Working Paper
For circulation at the 2017 Global Digital Futures Forum
May 5, 2017

COLUMBIA|SIPA
School of International and Public Affairs

The Future of Global Cyber Trust:

Fragmentation v. Universality Tradeoffs[i]

May, 2017

By Dr. Laura DeNardis[ii]

1. Introduction

Commerce, speech, social life, and every imaginable industrial sector are now digitally mediated and therefore contingent upon the security and integrity of Internet infrastructure. Emerging technological advances such as cyber physical systems, cryptocurrencies, and artificial intelligence raise the stakes of network stability significantly. What are the implications of these trust dependencies on modern society and the Internet itself? Until societies experience economic or social upheaval, the role of trust in maintaining societal stability exists as a taken for granted background context of daily life. Individuals trust that financial institutions will secure their bank accounts, cars will not malfunction, airplanes will stay in the sky, and medical test results remain confidential. Democracies depend upon the integrity of voting systems and commercial transactions rely upon trust between buyers and sellers. What has changed in recent decades is that all of these trust dependencies now also depend upon the integrity and security of underlying digital infrastructure.

Even while societal dependencies on digital infrastructure mount, there is evidence of some loss of trust in this very infrastructure and its governing institutions. Some of this loss of trust stems from actions in the political realm, whereby governments establish policies, such as data localization laws or national cybersecurity measures, to enhance national sovereignty or address privacy concerns about foreign intelligence gathering practices. Loss of trust among Internet users arises from rising awareness of government surveillance and private sector data gathering practices, as well as high-profile cybersecurity breaches, including the massive data breaches at Yahoo!, Target, and the US Office of Personnel Management (OPM).

The 2017 CIGI-Ipsos Survey on Internet Security and Trust, polling more than 24,000 users in 24 countries, found that a majority of respondents were more concerned about privacy than they had been in the previous year, partly related to cybercrime but, increasingly, also due to concerns about their own

governments (CIGI-Ipsos 2017). The poll indicated that only half of respondents trust their governments to act responsibly online.

Trust has always been a requirement for keeping the Internet operational, but society is approaching a tipping point in which significant improvements in digital trust are necessary to sustain a global digital economy and public sphere. Indeed, many of the most contentious global policy issues in the cyber arena involve struggles over trust: in the stability of infrastructure, voting systems, digitally mediated news, the security and privacy of user data, the authenticity of information and users, and commercial transactions. Not surprisingly, considerable policy and scholarly attention has focused on these issues, and especially, the close association between cybersecurity technologies and trust policies (Schneider 1998, Singer & Friedman 2014, Hampson & Jardine 2016).

Constructions of trust in cyberspace will affect whether the Internet continues to expand into a universal network or fragment into segments enclosed by geopolitical borders or proprietary market ecosystems. A great deal of policy and scholarly attention has examined tensions between Internet universality and fragmentation (Werbach 2008, Force Hill 2010, DeNardis 2016, Drake et al., 2016, Mueller 2017). What has been addressed less is the more narrow policy intersection between cyber trust and fragmentation. Can digital trust and Internet universality co-exist in the long term in light of technological and geopolitical changes facing the Internet? There is a moment of opportunity to examine intersections between digital trust and fragmentation and explore which future solutions – public policy, market approaches, civil society interventions, and technical design – can foster the trust necessary for the stability and security of digital systems while also enabling a universal Internet supporting digital trade, freedom of expression, and access to knowledge.

2. Digital Trust Points as a Precursor to Internet Universality

The Internet is not a single network but an interconnected collection of mostly privately owned networks able to interoperate because they adhere to common sets of standards for formatting and exchanging information. Trust between network operators has always been a requirement for this interconnection, just like trust between trading partners is necessary for the global digital economy to function. Each autonomous system advertises the routes (i.e. collections of Internet Protocol addresses) reachable through that network using Border Gateway Protocol (BGP). Historically, network operators have trusted adjacent networks to advertise accurate routes, although security breaches certainly occur

at these borders. The ability to access information on a website from anywhere in the world similarly depends upon trust in the Internet's Domain Name System (DNS), the globally distributed system that translates domain names into corresponding Internet addresses locating information online. Trust in the DNS is a necessary precursor for the Internet to globally operate. Technical infrastructure trust mechanisms such as public key cryptography authentication are increasingly engineered into these systems.

