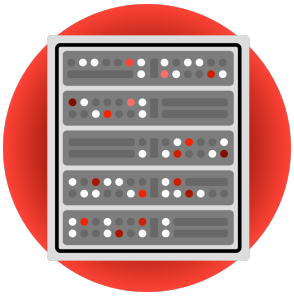
Written Evidence Submitted by the Internet Infrastructure Coalition (i2Coalition) To the House of Commons Select Committee on Science and Technology In the Matter of the Draft Investigatory Powers Bill

INTERNET INFRASTRUCTURE COALITION



718 7th Street NW
2nd Floor
Washington DC 20001

membership@i2coalition.com

(202) 524-3183

1. The i2Coalition appreciates the opportunity to present its comments to the House of Commons Select Committee on Science and Technology (the "Committee") in the Matter of the Draft Investigatory Powers Bill (the "Draft Bill").

2. **Executive Summary**
   - The creation of backdoors, or requirements that providers decrypt and re-encrypt communications prior to delivery creates vulnerabilities in the Internet infrastructure that make society less safe. Prior attempts to do so demonstrate this.
   - Consumers and businesses depend on assurances of security prior to transacting business on the Internet.
   - The Draft Bill increases the cost of doing business for small business by requiring them to reengineer their networks to accommodate the Draft Bill's technical provisions. The Draft Bill does not promise to fulfill the government's incurred costs. Rather it promises a "contribution" that will be "not nil."
   - Data storage requirements are unduly burdensome to small business, and the Technical Advisory Board anticipated by the Draft Bill may not have the capability to fully analyze those costs.
   - The provisions of the Draft Bill will undermine the moral authority of the United Kingdom the long term security position of the U.K. will be strengthened when countries of the world such as the U.K. remain in the forefront of promoting fundamental rights and freedoms such as free speech and association.
   - Many of the provisions set out in the Draft Bill were considered by the Congress of the United States in the late 1990's and rejected. In addition, in an analysis the National Academy of Sciences determined that backdoors were technologically compromised and that free expression issues were materially impacted by weakening encryption standards.
   - The Draft Bill will encourage other countries to implement similar laws having extraterritorial effect. Those laws will not take into consideration concerns of U.K. citizens, such as privacy, that are important priorities.

3. We acknowledge that the Government has taken pains to state that that it is not the intent of the Draft Bill, or the Government in general to break encryption, or outlaw its use. However, sections 188 and 189 contain general and broad statements related to the use and operation of encryption, that could be, and appear to us to have the effect of, leading to a requirement of a backdoor. Indeed, it appears realistic to view the Draft Bill with an eye that Internet infrastructure providers themselves could be required to build backdoors to their own systems.

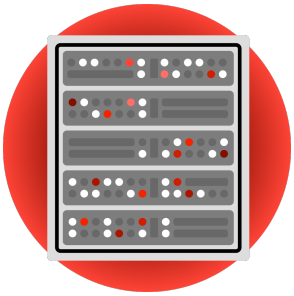
4. **There is no encryption with a backdoor.** If a backdoor is created in cryptographic code, it will be uncovered by those with bad intent. In past years, encryption vulnerabilities have been discovered in a number of mass market technology platforms. Those include CRIME, BEAST, Heartbleed and Logjam. A vulnerability is the same as a backdoor: if an Internet infrastructure provider can direct law enforcement to a backdoor to gain access to encrypted communication, those with bad intent can just as easily discover it. Every computer security expert who has testified on this subject has stated that backdoors weakens Internet security.

5. **Backdoors introduce vulnerabilities.** Indeed, the "Clipper Chip" developed by the U.S. National Security Agency for the first U.S. legislative encryption proposal of the modern Internet era, was determined after the fact to have a vulnerability that would have significantly undermined the security of networks to which it was attached. Further credibility that backdoors introduce vulnerabilities into networks is demonstrated by the "Athens Affair" in which criminals exploited the required backdoor wiretapping access of a mobile phone provider to gain access to the conversations of prominent politicians.

