CIGI

CHATHAM HOUSE
The Royal Institute of International Affairs

Toward a Social Compact for Digital Privacy and Security

Statement by the Global Commission on Internet Governance

Toward a Social Compact for Digital Privacy and Security

Statement by the Global Commission on Internet Governance

Published by the Centre for International Governance Innovation and Chatham House.

CIGI

67 Erb Street West
Waterloo, Ontario N2L 6C2
Canada
tel +1 519 885 2444 fax +1 519 885 5450
www.cigionline.org

CHATHAM HOUSE
The Royal Institute of International Affairs

10 St James's Square
London, England SW1Y 4LE
United Kingdom
tel +44 (0)20 7957 5700 fax +44 (0)20 7957 5710
www.chathamhouse.org

Contents

Global Commissioners

Carl Bildt
Chair of the Global Commission on Internet Governance

Gordon Smith
Deputy Chair of the Global Commission on Internet Governance

Fen Osler Hampson
Co-Director of the Global Commission on Internet Governance

Patricia Lewis
Co-Director of the Global Commission on Internet Governance

Laura DeNardis
Director of Research of the Global Commission on Internet Governance

Sultan Sooud Al Qassemi
Dominic Barton
Pablo Bello
Pascal Cagni
Moez Chakchouk
Dae-Whan Chang
Michael Chertoff
Dian Triansyah Djani
Anriette Esterhuysen
Hartmut Glaser
Dorothy Gordon
Angel Gurría
Dame Wendy Hall
Melissa Hathaway
Mathias Müller von Blumencron
Beth Simone Noveck
Joseph S. Nye
Sir David Omand
Nii Quaynor
Latha Reddy
Marietje Schaake
Tobby Simon
Michael Spence
Paul Twomey
Pindar Wong

Executive Summary

The Global Commission on Internet Governance (GCIG) was established in January 2014 to articulate and advance a strategic vision for the future of Internet governance. In recent deliberations, the Commission discussed the potential for a damaging erosion of trust in the absence of a broad social agreement on norms for digital privacy and security. The Commission considers that, for the Internet to remain a global engine of social and economic progress that reflects the world's cultural diversity, confidence must be restored in the Internet because trust is eroding. The Internet should be open, freely available to all, secure and safe. The Commission thus agrees that all stakeholders must collaborate together to adopt norms for responsible behaviour on the Internet. On the occasion of the April 2015 Global Conference on Cyberspace meeting in The Hague, the Commission calls on the global community to build a new social compact between citizens and their elected representatives, the judiciary, law enforcement and intelligence agencies, business, civil society and the Internet technical community, with the goal of restoring trust and enhancing confidence in the Internet.

It is now essential that governments, collaborating with all other stakeholders, take steps to build confidence that the right to privacy of all people is respected on the Internet. It is essential at the same time to ensure the rule of law is upheld. The two goals are not exclusive; indeed, they are mutually reinforcing. Individuals and businesses must be protected both from the misuse of the Internet by terrorists, cyber criminal groups and the overreach of governments and businesses that collect and use private data.

A social compact must be built on a shared commitment by all stakeholders in developed and less-developed countries to take concrete action in their own jurisdictions to build trust and confidence in the Internet. A commitment to the concept of collaborative security and to privacy must replace lengthy and over-politicized negotiations and conferences.

The following are the core elements that the Commission advocates in building the new social compact:

- Fundamental human rights, including privacy and personal data protection, must be protected online. Threats to these core human rights should be addressed by governments and other stakeholders acting both within their own jurisdiction and in cooperation.
- Interception of communications, collection, analysis and use of data over the Internet by law enforcement and government intelligence agencies should be for purposes that are openly specified in advance, authorized by law (including international human rights law) and consistent with the principles of necessity and proportionality. Purposes such as gaining political advantage or exercising repression are not legitimate.
- In particular, laws should be publicly accessible, clear, precise, comprehensive and non-discriminatory, openly arrived at and transparent to individuals and businesses. Robust, independent mechanisms should be in place to ensure accountability and respect for rights. Abuses should be amenable to appropriate redress, with access to an effective remedy provided to individuals whose right to privacy has been violated by unlawful or arbitrary surveillance.
- Businesses or other organizations that transmit and store data using the Internet must assume greater responsibility to safeguard that data from illegal intrusion, damage or destruction. Users of paid or so-called "free services" provided on the Internet should know about, and have some choice over, the full range of commercial use on how their data will be deployed, without being excluded from the use of software or services customary for participation in the information age. Such businesses should also demonstrate accountability and provide redress in the case of a security breach.
- There is a need to reverse the erosion of trust in the Internet brought about by the non-transparent market in collecting, centralizing, integrating and analyzing enormous quantities of private information about individuals and enterprises — a kind of private surveillance in the service of "big data," often under the guise of offering a free service.
- Consistent with the United Nations Universal Declaration of Human Rights, communications should be inherently considered private between the intended parties, regardless of communications technology. The role of government should be to strengthen the technology upon which the Internet depends and its use, not to weaken it.
- Governments should not create or require third parties to create "back doors" to access data that would have the effect of weakening the security of the Internet. Efforts by the Internet technical community to incorporate privacy-enhancing solutions in the standards and protocols of the Internet, including end-to-end encryption of data in transit and at rest, should be encouraged.
- Governments, working in collaboration with technologists, businesses and civil society, must help educate their publics in good cyber-security practices. They must also collaborate to enhance the training and development of the software workforce globally, to encourage creation of more secure and stable networks around the world.
- The transborder nature of many significant forms of cyber intrusion curtails the ability of the target state to interdict, investigate and prosecute the individuals or organizations responsible for that intrusion. States should coordinate responses and provide mutual assistance in order to curtail threats, to limit damage and to deter future attacks.