Even though the digital economy has experienced tremendous growth – the Internet has more than 3 billion Internet users and contributes more than $4 trillion USD to the global economy – the Internet is not yet universal. Viewed through the lens of physical infrastructure and bandwidth, nearly half the world still does not have access and, among those who do, access speeds vary considerably (ITU 2015). At the logical, software-defined layer of the Internet, there is also fragmentation, such as the use of the DNS to carry out censorship and other content controls. At the application and content layer, the Internet is not yet universal because of language differences, including barriers to universal accommodation of internationalized domain names (IDNs) that incorporate non-Latin characters such as those used in Arabic, Chinese, and Cyrillic text. Regional policies block content locally, such as the Right to be Forgotten in the European Union, the geo-IP restriction of Netflix in Canada, and systems of censorship and blocking in China and elsewhere. Fragmentation of networks for security reasons, via firewalls and virtual private networks, is of course the norm for most corporate networks. This choice to create fragmentation for security reasons is quite distinct from fragmentation that is not a user choice. Overall, the Internet has continued to expand globally because of trust among networks, between websites and browsers, and in common technical standards and systems of routing and addressing.

3. Geopolitical Trust Tensions Are Creating Fragmentation

Despite the historical growth trajectory of the Internet, several geopolitical trust problems are creating digital fragmentation. Values of privacy, security, and national sovereignty increasingly conflict with values of universality and the free flow of information across borders. Some of these conflicts arise from problems of jurisdiction, as well as incongruities between technological and nation-state boundaries. The virtual architecture of the Internet and the cross-border nature of data flows are often incommensurable with political borders. While routers make decisions about the flow of information based on engineering optimization rather than geography, what counts as privacy, hate speech,

indecency, and freedom of expression, differs greatly across geopolitical borders. Legal authority over citizens and institutions within borders does not comport well with the cross-border and distributed nature of cyberspace. Interoperability and harmonization of Internet policies across borders can prevent Internet fragmentation, but cultivating cultural and political agreement on many Internet policy issues can be an intractable problem, even in areas such as intellectual property rights enforcement and cybercrime. The jurisdictionally complex task of enforcing laws often falls to private intermediaries, creating a privatization of governance unprecedented in the contemporary era.

A trust-related example of attempts to harmonize national borders with virtual borders involves the introduction of data localization laws placing constraints on how private companies (e.g. banks, retail, or technology companies) handle customer data, including requirements that data be stored on servers within a nation's borders (Chander and Le 2015). The rationales for these policies often cite concern about customer privacy in the context of foreign surveillance, even though concentrating data in a fixed location can facilitate efficient surveillance and create a host of technical complexities and economic costs (Bauer, et al. 2016).

Governments increasingly view control of Internet infrastructure as a proxy for state power, whether motivated by national security, cyber war concerns, censorship, or economic objectives. China and other countries seeking greater control over information flows have advocated for top-down, bordered, government-centric cyber sovereignty approaches that supplant traditional private sector led governance approaches in the name of cyber order (DeNardis, Goldstein and Gross 2016). Some of these efforts to assert cyber sovereignty arise from lack of trust in the institutions that govern the Internet and raise the possibility of fragmentation not only of digital networks but of the global governance structures tasked with keeping networks operational.

4. Emerging Trust Terrains: IOT, Currency, and AI

Emerging technological innovations raise the stakes of digital trust and also challenge some prevailing assumptions that the goal of a universal Internet is always in the public interest. Internet of Things (IOT) projections envision the ability to interconnect an estimated 50 billion objects to the global Internet. The diffusion of the Internet into material objects - remote sensor devices, health monitoring devices, home appliances, traffic systems, and networked vehicles – raises the stakes for digital trust. For example, a disruption of a network-connected cardiac implant threatens human safety rather than simply

the ability to communicate. Digitally dependent and digital-only cryptographic currencies also continue to gain traction, often outside of traditional regulatory frameworks. What trust mechanisms are necessary to preserve confidence, integrity, and security in financial systems? As decisions about how information is organized and how data is analyzed move to machine learning and artificial intelligence systems, new systems of accountability and human safety will be necessary to instill trust in digital environments.