6. **Strong security is the backbone of the Internet economy.** Secure and trusted encryption is the lynchpin of that security. For example, the ability of customers to trust that the locked symbol in their browser means that their information is secure, leads to overall trust in the Internet economy in general. The vulnerabilities identified in paragraph 4 above created a grave crisis of confidence that Internet infrastructure providers can secure their networks. Backdoors will exponentially increase the vectors that may be used by bad actors to access the Internet. This will cause more frequent, and more profound, security breaches than previously seen, leading to a decrease in trust overall in the Internet. The United Kingdom has made great efforts to position itself as a center for the Internet infrastructure economy not only in Europe, but around the world. One need look no further than the high demand for colocation and data center space in the London area as evidence that those efforts have borne success. Weakening encryption by introducing vulnerabilities jeopardizes that economic effort.

7. **Introducing vulnerabilities into an encryption product only disadvantages U.K. businesses.** Not only will it be known that Internet businesses based in the United Kingdom are less secure than those who are based where security has not been weakened, but non weakened technology will be available outside the U.K. This will have at least two effects: Internet infrastructure providers will move from the U.K. to jurisdictions that are less hospitable to U.K. law enforcement requests; and second bad actors will simply switch to the great number of already available free and open source encryption products available on the Internet. In essence, the Draft Bill will not stop bad actors from securing their communications. It will only make it more difficult for law enforcement to gain access to information in other ways that may help them do their job, while at the same time strengthening the economies of other countries.

INTERNET INFRASTRUCTURE COALITION



718 7th Street NW
2nd Floor
Washington DC 20001

membership@i2coalition.com

(202) 524-3183

8. **The U.K. is in a unique position as a hub of Internet innovation.** The Draft Bill, and the technologically backward looking nature of its provisions, will undermine that position. Those seeking to start businesses, or relocate them, look closely at whether the laws in a country are "tech positive" and encourage the kind of innovation and imagination necessary to create a new business. The Draft Bill introduces vulnerabilities into networks, requires complex engineering tasks to be borne by companies, and increases the opportunities for bad actors to gain access to sensitive data. None of these could reasonably be considered to result in a determination that the U.K. was a good place for technology innovation.

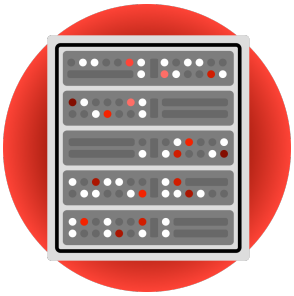
9. **The largest economic impact of the Draft Bill will be felt by small to medium sized Internet infrastructure businesses.** Currently the Internet infrastructure is composed primarily of small to medium sized businesses. The current low barrier to entry has resulted in an incredibly robust, vibrant and competitive hosting environment. This means that most web hosts, and other Internet infrastructure providers exist on very thin margins. Even if the technical provisions mandated in the Draft Bill were technologically feasible, they would only be so on a very large scale. For example, encrypting data, decrypting it, and then re-encrypting it would require the addition of two extra steps. Because encryption and decryption is resource intensive, the Draft Bill would conceivably increase the cost of doing business in the U.K. by two times.

10. **The costs to business could be staggeringly high.** While it is current U.K. Government policy to provide complete reimbursement of legitimately incurred costs, the Draft Bill does not provide adequate confidence that this will be the case. The Draft Bill states that it will provide a "contribution" that will be "not nil." This does not inspire confidence that 100% of the costs of complying with the Draft Bill will be covered. **Recommendation:** *We respectfully suggest that the Secretary of state be required to reimburse all costs that are, or were, in her opinion, legitimately incurred in observance of a retention notice, or in observance of other notices or authorizations.*

11. **Because no two Internet infrastructure providers are alike, the engineering operation inherent in the Draft Bill is immense.** Because of the bespoke nature of each company's network, each company will be required to reengineer their network to accommodate the requirements of the Draft Bill to encrypt and decrypt, as well as store information.