This statement provides the Commission's view of the issues at stake and describes in greater detail the core elements that are essential to achieving a social compact for digital privacy and security.

Introduction: The Opportunities and Risks Emerging from the Internet

In a short period of time, the Internet has become enmeshed in our daily lives. Now, people can exchange text, voice, images and data of all kinds — from anywhere in the world, instantly. We can create content, interact digitally, shop internationally with ease, exchange knowledge and ideas, and work together globally. The Internet, as a network of networks, is already capable of communicating and storing almost unimaginable volumes of data online, including data that can be associated with each of us individually and can be used for good or for ill.

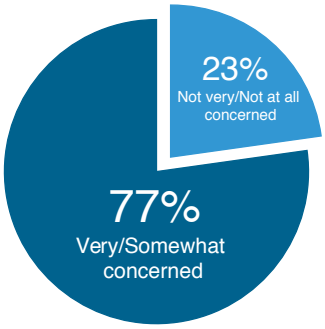
In developed economies, the Internet has already delivered substantial social and economic benefits and is now an essential vehicle for innovation. For the developing world, the Internet can represent a powerful medium for social progress and economic growth, lifting millions of people out of poverty. For those struggling against repressive regimes, it represents a window into the wider world, a voice and a means to mobilize resistance and support. For those wishing to spread violent and hateful ideologies, it represents an unparalleled opportunity to try to radicalize new audiences. For those seeking criminal gains, it represents a way of conducting traditional crimes on a larger scale and conducting new forms of Internet-enabled crime.

It is important to recognize that the communications and data of all of these actors are mixed together in the packet-switched networks and data clouds of the Internet. They all use the same fixed and, increasingly, mobile devices operating with the same Internet protocols. For the authorities charged with tracking down terrorists, countries that conduct espionage, cyber vandals and criminals of all kinds, the Internet provides a reservoir of information about their targets. But at the same time, the ability to access the intermingled data raises concerns over personal privacy and data protection.

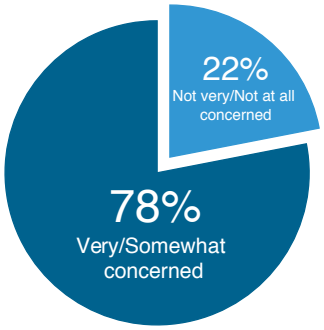
All developed economies now have multiple Internet dependencies. As the global reliance on the Internet rises, the vulnerability to disruption increases. Although Internet access is far from universal, by 2020 the number of Internet users is expected to reach five billion, with each user capable of interacting with any other. The largest portion of this further growth will be in the

developing economies. The opportunities to collect, retain and use data for commercial profit, for harm and criminal gain, and for intelligence and security purposes, will increase commensurately. All stakeholders' capacity to protect fundamental human rights and to respond effectively will need to keep pace.

