Internet Architecture Board (IAB) comments on the Australian Assistance and Access Bill 2018

10 October, 2018

The Internet Architecture Board (IAB) provides long-range technical direction for Internet development, ensuring the Internet continues to grow and evolve as a platform for global communication and innovation. It also provides oversight of a number of administrative activities and relationships on behalf of the Internet Engineering Task Force (IETF). The IAB is chartered both as a committee of the IETF and an advisory body of the Internet Society. Further details about the IAB are documented in RFC 2850.

The IETF is a global organization whose goal is to make the Internet work better. The IETF is responsible for the key technology standards that are used on the Internet, including IP, TCP, DNS, BGP, TLS, and HTTP, to name but a few. IETF standards are published in the RFC series. For further information about the purpose and mission of the IETF, see RFC 3935, "A Mission Statement for the IETF".

The IAB welcomes the opportunity to comment. While we normally do not review proposed legislation, we are concerned that this proposal might have a serious and undesirable impact upon the Internet and, taken as a model, the sum of similar legislation may result in the fragmentation of the Internet.

Encryption, Trust and Systemic Vulnerability

We appreciate the stated goal of avoiding the addition of systemic weakness into forms of electronic protection, thereby undermining security through "backdoors" in encryption implementations. Encryption is one of the core primitives that is used to secure the Internet, and any interference in its operation puts the Internet at risk; for more information, see our Statement on Internet Confidentiality.

However, requiring access to data that's intended to be kept confidential after it has been decrypted can cause weaknesses and harms that are equivalent to or greater than those caused by backdoors in encryption itself. This is because it is very common for Internet protocols to require a level of trust between two (or more) parties in addition to the surety that encryption provides. That trust isn't backed by technical guarantees; it depends wholly on the relationship between the parties.

Some services that require such trust are considered critical Internet infrastructure. For example, the Public Key Infrastructure (PKI) system is the underpinning of encryption for applications like the Web. Certificate Authorities (CAs) are trusted by applications and users to faithfully and truthfully issue certificates, so that parties that they are communicating with can be correctly identified.

Furthermore, CAs publicly attest to all certificates they issue using Certificate Transparency, in order to assure their trustworthy operation. Requiring them to break those agreements will jeopardize the trust arrangements at the core of the Internet's operation.

Any method used to compel an infrastructure provider to break encryption or provide false trust arrangements introduces a systemic weakness, as it erodes trust in the Internet itself.

In other words, the mere ability to compel Internet infrastructure providers' compliance introduces that vulnerability to the entire system, because it weakens that same trust. The Internet, as a system, moves from one whose characteristics are predictable to one where they are not.

We understand that Australia intends to develop appropriate oversight mechanisms to avoid misuse or overuse of these instruments within its borders. However, as custodians of the Internet's architecture, we are required to take a global view. This approach, if applied generally, would result in the Internet's privacy and security being the lowest common denominator permitted by the actions taken in myriad judicial contexts. From that perspective, this approach drastically reduces trust in critical Internet infrastructure and affects the long term health and viability of the Internet.

Fragmentation Risk

As a global network of networks, the Internet operates best when its infrastructure is highly redundant and when responsibility for various services is shared between many parties that are geographically distributed.

We are concerned that the proposed legislation may cause these service providers to violate contracts or laws in other jurisdictions, depending upon the exact nature of the requests made. For example, companies with European presence are required to handle sensitive data according to the GDPR, and by complying with an Australian order for data that might be located in Europe, that provider could be required to violate the GDPR to satisfy Australian law.

This risk might cause some infrastructure providers to relocate, reduce service or even block service to Australian users. Such fragmentation of the Internet is one of the primary concerns we have today, as it reduces the value of a global, highly-connected Internet.

Impact upon Standards Bodies

We were also concerned to read this description in Section 317C of the Explanatory Document:

> **Item 6** of the table lists persons that develop, supply or update software used, for use, or likely to be used, in connection with a listed carriage service or an electronic service that has one or more end-users in Australia. This category would include, for example, persons involved in designing trust infrastructure used in encrypted communications or software utilised in secure messaging applications.

In our reading, this text implies that the instruments defined by this legislation could be used in an attempt to compel various forms of cooperation by the IETF and other Standards Developing Organizations, or their participants.

The IETF, in RFC 2804, has rejected the development of any system designed to aid state actors in compromise of the security of Internet communications. Compelling individual participants to act contrary to that consensus introduces doubts about the motivations of and influences upon a participant's actions, and therefore may disadvantage Australian participants in these processes.

Internet standards development is based upon mutual trust, cooperation and good-faith participation. Having those undermined by this legislation does not appear to be an appropriate result.

The following Listed Acts or Things increase our concern, when applied to standards participants:

> **317E(1)(h)** provides modifying, or facilitating the modification of, any of the characteristics of a service provided by the provider as an act or thing that may be specified in a technical assistance request, technical assistance notice or technical capability notice. By way of example, modification of a service could include blocking the delivery of a specific service to a target.
>
> **317E(1)(i)** provides substituting, or facilitating the substitution of, a service provided by the provider for additional services as an act or thing that may be specified in a technical assistance request, technical assistance notice or technical capability notice.

Since the "service provider" in the case of Item 6 is someone who "designs trust infrastructure", it seems that these instruments could compel a participant to influence the design of the trust infrastructure. While Section 317ZG might rule out overt compromises of encryption through this mechanism, the lack of definition around "systemic vulnerability" and "systemic weakness" make this difficult to estimate.

Recommendations

The ability to compel compromises to the mechanisms that provide security, privacy, and trust on the Internet erodes trust in the Internet as a whole. That erosion, multiplied by the number of political and judicial contexts in which similar approaches might be adopted, represents an existential threat to both the Internet's security and its integrity.

With these considerations in mind, we request that you review the proposed legislation to more generally consider the security and integrity of the Internet as a system. In addition to that, we recommend specifically that any final legislation:

1. Significantly clarifies the meaning of "systemic vulnerability" and "systemic weakness" in relation to a number of different types of systems, including critical Internet infrastructure.
2. Explicitly prohibits the use of this legislation to compel cooperation by operators of critical Internet infrastructure services, including but not limited to DNS, PKI, and BGP.
3. Likewise, prohibits the use of this legislation to compel cooperation by implementations of Internet Standards-Track protocols such as HTTP, DNS, TCP, QUIC, IP and TLS.
4. Likewise, prohibits the use of this legislation to compel cooperation by standards developing organisations and their participants (in that capacity).
5. Provides for cases where this legislation clashes with the commitments a recipient might have in other jurisdictions.

Respectfully submitted,

Ted Hardie
Chair, Internet Architecture Board