, whether the source code is modified from that which is publicly available or not. “Building” the code results in a program which reflects the code which was compiled, and which can easily be redistributed over the Internet. There is no technically feasible way for Mozilla to modify the source code during a user’s independent build process. Thus, an unmodified version of the product will always be available to those with a little technical skill, and to anyone with whom those users have contact.

4. Duty not to make unauthorised disclosures

4.1 In light of the above, we are concerned about requirements to maintain the secrecy of surveillance capabilities built in to products and about the criminal penalties associated with violating that secrecy.[10] As outlined in Section 3, such restrictions on disclosure would not only contravene Mozilla's policies on notice and transparency, but would in many cases be technically infeasible as our products are open source and free software.

4.2 We believe that the wide use of open source software brings many benefits to users, businesses, and governments, and should be encouraged. The bill would instead create an environment of legal and practical uncertainty for Mozilla and other open source software developers and users.

5. Bulk interception compromising privacy of communications through passive surveillance

5.1 We are also concerned about bulk interception of communications data proposed in the bill. In particular:

- The interception of overseas-related communications;[11]
- The obtaining of related communications data from such communications, which can include data in transit or in storage;[12] and

[9] http://www.gnu.org/philosophy/free-sw.html

[10] Section 43, Duty not to make unauthorised disclosures, and Section 44, Offence of making unauthorised disclosures, Chapter 3, Part 2, Investigatory Powers Bill

[11] Section 106 (3), Bulk interception warrants, Investigatory Powers Bill

[12] Section 106 (7), Bulk interception warrants, Investigatory Powers Bill

- The obtaining of communications metadata[13] and the content of communications.[14]

5.2 We recognise that GCHQ and other country intelligence agencies currently engage in bulk collection of Internet communications. These practices fundamentally undermine the expectations of users of the privacy of communications and transactions online, and their lawfulness under European law is currently being considered by the European Court of Human Rights.[15] We are concerned that this bill would explicitly legalise these harmful practices, when it should instead rein them in.

5.3 Security and privacy are essential parts of the user experience. We and other browser makers are pushing for a fully encrypted Web in order to protect users everywhere. The use of encryption is growing daily, protecting more and more communications from interference and interception. While some Web traffic remains unencrypted, the overwhelming majority of online traffic belongs to law-abiding citizens, and has no connection to any legitimate governmental purposes. We believe that all Internet users have an expectation of privacy in the network exchange of their communications, and companies and technologists continue to support this expectation through policy and through technology. Governments should not violate it to conduct bulk surveillance of innocent people.

6. Mandatory data retention

6.1 Finally, we have serious concerns with the mandatory data retention provisions, which would require CSPs to hold on to data for 12 months.[16] As the Court of Justice of the European Union ruled in 2014, indiscriminate collection and storage of communications data is a disproportionate interference with the right to privacy.[17] Mandatory data retention creates risk and undermines trust for the users of Firefox and other Mozilla products and services. Making troves of private user information vulnerable to malicious actors and holding user data longer than necessary for business purposes creates additional, and unnecessary, liability and risk. As the nearly daily parade of data breaches make clear, amassing the personal information of everyone exposes those data to breach, theft, misuse, and abuse. Data acquired are data at risk, and such threat to user security and privacy is not warranted.

[13] Section 193 (5), Telecommunications definitions, Investigatory Powers Bill

[14] Section 193 (6), Telecommunications definitions, Investigatory Powers Bill

[15] Human Rights Organisations v UK, see: https://www.privacyinternational.org/node/555

[16] Section 71, Powers to require retention of certain data, Part 4, Investigatory Powers Bill

[17] Digital Rights Ireland v Ireland, see: http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=12322

7. Conclusion

7.1 Thank you for the opportunity to comment on the draft Investigatory Powers Bill. As a global community of developers and engineers, Mozilla prides itself on providing secure and open products and services to our users. Mozilla sees the draft Investigatory Powers bill as a missed opportunity to set a strong global standard in reforming surveillance powers, and a harmful step backward for the interests of Internet users and the Internet economy. However, the UK parliament still has the opportunity to amend the bill, and we hope the Science and Technology committee and forthcoming committees will carefully weigh the intended objectives with the consequences for the continued success of UK businesses and the security of users. Comprehensive revision of the draft Investigatory Powers bill is necessary to protect online commerce, and user privacy, security, and trust.

7.2 We look forward to working with you and other Committees to create meaningful surveillance reform over the next year, and are happy to answer any questions you may have.

7.3 For more information, please contact:
Raegan MacDonald, Senior EU Policy Manager (raegan@mozilla.com)
Chris Riley, Head of Public Policy (mchris@mozilla.com)

*   *   *