Public Concern over Hacking of Personal Accounts



Public Concern over Personal Financial Cybercrime



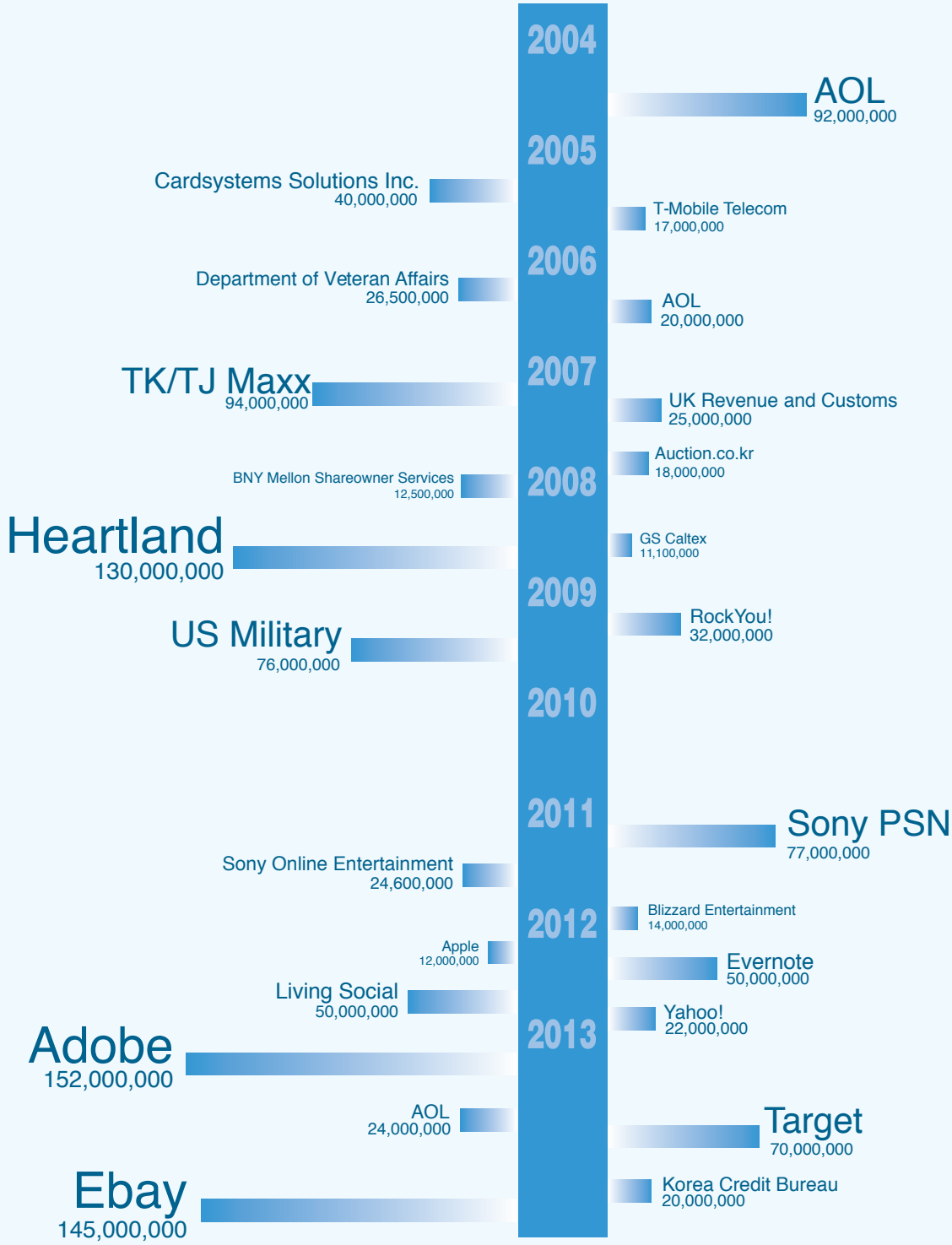
Data source: CIGI-Ipsos Global Survey on Internet Security and Trust. Available at www.cigionline.org/internet-survey.

Note: The CIGI-Ipsos Global Survey was conducted between October 7, 2014, and November 12, 2014. Twenty-four countries were polled, including Australia, Brazil, Canada, China, Egypt, France, Germany, Great Britain, Hong Kong, India, Indonesia, Italy, Japan, Kenya, Mexico, Nigeria, Pakistan, Poland, South Africa, South Korea, Sweden, Tunisia, Turkey and the United States. In total, 23,326 Internet users were polled, aged 18–64 in Canada and the United States, aged 16–64 in every other country.

This shift in the availability of personal, commercial and public sector information, and the potential for access to infrastructure and control systems, represents a new source of vulnerability for society, magnified by the growing use of mobile devices and wireless networks that offer additional ways for networks to be penetrated.

These dangers will be accentuated by the advent of the "Internet of Things" that is already starting to connect the key objects and instruments of daily life — our cars, our homes, our appliances, our clothing and much more. In the emerging world of the Internet of Things, everything we do, see, use or touch will leave electronic tracks, enlarging further both the potential commercial and social value of such data. It also will expand the opportunities provided for police and intelligence agencies to learn more about their suspects. Important questions still have to be addressed concerning the vulnerability of such connected systems and the privacy implications of allowing state and private-sector actors to have access to and to share the big data that they will generate. Similarly, there will be a need to clarify that whatever access there is must have a legal basis.

Data Breaches Affecting over 10 Million



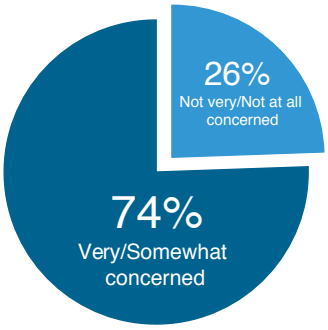
Data source: Business Insider. Available at: www.businessinsider.com/data-breaches-infographic-2014-12.

Individuals, Businesses and Governments Face New Challenges

This data revolution has significant and complex negative implications for three sets of actors: individuals, businesses and governments.

