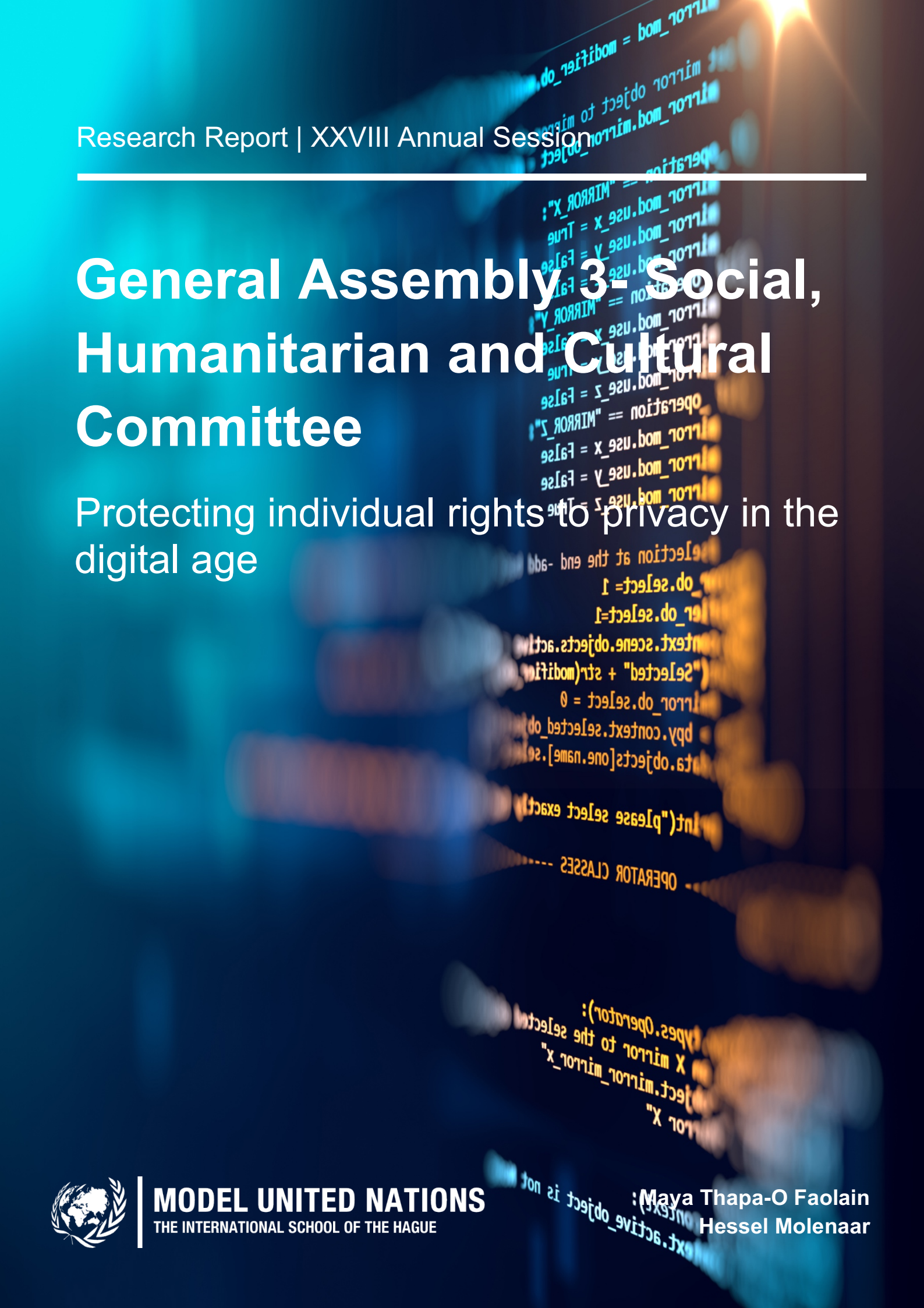
Research Report | XXVIII Annual Session

General Assembly 3- Social, Humanitarian and Cultural Committee

Protecting individual rights to privacy in the digital age



MODEL UNITED NATIONS
THE INTERNATIONAL SCHOOL OF THE HAGUE

Maya Thapa-O Faolain
Hessel Molenaar

Forum:	General Assembly 3
Issue:	Protecting individual rights to privacy in the digital age
Student Officer:	Hessel Molenaar
Position:	Deputy chair

Introduction

The Internet is a site where we trade our privacy for services. Ever since the World Wide Web was created in 1991, there has been no binding law that was enforced on the Internet, partly because there is no real way to indicate a jurisdiction, so enforcing the law is difficult. Even at this point in time, the Internet is a place that one can use as one sees fit. People could use the Internet to store all our data, look through our devices and restore information we might have thrown out, use the cameras on our devices and know the location of our devices at any given time. In the digital era, people live their lives online, however not everyone is aware that everything they do online is being monitored and stored. Big corporations will track your online footprint from the moment you use their site. Hence, your privacy is worth more to these big corporations than it is to you. On the web, the users are not the customers: they are the product because big corporations create vast capital with their personal information. By using these devices and online services on a daily basis, we open ourselves up to mass surveillance and the inability of having privacy. Nowadays, however, it seems impossible to live without these devices and services as a lot of us use them for our work or school, and without them, we wouldn't be able to keep up. Hence, the Internet should have clear regulations that ensures that no party is violating privacy and so create a safe and private place for all people to use.

