INTERNET SOCIETY SUBMISSION TO THE U.N. SPECIAL RAPPORTEUR ON THE PROTECTION AND PROMOTION OF THE RIGHT TO FREEDOM OF EXPRESSION AND OPINION REGARDING THE USE OF ENCRYPTION AND ANONYMITY IN DIGITAL COMMUNICATIONS

DATE: 10 FEBRUARY 2015

About the Internet Society

The Internet Society is the trusted independent source for Internet information and thought leadership around the world. It is also the organizational home for the Internet Engineering Task Force (IETF). With its principled vision, substantial technological foundation and its global presence, the Internet Society promotes open dialogue on Internet policy, technology, and future development among users, companies, governments, and other organizations. Working with its members and Chapters around the world, the Internet Society enables the continued evolution and growth of the Internet for everyone.

Introduction

The Internet Society welcomes the opportunity to contribute to the report that will be prepared by the Special Rapporteur on the protection and promotion of the right to freedom of opinion and expression, David Kaye. The topic of the report, "the legal framework governing the relationship between freedom of expression and the use of encryption to secure transactions and communications, and other technologies to transact and communicate anonymously online", is of utmost importance. Our comments are intended to highlight the central role that anonymity and confidentiality (e.g. through encryption) play in facilitating the exercise of fundamental human rights such as privacy and freedom of expression. We also wish to emphasize that policy efforts should focus on how to achieve law enforcement and other societal objectives in a world where anonymity and encryption exists, rather than striving to prevent its use. This will be a challenging task, but a necessary one, if individuals around the world are to be able to fully exercise their rights online.

The ability to communicate confidentially online

The ability to communicate privately is a key aspect of the enjoyment of the right to privacy. If communications are unmonitored and ephemeral like a conversation between two individuals standing in an otherwise empty park, there may be no need for whispers, code or other means of ensuring confidentiality. However, where communications are, or could be, monitored, collected, intercepted, recorded, stored, retrieved and analysed in real time or at a later date, the ability to communicate confidentially becomes of paramount importance if individuals are to be able to fully exercise their right to privacy.

Every aspect of our online life depends on communication passing through third party intermediaries (e.g. ISPs, email providers, search engines, cloud services, e-commerce platforms, etc.): there is no digital equivalent to the "empty park".

In 2014, the Internet Society invited Internet users to share their needs and expectations with respect to confidential online communications through a survey. The results of that survey are available here. We recorded 1347 responses. We consider this sample to be too small to be representative and assume there was a self-selection bias towards individuals with an interest in confidentiality. Nonetheless, the responses confirmed our hypothesis that the need for confidential online communication spans national borders and cultures.

One of the principal methods for achieving confidentiality for online communications is encryption. Other methods might include obfuscation[1] and social stenography[2]. In light of the 2013 revelations concerning online pervasive surveillance activities, some application service providers adopted new measures to protect the confidentiality of their customers' communications from unauthorised third parties (e.g. Google and Yahoo encrypted data in transit between their respective data centres[3]). However, such "measures ("point to point", rather than end-to-end encryption) do not prevent the application service provider from viewing the communications. And …. if the application service provider (an intermediary) has access to unencrypted customer content, so might an attacker.

Trusted end-to-end encryption solutions allow Internet users to protect the confidentiality of their communications, not just from outsiders, but also from prying intermediaries. They also serve to reinforce user confidence, which is fundamental for a successful digital economy.

Why the ability to interact online anonymously matters

Anonymity is a tool **for social participation**. There are many legitimate and socially desirable reasons why Internet users might wish to be anonymous online, keep the content they are reading or sharing private, and why they may not want others to know which services they are using: privacy, personal security; concerns about surveillance by governments or private companies; concerns about potential repercussions for statements made in social media and/or hosting blogs for "cyber-activists"; and concerns about conclusions that may be drawn about them based on what they see and communicate on the Internet, to name a few. Conversely, some may wish to hide their involvement in illegal activity, but even if anonymity is banned, they will find another way – e.g. by impersonating, and thereby, implicating innocent third parties. Banning anonymous access, perversely, might generate a black market in valid, 'clean' credentials, encouraging unscrupulous activity by bad actors and putting legitimate users at risk.

Anonymity is also an important enabler **for the exercise of the right of freedom of expression** in communities where criticism is viewed unfavourably. While criticism may be challenging, it is a healthy input to good governance (whether political or corporate). It also allows vulnerable communities to communicate freely without fear of repression or worse. Privacy, as some have put it, is a foundational right without which many other rights become impossible to exercise.

In this regard, it is important not to allow the debate over confidential communications to be reduced to a simple question of whether or not reliable encryption should be allowed. Encrypting the contents of a conversation between two individuals provides, at best, only partial confidentiality: it is still obvious to a third party that the conversation has taken place, and between whom, and when and where. This metadata can also be linked with other observable online activities, creating a "social graph" of the communicating parties' other acquaintances, and contributing to a digital profile that, over time, reveals their behaviour, characteristics and even future intentions.

So, as well as encryption and anonymity, the following factors should also influence our approach to digital confidentiality:

- Pseudonymity – Are the parties to a private conversation immediately identifiable, anonymous, or identifiable only if certain additional conditions are met?