A number of surveys indicate that, for individual and corporate users of the Internet, the primary concern is to have adequate assurance of the security of their information against misuse: the cybercrime, vandalism, theft and even terrorist acts that the Internet enables. Not all individuals understand the full scope of what they have placed online deliberately or what information has been captured and stored by others as they go about their daily activities. Nor do most individuals know to what commercial use their data are deployed.

Internet Users' Concern over Private Company Monitoring of Online Activity and Sale of User-generated Data



Data source: CIGI-Ipsos Global Survey on Internet Security and Trust. Available at www.cigionline.org/internet-survey.

Third parties who have access to data have the potential to monitor, obtain and put to use enormous quantities of private information about individuals and businesses, their communications, their plans, their locations and behaviour, even their shopping, viewing and reading habits. These developments and increasing awareness of them pose a substantial challenge to safety and security, to privacy rights and to citizens' trust in the Internet, which has steadily been eroding. Therefore, these developments are also a substantial threat to the social and economic value of the Internet.

Today, some companies exceed governments in their capacity to collect, store in centralized repositories, integrate, analyze and make use of personal data. These companies are increasingly attractive targets for cyber intrusion, and susceptible to efforts to jeopardize the confidentiality, availability and integrity of these large data pools. These companies have to demonstrate to their users a high level of respect for, and protection of, the security and privacy of their information. At the same time, companies must exhibit corporate social responsibility in responding to government requests for access to their users' data. They also must contend with increasing requests for access to data from law enforcement overseas due to the transborder nature of many activities taking place on the Internet.

Many companies operating on the Internet also are building their businesses on the use and sale of the data they gather. Often the data are accessed in exchange for providing a free service to their users. Data collected from customers are often used for purposes not explicitly revealed to those who provide the data, and used without their permission. On one hand, this is fuelling data analytics to the benefit of innovation. On the other, it raises concerns about the respect for users' privacy. There is a rising call for regulators, or for the industry itself, to establish standards for transparency and accountability mechanisms to increase confidence in the marketplace.

Governments have the responsibility to pursue Internet policies that are consistent with fundamental human rights and the rule of law, and that promote economic well-being. At the same time, they have a duty to address threats from both state and so-called "non-state actors" such as dictators, insurgents, terrorists and other criminals of all kinds. As data and communications of all types moved from traditional telephone and radio technologies to Internet-based transmission, the opportunities for intelligence agencies to monitor such targets by intercepting and exploiting digital data increased. Yet it is difficult for law enforcement officials to interdict and prosecute transnational criminal activity without having assistance from secret intelligence agencies and their powerful tools of digital intelligence gathering. For example, the pattern and content of messages sent between al-Qaeda, Boko Haram, ISIL (Islamic State of Iraq and the Levant) or other terrorist operatives, and those between members of transnational criminal organizations, would be a high priority for interception by the intelligence and law enforcement agencies of many nations. Cooperation may be required to share specialized resources, because a great deal of criminal and socially damaging activity takes place in the deep recesses of the Internet, including the so-called "dark web." Oversight is required to assure citizens that their rights are not infringed upon in the pursuit of a range of bad actors.

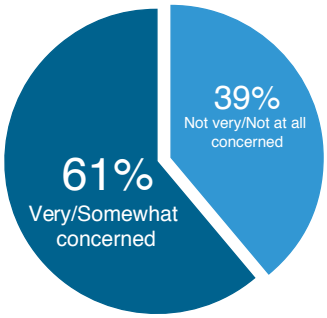
Government activities themselves are vulnerable to terrorists and cyber criminals through the Internet. Many governments are seeking to work with businesses to improve national cyber security to counter the risks of cybercrime, disruption and destruction, especially of critical national infrastructure. These increased risks underscore the importance of governments monitoring threats and attacks online. Nevertheless, some governments are conducting both targeted and mass surveillance in ways that have a chilling effect on fundamental human rights and, in particular, freedom of expression and legitimate dissent and protest, and threatens the realization of the Internet's economic and social benefits.

National and International Responses

The speed of these contradictory developments in the use of the Internet has left policy lagging behind. Governments struggle to know how to manage the harms the Internet facilitates while preserving its power for good.

At a domestic level, responding to pressure from privacy and civil liberties organizations, in several nations a debate has started about the nature, capacity and legal framework of their digital intelligence activities. Some Internet and telecommunications companies now publish transparency reports about the demands governments place on them. Some nations already have comprehensive legislation to regulate intrusive digital intelligence powers; others do not. Some have parliamentary or judicial oversight (or both) of such activity while some do not have either. Personal data protection regulations are mostly not yet suited to the complexity of the digital age — for example, by not adequately regulating the extensive secondary use of personal data or ensuring the transparency of exceptions to privacy for sovereignty and national security purposes. The military utility of offensive cyber operations and intelligence attacks is increasingly recognized, as are the dangers posed by advanced malware and software flaws.

