COLUMBIA | SIPA
School of International and Public Affairs

70 SIPA | WHERE THE WORLD CONNECTS

Global Digital Futures Policy Forum 2016: Issues Brief

Panel 1: Global Security Challenges and Data: Intelligence Gathering, Encryption, and Sharing in a World of ISIS

By David Omand

We are living through the beginnings of a revolution in human affairs enabled by the digitization of information and means of communication through the Internet, web and mobile devices (with the Internet of Things to come). We are now dependent on this technology for our economic and social progress, to deliver international economic development and for our national security and public safety. As set out below, trust has to be built in the open Internet as a safe place to innovate, to do business, to shop and to interact socially, and in the ability of the authorities to be able to uphold the law in cyberspace. That trust cannot be taken for granted.

Conflicting priorities arise at three levels:

- Surveys record increasing *concerns by individuals* for their right to privacy, for protection of their personal information from hackers, from carelessness on the part of corporations, from unrestrained government surveillance, from new techniques such as predictive analytics, and from the very business model of the Internet that rests on the monetization of personal data. One result is the demand for end-to-end encryption, anonymization software, for secure apps and mobile devices and for stronger data protection law. Another is the risk of fragmentation of the Internet as some governments seek to restrict where their citizens' data may be processed or stored.

- At the same time, *law enforcement* expresses growing concern over the way that serious criminals are able to exploit the vulnerabilities of digital technology (and human behavior when using it) to conduct their crimes at scale. Daesh terrorists have been able to use the web to publicize their atrocities and recruit new followers whilst being able to hide their communications from the authorities. Criminal activity using the Internet (including the Dark Net) includes terrorist facilitation, sale of cyber attack exploits, global fraud and money laundering, narcotics trafficking, proliferation of weapons of mass destruction, human trafficking, child sexual abuse and intellectual property theft. Law enforcement is finding it increasingly difficult to counter these threats, to establish the identities of those responsible and to secure the evidence they might have in the past to bring the criminals to justice, especially when they are hiding overseas, or the evidence is in corporate databases in another jurisdiction.

- Meanwhile, *national intelligence agencies* have been able to exploit digital technology to gather information for the protection of national security (the fundamental duty of government) including generating intelligence for military operations and force protection around the world, to support diplomacy and national security policy making and to protect the critical national infrastructure from destructive cyber attacks. At the same time, intelligence agencies have been trying to use their advanced capabilities to assist law enforcement in their mission to keep the public safe, uncovering global criminal networks, and especially tracking terrorists across frontiers. The legal framework for such activity has been shown to be defective or missing altogether in many nations. The exposure of many of these capabilities has heightened the concerns over privacy described above.

As with all hard public policy issues there is no easy way of reconciling competing demands. Place security of personal data and anonymity on the Internet above all else and law enforcement is shut out, the rule of law is undermined, crime, terrorism and cyber attacks will flourish. Prioritize access for law enforcement and intelligence agencies, for example through weakening encryption standards, and confidence in the Internet as a secure medium will be lost and fragmentation of the Internet will spread.

A set of satisficing measures is needed sufficient to ensure respect for *all* our fundamental rights - to the rule of law, to life, to freedom of speech and assembly, to enjoyment of property, to privacy for personal and family life - without lurching to any extreme. In particular, security and privacy should not be traded off one for the other: a sufficiency of both is necessary in a civilized society.

What makes these issues even harder is that solutions have to be found not just nationally but internationally, and in the context of a global struggle over the governance of the Internet itself. Measures are needed that reinforce the nature of the Internet as a secure, open and safe medium, that are technically sound and that make business sense as well as encouraging the 'permissionless' innovation that is the hallmark of the Internet. Government policies might therefore:

- Insist upon continuing multi-stakeholder Internet governance engaging governments, the Internet companies, the tech community and civil society.

- Oppose mandatory data localization and the fragmentation of the Internet into national blocks.