12. **The engineering complexities can be seen in sections 51 through 53.** These sections refer to requirements that Internet infrastructure providers provide live application programming interfaces (API) that will facilitate access to disparate data stores and enable searches across different data sets. These programming efforts are difficult when designed for a specific commercial product, much less the individual and unique environments used by each component of the Internet infrastructure.

INTERNET INFRASTRUCTURE COALITION



718 7th Street NW
2nd Floor
Washington DC 20001

membership@i2coalition.com

(202) 524-3183

13. **The Draft Bill does not contemplate the loss of opportunity costs associated with compliance.** Even if an Internet infrastructure provider builds a compliance system and is reimbursed the costs of building it, the provider will still forego the business benefits that would have been achieved by devoting its efforts towards building a business, rather than building compliance. As is evidenced throughout these comments, the costs and engineering complexities associated with compliance with the Draft Bill are large, once built, Internet infrastructure providers will still spend time and efforts ensuring continued compliance rather than devoting those continuing efforts towards improving and expanding their business.

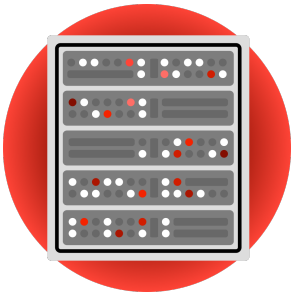
14. **These engineering requirements also jeopardize the security of the Internet as a whole.** Good security practices require Internet infrastructure providers to engineer the complexity out of their networks. The Draft Bill introduces significant additional complexities into network operations, increasing the vulnerability of individual providers and the Internet as a whole. When vulnerabilities are discovered in the APIs and other technical measures required by the Draft Bill, as they inevitably will be, these will weaken the U.K.'s national security. This weakening must be taken into account when analyzing the costs and benefits of the Draft Bill.

15. **The unique nature of each Internet infrastructure provider's network calls into question laboratory assessments of the feasibility of the technical measures called for in the Draft Bill.** Simply put, no controlled environment can be expected to pose the real world challenges of the daily evolution of each Internet infrastructure provider's network. Each day these providers must meet requests presented by their customers for new features, implementation of "bug fixes" and new versions required by vendors, and threats posed by bad actors. The "filtering system" is a prime example of this complexity.

16. **The data storage mandates set out in the Draft Bill would also significantly increase the costs of doing business.** It is important to understand that data storage is not without costs. In addition to the cost of hardware necessary to store the "meta data" identified in the Draft Bill, Internet infrastructure providers would be required to pay for electricity, cooling, additional colocation resources, and employees to maintain facilities. These companies would also be tasked with securing highly sensitive, and as a result, high profile, personal data from bad actors. This creates an additional security vulnerability whose cost must be significantly weighed.

17. **Recommendation: If in fact the data storage mandates are included, small to medium sized Internet infrastructure providers must be included in the Technical Advisory Boards contemplated by the Draft Bill.** Only in doing so will those charged with determining the feasibility and burdensomeness of individual storage requests understand the impact on the Internet infrastructure as a whole. Relying simply on large, or well known, businesses for this input will result in incomplete, and possibly economically damaging, analysis.