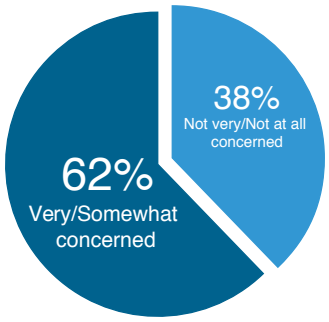
Public Concern over Domestic State Surveillance



Data source: CIGI-Ipsos Global Survey on Internet Security and Trust. Available at www.cigionline.org/internet-survey.

At the international level, all states have subscribed to the UN Universal Declaration on Human Rights, and almost all states have ratified the UN International Covenant on Civil and Political Rights, both of which enshrine the right to privacy in international human rights law. Additionally, some groups of states have usefully developed the right to privacy further, such as in the Convention on Human Rights from the Council of Europe and by implementing the judgments of the European Court of Human Rights. Furthermore, both the NETmundial outcome document and the two recently adopted resolutions from UN General Assembly on the Right to Privacy in the Digital Age affirmed that the same rights that people have offline must also be protected online, including the right to privacy.

Public Concern with Foreign Government Surveillance



Data source: CIGI-Ipsos Global Survey on Internet Security and Trust. Available at www.cigionline.org/internet-survey.

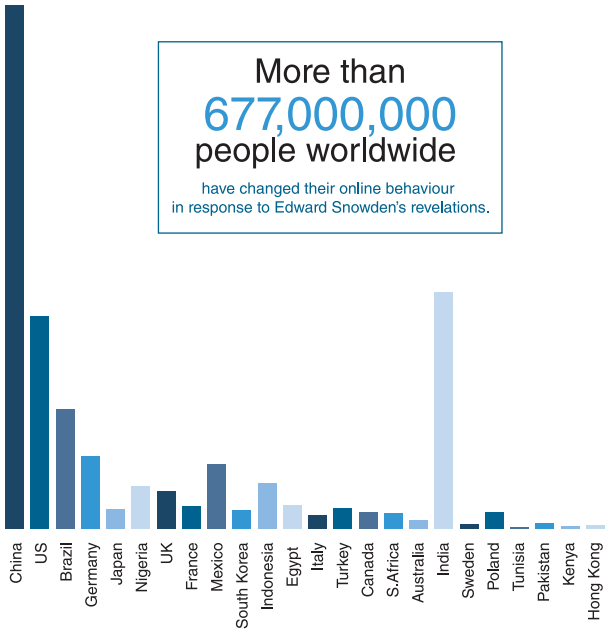
The obligation of states to protect and promote rights to privacy and freedom of expression are not optional. Even if they are not absolute rights, limitations to these rights, even those based on national security concerns, must be prescribed by law, guaranteeing that exceptions are both necessary and proportionate. Governments should guarantee the same human rights protection to all individuals within their borders. Clearly, any interference with the right to privacy should not be arbitrary or unlawful, bearing in mind what is reasonable to the pursuance of legitimate aims. The Organisation for Economic Co-operation and Development (OECD) Privacy Guidelines state that exceptions to its principles, including those relating to national sovereignty, national security and public policy (ordre public), should be as few as possible, and made known to the public. The 2013 International Principles on the Application of Human Rights to Communications Surveillance, developed at the initiative of civil society, are an important reference regarding how international human rights law should apply in the current digital environment. States are called to comply with the following principles: legality, legitimate aim, necessity, adequacy, proportionality, competent judicial authority, due process, user notification, transparency, public oversight, integrity of communications and systems, safeguards for international cooperation, safeguards against illegitimate access and the right to effective remedy.

Formal and informal efforts such as these are early steps in the emergence of a new social compact for the digital age.

Core Elements of a Social Compact for a Digital Society

There must be a mutual understanding between citizens and their state that the state takes responsibility to keep its citizens safe and secure under the law while, in turn, citizens agree to empower the authorities to carry out that mission, under a clear, accessible legal framework that includes sufficient safeguards and checks and balances against abuses. Business must be assured that the state respects the confidentiality of its data and they must, in turn, provide their customers the assurance that their data is not misused. There is an urgent need to achieve consensus on a social compact for the digital age in all countries. Just how urgent is shown by current levels of concern over allegations of intrusive state-sponsored activities ranging from weakening of encryption to large-scale criminal activity, to digital surveillance, to misuse of personal data and even to damaging cyber attacks and disruption.

Online Behavioural Change in Response to Edward Snowden's Revelations



Data source: CIGI-Ipsos Survey on Internet Security and Trust, available at www.cigionline.org/internet-survey and World Bank Indicators on Population and Internet Penetration Rates, available at http://data.worldbank.org/indicator.