5. Framing Questions for the Panel

Fragmentation as a Context-Dependent Value. Given threats from cyberattacks, cybercrime, and geopolitically motivated Internet conflict, and considering that the cyber realm now includes industrial control systems, medical devices, vehicles and other human safety-related contexts, is fragmentation necessarily something that should be minimized? Conversely, in highly trust dependent areas, under what conditions is fragmentation actually desirable?

The Tension between Privacy/Security and Universality. Can values of privacy and security, and the trust solutions necessary to sustain these values co-exist with norms of Internet universality?

Trust as a Precursor for Universality. Where Internet universality has positive economic and social effects (e.g. freedom of expression, global commerce), what are the most pressing trust dependencies necessary for the growth of the global digital economy and digital public sphere?

Trust Solutions. What solutions - in technical architecture, market approaches, government policies, and international agreements – hold the most promise to create trust conditions necessary for an appropriate balance between Internet universality and fragmentation?

Emerging Trust Dependencies. What policy solutions of today can address emerging technological phenomena such as artificial intelligence, cryptographic currencies, and cyber physical systems?

Reference

1. Bauer, Matthias, Martina Ferracane and Erik van der Marel (2016). "Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localization," *Global Commission on Internet Governance Papers Series* No. 30, May. Accessed at https://ourinternet-files.s3.amazonaws.com/publications/ gcig_no30web.pdf.
2. Chander, Anupam and Uyen Le (2015). "Data Nationalism," *Emory Law Journal*, Vol. 64, No. 3.
3. CIGI-Ipsos Global Survey on Internet Security and Trust, April 2017. Accessed at https://www.cigionline.org/internet-survey.
4. DeNardis, Laura (2016). One Internet: An Evidentiary Basis for Policy Making on Internet Universality and Fragmentation, Global Commission on Internet Governance, GCIG Paper No. 38, July 19. Accessed at https://www.cigionline.org/publications/one-internet-evidentiary-basis-policy-making-internet-universality-and-fragmentation.
5. DeNardis, Laura, Gordon Goldstein, and David A. Gross (2016), "The Rising Geopolitics of Internet Governance: Cyber Sovereignty v. Distributed Governance," Columbia SIPA Working Paper, November 30.
6. Drake, William J., Vinton G. Cerf and Wolfgang Kleinwächter (2016) "Internet Fragmentation: An Overview." World Economic Forum Future of the Internet Initiative White Paper, January. Accessed at www3.weforum.org/docs/WEF_FII_ Internet_Fragmentation_An_Overview_2016.pdf.
7. Force Hill, Jonah (2012). "Internet Fragmentation: Highlighting the Major Technical, Governance and Diplomatic Challenges for U.S. Policy Makers," Belfer Center for Science and International Affairs, Harvard Kennedy School. Accessed at http://belfercenter.ksg.harvard.edu/files/ internet_fragmentation_jonah_hill.pdf.
8. Hampson, Fen Osler and Eric Jardine (2016). Looks Who's Watching: Surveillance, Treachery and Trust Online, Center for International Governance Innovation (CIGI) Press.
9. ITU (2015). International Telecommunication Union (ITU), "ICT Facts and Figures – The World in 2015," 2015. Accessed at http://www.itu.int/en/ITU-D/Statistics.
10. Mueller, Milton (2017). *Will the Internet Fragment? Sovereignty, Globalization and Cyberspace*, Polity Press.
11. Schneider, Fred B., ed. (1998). *Trust in Cyberspace*, National Academy of Science Press.

12. Singer, P.W. and Allan Freidman (2014). *Cybersecurity and Cyber War: What Everyone Needs to Know*, Oxford University Press.
13. Werbach, Kevin (2008). "The Centripetal Network: How the Internet Holds Itself Together, and the Forces Tearing it Apart," *University of California Davis Law Review*.

---

[i] Background Thought Piece - Digital Futures Policy Forum Panel: Developing Trust and Assurance

[ii] Adjunct Senior Research Scholar, Columbia SIPA, Professor, American University