- Linkability – Is it possible to associate different online actions with the same user, over time, whether or not they wish this to be done?
- Observability – Does looking at the network provide enough data to tell whether or not a given individual is active on it or not?

These principles are clearly articulated and explained in a paper by Dr Andreas Pfitzmann and Marit Hansen[4].

The future of Internet communications: encryption should be the norm

Cryptography pre-dates the Internet, however, the vast majority of Internet traffic is unencrypted. But, the "default" is beginning to shift towards encryption. While, over time, there has been a gradual trend towards greater use of encryption for data security and privacy, the rate of change increased not insignificantly following the global revelations of pervasive surveillance of Internet traffic.

For example, according to Sandvine, encrypted traffic increased from 1.47% to 6.10% in Europe, 1.8% to 10.37% in Latin America, 2.29% to 3.8% in North America.[5] The Internet Initiative Japan Inc. attributes the rapid growth in HTTPS traffic since June 2013 to major service providers such as Google, Akamai, Amazon, Facebook, Twitter, Microsoft making more regular use of HTTPS for their services.[6]

The Internet technical community has also accelerated existing work to make the Internet communications more secure. In November 2014, the Internet Architecture Board (IAB) issued a statement:

> *"… Newly designed protocols should prefer encryption to cleartext operation. There may be exceptions to this default, but it is important to recognize that protocols do not operate in isolation. Information leaked by one protocol can be made part of a more substantial body of information by cross-correlation of traffic observation. There are protocols which may as a result require encryption on the Internet even when it would not be a requirement for that protocol operating in isolation.*
>
> *We recommend that encryption be deployed throughout the protocol stack since there is not a single place within the stack where all kinds of communication can be protected.*
>
> *The IAB urges protocol designers to design for confidential operation by default. We strongly encourage developers to include encryption in their implementations, and to make them encrypted by default. We similarly encourage network and service operators to deploy encryption where it is not yet deployed, and we urge firewall policy administrators to permit encrypted traffic. …"*

The Internet Society Board of Trustees supports this position of encryption-by-default.[7]

At the same time, concerns have been raised by law enforcement and others regarding what impact pervasive use of encryption solutions for Internet traffic might have on their activities. There have even been suggestions to prohibit the use of encryption, to require backdoors for governments, to limit the level of permitted complexity, or otherwise weaken cryptographic standards.

Trying to limit the utility of encryption is an "all or nothing" approach to the issues facing Internet users and governments. In any case, it would be technically impossible to preclude the use of encryption on the Internet: the technology and knowledge is freely and widely available. If necessary, malicious actors will just create their own implementations. Further, even attempting to limit the uses of encryption would have negative effects on data security, privacy, integrity and

trust. (For example, how would such rules affect the legitimate use of anonymous communications, as well as other key services such as online banking that rely on encrypted transactions?) A challenging, but better approach is to consider how to reasonably achieve public policy objectives such as law enforcement in a world where encrypted Internet traffic is the norm.

Another area that merits closer examination is how to ensure that encryption is an available solution for all users, not just those with all the resources and/or expertise. In this regard, the Internet Society survey referred to above highlighted that encrypted communication is not easy for Internet users.

There are a number of fundamental obstacles, including:

- insufficient information/guidance on how to use the tools;
- general usability issues;
- a dependency on other Internet users using the same tools;
- incompatibility between tools and other interoperability hurdles.

Additionally, among other things, the Snowden disclosures made it clear that confidential communications can be compromised far more easily by attacking the implementation, deployment and use of encryption technology than by trying to crack the encryption itself. Ensuring that encryption is robustly deployed and securely used remains a huge task.

To that end, the Internet Society favours and supports the development of secure, usable cryptographic products based on open standards. The cryptographic products themselves must be complemented by good design, and tools that support secure management once they are deployed (reliable creation of webs of trust, key distribution and management, secure update of deployed products, secure management of the artefacts of encryption/digital signature, and so on).

Conclusion

The Internet Society actively participates and contributes on issues at the intersection of the Internet and rights at the Human Rights Council. We are grateful to have had this opportunity to contribute to this important report. We will continue bringing our technical expertise and user centric principles to these debates at the March session of the Council and beyond.

CONTACT INFORMATION
Ms. Christine Runnegar
Director, Public Policy
Internet Society
runnegar@isoc.org

[1] See for example, https://en.wikipedia.org/wiki/Obfuscation_%28software%29

[2] http://dmlcentral.net/blog/danah-boyd/social-steganography-learning-hide-plain-sight

[3] Media reports: e.g. http://www.theverge.com/2014/3/20/5530072/google-encrypts-gmail-between-data-centers-to-keep-out-nsa and http://www.pcworld.com/article/2139440/yahoo-turns-on-encryption-between-data-centers.html

[4] http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf - Hansen, M.; Pfitzmann, A.; Technical University of Dresden

[5] See article regarding Sandvine report in http://www.wired.com/2014/05/sandvine-report/

[6] See IIJ Broadband Traffic Report http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol24_report_EN.pdf

[7] Internet Society Commends Internet Architecture Board Recommendation on Encryption-by-Default for the Internet http://www.internetsociety.org/news/internet-society-commends-internet-architecture-board-recommendation-encryption-default