In an environment of rapidly changing technologies and social attitudes, a normative approach would be a practical starting point for such an effort. Key elements of a social compact for the digital age will necessarily take different institutional and legal forms in different societies and cultures. Nevertheless, a global social compact should be informed by a number of core elements:

- Fundamental human rights, including privacy and personal data protection, must be protected online. Threats to these core human rights should be addressed by governments and other stakeholders acting both within their own jurisdiction and in cooperation.

- Interception of communications, collection, analysis and use of data over the Internet by law enforcement and government intelligence agencies should be for purposes that are openly specified in advance, authorized by law (including international human rights law) and consistent with the principles of necessity and proportionality. Purposes such as gaining political advantage or exercising repression are not legitimate.

- In particular, laws should be publicly accessible, clear, precise, comprehensive and non-discriminatory, openly arrived at and transparent to individuals and businesses. Robust, independent mechanisms should be in place to ensure accountability and respect for rights. Abuses should be amenable to appropriate redress, with access to an effective remedy provided to individuals whose right to privacy has been violated by unlawful or arbitrary surveillance.

- Businesses or other organizations that transmit and store data using the Internet must assume greater responsibility to safeguard that data from illegal intrusion, damage or destruction. Users of paid or so-called "free services" provided on the Internet should know about, and have some choice over, the full range of commercial use on how their data will be deployed, without being excluded from the use of software or services customary for participation in the information age. Such businesses should also demonstrate accountability and provide redress in the case of a security breach.

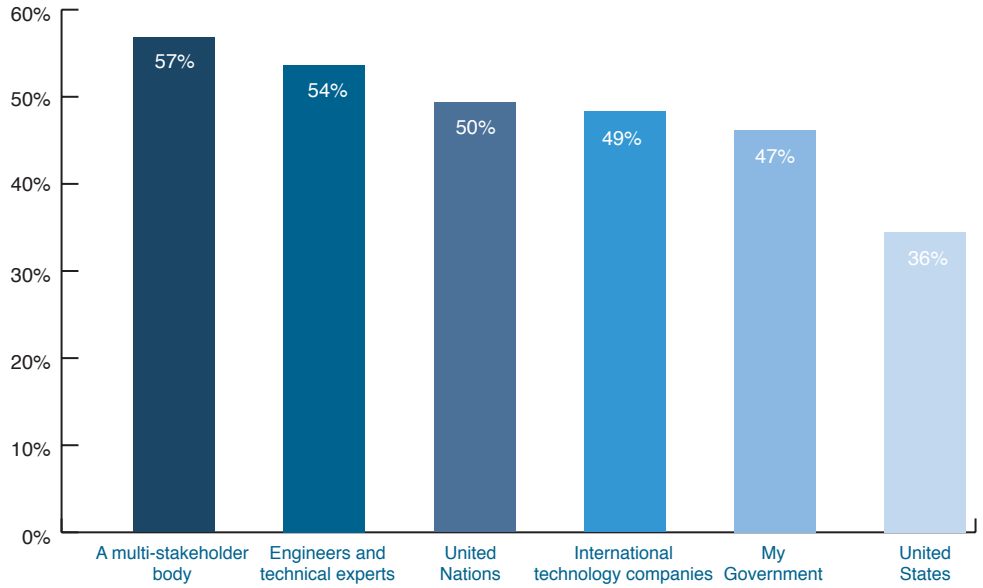
- There is a need to reverse the erosion of trust in the Internet brought about by the non-transparent market in collecting, centralizing, integrating and analyzing enormous quantities of private information about individuals and enterprises — a kind of private surveillance in the service of "big data," often under the guise of offering a free service.
- Consistent with the United Nations Universal Declaration of Human Rights, communications should be inherently considered private between the intended parties, regardless of communications technology. The role of government should be to strengthen the technology upon which the Internet depends and its use, not to weaken it.
- Governments should not create or require third parties to create "back doors" to access data that would have the effect of weakening the security of the Internet. Efforts by the Internet technical community to incorporate privacy-enhancing solutions in the standards and protocols of the Internet, including end-to-end encryption of data in transit and at rest, should be encouraged.
- Governments, working in collaboration with technologists, businesses and civil society, must help educate their publics in good cyber-security practices. They must also collaborate to enhance the training and development of the software workforce globally, to encourage creation of more secure and stable networks around the world.
- The transborder nature of many significant forms of cyber intrusion curtails the ability of the target state to interdict, investigate and prosecute the individuals or organizations responsible for that intrusion. States should coordinate responses and provide mutual assistance in order to curtail threats, to limit damage and to deter future attacks.