INTERNET INFRASTRUCTURE COALITION



718 7th Street NW
2nd Floor
Washington DC 20001

membership@i2coalition.com

(202) 524-3183

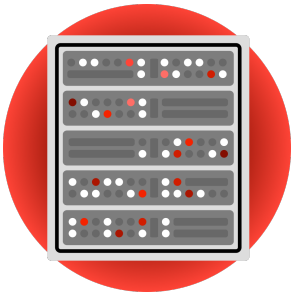
18. **Many of the countries with a developing Internet infrastructure will follow the U.K.'s lead, and demand backdoor access of their own.** While the Draft Bill's intentions are noble, the same cannot be said for the intentions of other countries. Indeed, the U.K. has taken the lead in ensuring that the Internet remain free, fair and open; challenging actions by China and Russia to impose governmental controls over the mechanisms of Internet functioning. Indeed, in China U.K. businesses must already significantly compromise the integrity of their networks to simply gain market access. The Draft Bill will undermine effective and persuasive arguments about network integrity that have, to date, preserved the ability of U.K. businesses to engage in commerce worldwide. While issues such as freedom of speech, and the right to assemble, are beyond the i2Coalition's mandate, the Draft Bill would make it much more difficult to argue that governments should not have access to data in order to control its message, tone or dissemination.

19. **While some of the provisions of the Draft Bill are unique, many were previously considered and previously rejected by the United States.** Indeed, in the "crypto wars" of the late 1990's the United States considered, and rejected many of the items in the Draft Bill including similar data retention and access requirements. Importantly, in an exhaustive study by the U.S. National Academy of Science, provisions not unlike those contemplated in the Draft Bill were rejected as technologically compromised, and significantly impinging on the right to free expression.

20. **The extraterritorial implications of the Draft Bill will have wide reaching implications.** The current focus of all Internet development worldwide is to decrease the geographic restrictions on business. The Draft Bill moves backwards on this issue. A simple review of the Draft Bill by global organizations has led to commitments that its provisions will lead them to restrict access by citizens of the U.K. to their networks. Those considering the Draft Bill should consider a U.K. in which citizens cannot take full advantage of the computing power provided by global cloud providers. This power has so significantly reduced the cost of bringing businesses online that it has created entire new industries such as "software as a service." These industries benefit economies such as the U.K. who may not have the market power of larger markets like the United States.

21. **Moreover, the Draft Bill will invite reciprocal action from other countries.** As it stands, the United States has resisted calls to consider similar legislation. This resistance is based, in part, on the willingness of allies like the United Kingdom to refrain from mandating access to data. It is not hyperbole to expect that U.K. laws having extraterritorial effect will invite similar laws. While some of these laws may come from countries having values similar to those in the U.K., others will come from countries like Russia who may not have the same law enforcement and national security concerns as the U.K.

INTERNET INFRASTRUCTURE COALITION



718 7th Street NW
2nd Floor
Washington DC 20001

membership@i2coalition.com

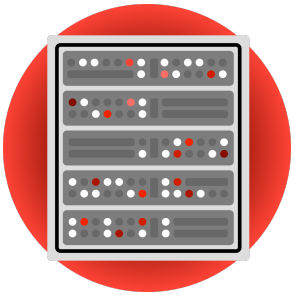
(202) 524-3183

22. **It is important to remember the limited volume of Internet traffic that passes through the United Kingdom.** Passage of the Draft Bill will encourage countries like the United States to pass legislation imposing obligations that will, target far more traffic that that in the U.K. These laws cannot be assumed to take into account the concerns U.K. citizens have about their personal data and the use of that data in ways that may contravene U.K. law.

About the I2Coalition

The i2Coalition is the global voice of Internet infrastructure providers such as web hosts, colocation providers, data centers and domain name registries and registrars. We support those at the center of the Internet. We believe the continued growth of the Internet is vital for growing an environment of innovation and seek to engage in ways to foster success of the Internet and Internet infrastructure industry. We seek to influence decision makers to weigh decisions on whether they are good or bad for the Internet economy and its foundational industries. In short, we seek to foster growth within the Internet infrastructure industry by driving others to harness the Internet's full potential. To learn more about i2Coalition, visit http://www.i2Coalition.com.

INTERNET INFRASTRUCTURE COALITION



718 7th Street NW
2nd Floor
Washington DC 20001

membership@i2coalition.com

(202) 524-3183