There is, furthermore, the problem of trying to regulate the internet. Internet regulation is extremely difficult for governments to manage because new technologies are cropping up at an exponential rate and many specialised teams of hackers are constantly finding ways to evade privacy regulations that are imposed. As such, governments are enormously tasked with trying to find strategies which can effectively counter the progress made by hackers and illegitimate organisations. Additionally, it is vital that governments allow their citizens to access the internet with as complete freedom as is possible without unnecessary censorship. To find this balance is something governments and other large-scale legitimate organisations have been confronted with as a significant challenge in recent years.

The key ways in which violations of privacy occur are through people giving out details and believing that the person or organisation to whom they are giving them is legitimate and will not use these in a nefarious way. As such, hackers and phishers often exploit people's trust in them by interfering in their WhatsApp messages, asking for their bank card details and then performing illegitimate transactions that essentially amount to theft. The people, caught up in the idea of, for example, selling something online, or making large amounts of money through a trade deal, are wont to ignore the warning signs and give

out their details in any event. The main reasons these violations of privacy occur can be summarised in two words: information and money. The harvesting of information allows the hackers to blackmail or exploit people by threatening them with the exposure of sensitive information. Similarly, for power gain, the other critical reason such privacy violations occur is so that the hackers can quickly and easily gain large sums of money. While there are many nuances in both of these situations, these are the key factors, and most privacy violations that occur can be found to trace back to these core reasons.

Definition of Key terms

Cookie

A small text file created by a website that is stored in the user's computer either temporarily for that session only or permanently on the hard disk. It is way to track your preferences throughout surfing the web. Cookies are commonly given as examples of ways that websites remember a person and can be hard to mitigate if one wishes to be 'forgotten' on the Internet.

Deep packet inspection (DPI)

Deep packet inspection (DPI) technology is a form of computer network packet filtering that examines the data and possibly also the header of a packet, as it passes an inspection point, searching for protocol non-compliance, viruses, spam, and intrusions.

Digital age

The 'digital age' or 'information age' is defined as the era of technological development starting in the 1970's, heralded by the introduction of the personal computer. It signaled the rise of the ability to transfer information freely and quickly, and is relevant to the topic at hand due to the era in which the Internet and social media has progressed in the last 30 years.

Internet privacy

Internet privacy is defined as: the privacy and security level of personal data published via the Internet. It is a broad term that refers to a variety of factors, techniques and technologies used to protect sensitive and private data, communications, and preferences. Internet privacy and anonymity are paramount to users, especially as e-commerce continues to gain traction. Privacy violations and threat risks are standard considerations for any website under development. Risks may include phishing, pharming, spyware and malware.

IP address

An IP Address or “identity protocol” address identifies one through their computer on a local network. IP addresses are the way to identify users and their actions in the cyber sphere, which can lead to infringing on rights to privacy by corporations and national intervention.

Mass surveillance

Mass surveillance is the intricate surveillance of an entire or a substantial fraction of a population in order to monitor that group of citizens. [1] The surveillance is often carried out by governments or governmental organisations, but may also be carried out by corporations, either on behalf of governments or at their own initiative.

Malware

An application used to illegally damage online and offline computer users through Trojans, viruses and spyware.

Pharming

An Internet hacking activity used to redirect a legitimate website visitor to a different IP address.

Phishing

An Internet hacking activity used to steal secure user data, including username, password, bank account number, and security PIN or credit card number. Spyware An offline application that obtains data without a user's consent. When the computer is online, previously acquired data is sent to the spyware source.

General Overview

Before the digital age, life was not as internationally connected as today, news spread on paper, people talked in person or via letters and it wasn’t until the telephone, that people could make appointments on short notice.

World Wide Web

Since the launching of the World Wide Web, the world stated to connect. Through the easy and immediate access to talk to anyone anywhere anytime the world started to speed up. This also created an ideal platform for the dissemination of knowledge, where people are also encouraged to participate and use this for their own personal growth.

Conjointly with the devices that allow us to use this platform anytime and anywhere, we cannot imagine a world without the Internet, which is what makes us even more

vulnerable to exploitation through the Internet. In article 12 of the Declaration of Humans Right it is stated that: “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his Honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.” This article, however, is binding to all UN member nations, and has yet to be applied to the Internet. With that in mind, the mass surveillance that multiple governments practice is illegal according to article 12 on privacy of the Declaration of human rights.