Moving toward a Social Compact for a Digital Society

The social compact for a digital society will require a very high level of agreement among governments, private corporations, individuals and the technical community. Governments can provide leadership, but cannot alone define the content of the social compact. Achieving agreement and acceptance will necessitate the engagement of all stakeholders in the Internet ecosystem. At first, it is unlikely that a universal social compact suitable to all circumstances could, or even should, be the immediate goal. The Internet is used and valued across all cultures and all borders. Significant changes of attitude can sometimes evolve more quickly and more flexibly than could be possible through negotiated treaties or international legal instruments. In the fullness of time, national approaches may gain recognition as good international practices, and may eventually acquire the status of customary international law. But that is many years away, and the speed of technological change argues for flexibility and innovative solutions. The area of secret intelligence is especially difficult to regulate since there is little international law governing it, but even that largely secret domain ought not to be free of ethical and legal considerations.

The social compact will contribute to building a new kind of "collaborative privacy and security." The term highlights a fundamental truth about the Internet: every part of the Internet ecosystem affects every other part. Thus, the new social compact is not about "balancing" human rights and privacy against states' interests or against commercial rights. It is about ensuring that a framework exists where each actor has the responsibility to act not only in their own interest, but also in the interest of the Internet ecosystem as a whole. By definition, the process should result in outcomes that are win-win rather than zero-sum games. Effective security, successful business models and human rights are mutually reinforcing in the long run. All interests must recognize and act on their responsibility for security and privacy on the Internet in collaboration with all others, or no one is successful.

The Public's Preference for Multi-stakeholder Governance



Data source: CIGI-Ipsos Global Survey on Internet Security and Trust. Available at www.cigionline.org/internet-survey.

In the end, it is in the interest of all stakeholders that the Internet remains trusted as a common global resource: open, affordable, unfettered and available to all as a safe medium for further innovation. Government, business and civil society must work together toward that aim.

Conclusion

These recommendations are put forward by the Global Commission on Internet Governance to encourage a strong consensus among all stakeholders that the benefits of the Internet for humankind must not be put at risk, whether by disproportionate state behaviour in cyberspace, by criminal activity or by business activity undermining assurance in the confidentiality, integrity and availability of information on the Internet. Advancing a new normative framework, which accounts for the dynamic interplay between national security interests and the needs of law enforcement, while preserving the economic and social value of the Internet, is an important first step to achieving long-term digital trust. The Commission is committed to building on this statement by continuing its program of research and publication, undertaken in collaboration with partners from all sectors.

Acknowledgements

The Commissioners wish to thank Bill Graham, CIGI senior fellow, and Aaron Shull, CIGI fellow, for their assistance in drafting this statement, Eric Jardine, CIGI research fellow, for preparing the charts and figures that appear in the document, and Samantha Bradshaw, CIGI research associate, for her research assistance.

Further Reading

In developing this Statement, Commissioners drew upon a number of publications that outline the issues of trust, privacy and security. A partial list of the works consulted and others recommended for further research can be found at: www.ourinternet.org. This is a representative list only, and is not intended to be complete or comprehensive.

Barnes, R. et al. 2015. "Confidentiality in the Face of Pervasive Surveillance: A Threat Model and Problem Statement." Network Working Group, Internet Engineering Task Force. www.ietf.org/id/draft-iab-privsec-confidentiality-threat-04.txt.

Bartlett, J. and Alex Krasodomski-Jones. 2015. "Online Anonymity, Islamic State and Surveillance." Demos. www.demos.co.uk/files/Islamic_State_and_Encryption.pdf?1426713922.

Bildt, C. 2013. Speech by Foreign Minister Carl Bildt at Seoul Conference on Cyberspace 2013, Seoul, October 17. Utrikesdepartementet, Sweden. www.government.se/sb/d/7956/a/226592.

Chertoff, M. and Tobby Simon. 2015. *The Impact of the Dark Web on Internet Governance and Cyber Security.* GCIG Paper No. 6. Waterloo: CIGI and Chatham House. https://ourinternet-files.s3.amazonaws.com/publications/GCIG_Paper_No6.pdf.

CIGI/IPSOS. 2014. "Global Survey on Internet Security and Trust." Waterloo: CIGI. www.cigionline.org/internet-survey.

Daigle, L. 2015. *On the Nature of the Internet.* GCIG Paper No. 9. CIGI and Chatham House. https://ourinternet.org/#publications/on-the-naure-of-the-internet.

Electronic Frontier Foundation et al. 2014. "The International Principles on the Application of Human Rights to Communications Surveillance." May. https://en.necessaryandproportionate.org/.

Internet Society. 2015. "Internet Society Approach to Cyber Security Policy." Internet Society. January 22. www.internetsociety.org/news/internet-society-approach-cyber-security-policy.

Internet Society. 2015. "Understanding Security and Resilience of the Internet." Internet Society. www.internetsociety.org/sites/default/files/bp-securityandresilience-20130711.pdf.

La Rue, F. 2013. *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue*. United Nations General Assembly: Human Rights Council. www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

NETmundial. 2014. "NETmundial Draft Outcome Statement." Global Multistakeholder Meeting on the Future of Internet Governance. http://document.netmundial.br/net-content/uploads/2014/04/NETmundial-draft-outcome-document_April_14.pdf .

