The Politics of Encryption: The Right to Privacy and the Need for Surveillance

Proposed by:
Centre for International Governance Innovation
Global Commission on Internet Governance
Royal Institute of International Affairs (Chatham House)

IGF 2015 Subthemes: Internet and Human Rights; Trust; Emerging Issues

Hashtags: #Encryption #Privacy #Surveillance #HumanRights #CyberSecurity

Description of Workshop: Encryption is a basic building block of trust on the Internet. It is needed to ensure freedom of speech, privacy and to facilitate e-commerce. Encryption ranges along a continuum from no encryption at all to unbreakable encryption with no backdoors. Technology, politics and public sentiment all factor in to determine the appropriate or socially optimal level of online encryption. This balance is not static, either over time or across countries. Often, technological moves toward high levels of encryption generate higher efforts to break encryption by state agencies, cueing off a proverbial "crypto war". Likewise, extreme political positions either in favour or against encryption generate their opposite. These trends raise several questions that this panel will address: What is the appropriate balance of encryption online? How should the systems of Internet governance respond to changing levels of demand and supply of encryption? After the Snowden disclosures, what protocol design approaches are needed to bring trust back into the system?

This panel will bring together experts from private business, government, technologists and civil society to discuss the politics of encryption and how society should best strike the balance between encryption to ensure the right to privacy and a lack of encryption to allow for the state to protect its citizens.

Background Paper: Encryption is one of the bedrock functionalities of the Internet. Encryption is needed to ensure that individuals can freely express their views online and that individual privacy is not violated at a whim. Public key encryption is also the central feature allowing for the occurrence of e-commerce. Without some level of encryption, it is fair to say that the Internet would not exist as it does today.

In the early 1990s, the first "crypto war" was waged in the United States. During this proverbial conflict between technologist and state agencies, the United States National Security Agency (NSA) tried to get strong encryption categorized as a 'munition'. The implication was that the export or public dissemination of encryption technology was subject to the Arms Export Control Act and the International Traffic in Arms Regulations. The early implication of this categorization was that designers of encryption would have to register as arms dealers! This initial effort to stymie encryption was defeated in Bernstein v. US Department of Justice, where it was determined that software design was a form of free speech. Shortly after this, the legal dimensions of the "crypto war" came to a close. Instead, state agencies moved to break encryption through technology and have been very successful in their endeavours.

The Edward Snowden disclosures showed how effective NSA surveillance techniques have become and set off a new drive toward higher levels of online encryption. The Internet Engineering Task Force (IETF) started developing standards for heightened online encryption. Google and Yahoo! responded quickly to the news of NSA spying by initiating end-to-end encryption of their email services to try to keep intelligence agencies out. Facebook, similarly, moved to the encrypted https from http as its baseline setting for its applications in response to the disclosures. Further to this trend, major mobile companies, such as Apple, has been developing encryption technology for the messaging function on a person's phone that would leave no backdoor into the device, even if the State approached the company with a legitimate court-issued warrant.

While these are inherently business decisions on the part of major Internet technology companies, they also have large political ramifications. Federal Bureau of Investigation Director James Comey has reportedly gone so far as to suggest that Apple's new unbreakable encryption could mean that the US is "no longer a country governed by the rule of law."[1] The debate about encryption again flared in the wake of the tragic attacks on the satirical magazine Charlie Hebdo in early 2015. Shortly after these events, British Prime Minister David Cameron came out against the idea that unbreakable encryption should be allow in society because it can be used by those that wish to harm others.

Encryption of online activity falls along a continuum. At times, encryption is stronger than state capabilities and that is acceptable. At other times, encryption is weaker than state capabilities and that, too, is socially acceptable. Technology, politics and public sentiment all factor in to determine the appropriate or socially acceptable level of online encryption. This balance is not static over time and certainly not static across countries. This panel brings together experts from the IETF, private business, government and civil society to discuss the role of online encryption in society.

This panel will address the following questions, which are relevant to the IGF subthemes of Internet and Human Rights, Trust, and Emerging Issues: what is the appropriate level of online encryption? How can the systems of Internet governance respond to the changing supply and demand for encryption, both over time and across countries? After the Snowden disclosures, how can encryption design protocols be developed to help bring higher levels of trust back into the system?

The panel will bring together members of civil society, business and former government officials to discuss these questions. The panel will result is a clearer understanding of what role encryption plays in society, how much in encryption is too much (and too little), and shed light on the current debate about new drives by private actors and the technical community to further encrypt Internet traffic.

[1] James Comey, cited in, Ken gude, "The FBI is Dead Wrong: Apple's Encryption is Clearly in the Public Interest," *Wired* (Nov 17, 2014). Available online at: http://www.wired.com/2014/10/fbi-is-wrong-apple-encryption-is-good/