- Maintain the open nature of the Internet where data flows are based upon efficient routing principles and protocols and on open standards openly arrived at.

A promising approach is to encourage in forums such as the OECD, the UN Governmental Group of Experts, the Internet Governance Forum, NETmundial, G20 and the World Summit on the Information Society the development of norms of responsible conduct in cyberspace for like-minded States (accepting that although not all States will initially comply, the reputational cost of bad behavior will be raised). Governments, civil society and the tech community should:

- Insist upon the application of International Humanitarian Law to constrain offensive activity in cyberspace as much as in the everyday physical world.

- Insist upon Governments not weakening or compromising encryption or other standards on which the integrity of the Internet depends. The core infrastructure of the Internet must remain stable and secure.

- Ensure the development of the Internet of Things includes security, and is not based on closed, proprietary systems.

- Enable cyber security partnerships between government agencies, the private sector operators of the critical national infrastructure and the tech community.

- Encourage the development of the cyber insurance industry.

- Insist that any restrictions on Internet content are solely for the purposes of public safety and security and as provided by law and oppose governments trying to shift to the private sector responsibility for policing the content of Internet traffic.

- Encourage the development of new trust architectures, such as may come from blockchain innovation

Governments should, in particular:

- Work to develop common standards of data protection across borders to build confidence in data hosting and processing where most efficient.

- Build effective international information and evidence arrangements to tackle current issues of terrorism, organized global criminality and cyber security. Starting with discussions between the US and the EU seek to reform Mutual Legal Assistance Treaty MLAT processes and develop cyber-MLATs and cross-border arrest warrants for cyber crimes.

To reinforce both security and privacy, governments, civil society and the tech community should:

- Accept the necessity for digital intelligence activity (including, when necessary, access to the Internet in bulk as a legitimate means of gathering foreign intelligence and managing the risks of hostile cyber attacks) but insist all such activity must be covered by the rule of law. Statutory safeguards should involve:

    - Regulation of intelligence and law enforcement agencies stipulating the purposes for which they may acquire secret intelligence and the safeguards for privacy and other human rights that must be applied when intrusive methods are used.

    - Authorization procedures that cover all the ways of accessing digital intelligence: from communications data, the content of communications, interference with equipment (including hacking into adversaries' systems) and the holding and exploitation of databases containing personal information about individuals.

    - Independent judicial and legislative oversight of intrusive intelligence activity.

  - Independent judicial investigation of allegations of abuse and right of redress if proven.

- Apply the principles of the Universal Declaration of Human Rights, accepting that the right to privacy in cyberspace is not absolute where there are legitimate, necessary and proportionate reasons for the authorities to intrude (including 'reasonable searches and seizures' as provided for in the U.S. Constitution's 4th Amendment).

- Accept that law enforcement has the right to seek, with proper authority, evidence relevant to investigations that is held by Internet companies, and that companies have a duty to respond cooperatively where there is no conflict of laws, where the request is legally sound and reasonable in the circumstances, and where to comply with the request would not place at risk unreasonably the security of other users of cyberspace.

- Accept that privacy rights are engaged when the authorities seek bulk access to personal information (in motion or stored). The extent of privacy intrusion, and thus whether it is compatible with privacy rights, depends then upon whether computerized search algorithms to filter, target and select material for analyst examination comply with the principles of lawfulness, necessity and proportionality. Mass surveillance, on the other hand, should be considered unlawful.

- Provide for added protection where legal professional privilege, journalistic material, ministers of religion and legislators are concerned.

- Accept that there are legitimate reasons for enabling anonymity on the Internet, including for use by dissidents in repressive regimes and by journalists to protect their sources but that, as with privacy, it is not an absolute right. In particular, there is no right to anonymity for operation of websites on the dark net.

- Redefine legal thresholds for so that the most revealing forms of meta data such as the complete browsing history of an individual are treated in the same way as content of communications, whilst allowing basic communication data – who called, when, where, for how long, by what means – to remain a basic tool of policing.