Nye. J. 2014. *The Regime Complex for Managing Global Cyber Activities*. GCIG Paper No. 1. Waterloo: CIGI and Chatham House. www.cigionline.org/sites/default/files/gcig_paper_no1.pdf.

OECD. 2013. *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (The Privacy Guidelines)*. OECD. www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf.

OECD. 2014. *OECD Principles for Internet Policy Making*. OECD. www.oecd.org/sti/ieconomy/oecd-principles-for-internet-policy-making.pdf.

Office of the High Commissioner for Human Rights. 2004. "Nature of the General Legal Obligation on States Parties to the Covenant." General Comment 31, Office of the High Commissioner for Human Rights. www1.umn.edu/humanrts/gencomm/hrcom31.html.

Omand, David. 2015. *Understanding Digital Intelligence and the Norms That Might Govern It*. GCIG Paper No. 8. Waterloo: CIGI and Chatham House. https://ourinternet-files.s3.amazonaws.com/publications/gcig_paper_no8.pdf.

Scheinin, M. 2010. *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, Martin Scheinin*. United Nations General Assembly: Human Rights Council. https://fas.org/irp/eprint/unhrc.pdf.

United Nations. 2011. "Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework." United Nations Human Rights Council Resolution 17/4. www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.

United Nations. 2012. "Brazil and Germany: Draft Resolution: The Right to Privacy in the Digital Age." Draft Resolution: Sixty-Eighth Session, Third Committee, UN General Assembly. www.hrw.org/sites/default/files/related_material/UNGA_upload_0.pdf.

United Nations. 2015. "The Right to Privacy in the Digital Age." Resolution Adopted by the UN General Assembly on December 18, 2014. www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/69/166.

Verhulst, Stefaan G. et al. 2014. *Innovations in Global Governance: Toward a Distributed Governance Ecosystem*. GCIG Paper No. 5. Waterloo: CIGI and Chatham House. https://ourinternet-files.s3.amazonaws.com/publications/gcig_paper_no5.pdf.

Weber, R. 2014. *Legal Interoperability as a Tool for Combatting Fragmentation*. GCIG Paper No. 4. Waterloo: CIGI and Chatham House. https://ourinternet-files.s3.amazonaws.com/publications/gcig_paper_no4.pdf.

About CIGI

The Centre for International Governance Innovation is an independent, non-partisan think tank on international governance. Led by experienced practitioners and distinguished academics, CIGI supports research, forms networks, advances policy debate and generates ideas for multilateral governance improvements. Conducting an active agenda of research, events and publications, CIGI's interdisciplinary work includes collaboration with policy, business and academic communities around the world.

CIGI's current research programs focus on three themes: the global economy; global security & politics; and international law.

CIGI was founded in 2001 by Jim Balsillie, then co-CEO of Research In Motion (BlackBerry), and collaborates with and gratefully acknowledges support from a number of strategic partners, in particular the Government of Canada and the Government of Ontario.

Le CIGI a été fondé en 2001 par Jim Balsillie, qui était alors co-chef de la direction de Research In Motion (BlackBerry). Il collabore avec de nombreux partenaires stratégiques et exprime sa reconnaissance du soutien reçu de ceux-ci, notamment de l'appui reçu du gouvernement du Canada et de celui du gouvernement de l'Ontario.

For more information, please visit www.cigionline.org.

About Chatham House

Chatham House, the Royal Institute of International Affairs, is based in London. Chatham House's mission is to be a world-leading source of independent analysis, informed debate and influential ideas on how to build a prosperous and secure world for all. The institute: engages governments, the private sector, civil society and its members in open debates and confidential discussions about significant developments in international affairs; produces independent and rigorous analysis of critical global, regional and country-specific challenges and opportunities; and offers new ideas to decision-makers and -shapers on how these could best be tackled from the near- to the long-term. For more information, please visit: www.chathamhouse.org.

CIGI Masthead

Managing Editor, Publications	Carol Bonnett
Publications Editor	Jennifer Goyder
Publications Editor	Vivian Moser
Publications Editor	Patricia Holmes
Publications Editor	Nicole Langlois
Graphic Designer	Melodie Wakefield
Graphic Designer	Sara Moore

Executive

President	Rohinton Medhora
Vice President of Programs	David Dewitt
Vice President of Public Affairs	Fred Kuntz
Vice President of Finance	Mark Menard

Communications

Communications Manager	Tammy Bender tbender@cigionline.org (1 519 885 2444 x 7356)

CIGI

67 Erb Street West
Waterloo, Ontario N2L 6C2, Canada
tel +1 519 885 2444 fax +1 519 885 5450
www.cigionline.org

CHATHAM HOUSE
The Royal Institute of International Affairs

10 St James's Square
London, England SW1Y 4LE
United Kingdom
tel +44 (0)20 7957 5700 fax +44 (0)20 7957 5710
www.chathamhouse.org