NSA

In June 2013, Edward Snowden blew the whistle on the USA National Security Agency. He leaked classified information on the mass surveillance of hundreds of millions of people, whose phone calls, emails and searches were stored. There was a direct court order to Verizon to hand over all its telephone data to the NSA on an “on-going daily basis”. Furthermore, the NSA tapped directly into the servers of nine Internet firms, including Facebook, Google and Yahoo, which had as goal to track online communication in a surveillance program known as Prism. This surveillance clearly violates act 12 of the Universal Declaration of Human Rights with the key word arbitrary, which means based on random choice. Edward currently faces espionage charges in the United States of America (USA) but has been granted temporary asylum in the Russian Federation.

China

In 2015, China had a worse Internet connection to the rest of the world in relation to the previous year, but other than that, no other country’s Internet connection has deteriorated. All nations are improving their connection to the Internet and thereby the world. This deterioration of China’s connection is caused by the extreme censorship China is upholding. The most powerful monitoring body in China is the Communist Party’s Central Propaganda Department (CPCPD) that employs over two million workers that review Internet posts by using keyword searches. China has also recently instated the rating system, where citizens will be awarded points by what they search online and who their friends are. In accordance to their rating, they will be granted more freedom and privileges.
Moreover, the Chinese government has the Golden Shield Programme in place, colloquially known as the Great Firewall. This firewall makes large-scale use of Deep Packet Inspection technology to block access based on keyword detection. This makes all outside services, music or video content nearly impossible to reach for the average Chinese person. All these efforts made by the Chinese party strive towards Chinese digital sovereignty. Nowadays,

there still is a huge risk that your information will be used for certain purposes which they should have not. In the picture to the right you will find the distribution of the risks.

Major Parties Involved

European Union (EU)

Within the EU, a new organ, called the European Union General Data Protection Regulation (EUGDPS), has been created to form an independent authority. It ensures the upholding of data protection laws.

Human Rights Watch (HRW)

The Human Rights Watch is a NGO which is the largest organisation with advocates for human rights. They have taken it upon themselves to create dialog on the abuse of human rights on the Internet. The organisation does research on human rights as well. Their headquarter is located in New York but also has centres in cities such as Amsterdam and Nairobi.

People's Republic of China

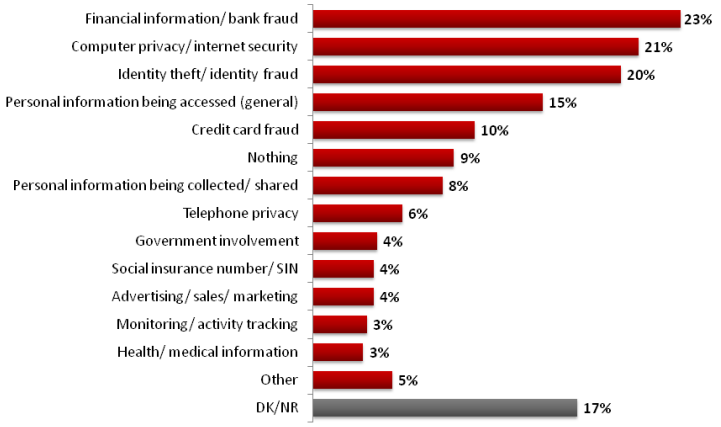
The People's Republic of China is a country where the Internet and the press is largely controlled by the government and as such, aims to create a digital sovereign State. Recently, the State has implemented the rating system that arbitrarily violates their citizen's privacy. Citizens and tourists have to use VPN to surf on the World Wide Web.

Privacy International

Privacy International is an UK based NGO that challenges governments' powers by advocating and litigating for stronger protections. They lead research and investigations to shine a light on powers and capabilities, and to instigate and inform debate. They advocate for good practices and strong laws worldwide to protect people and their rights. They equip civil society organisations across the world to increase public awareness about privacy. Privacy International raises awareness about technologies and laws that place privacy at risk, in order to ensure that the public is informed and engaged.

Figure 3: Perceived Risks to Privacy of Greatest Concern

Q4: What risks to your privacy concern you the most, if any?



Phoenix SPI for OPC: December 2012

Base: All; n=1513

United States of America (USA)

Ever since Edward Snowden, the United States of America has been front and centre in the issue of privacy on the Internet. Former president Barack Obama had taken some steps towards better Internet Privacy, however, president Donald Trump says that he would prioritise national security over respecting people's privacy on the Internet.

Timeline of Key Events

Timeline of events in reverse chronological order leading up to present day.

Date	Description of Event
14th of April 2016	The European Parliament adopted the Regulation
8th of April 2016	The European Council adopted the regulation
5th of June 2013	Edward Snowden releases NSA documents sparking huge controversy
January, 2012	The European commission proposed a regulation to reform the data protection rules in the EU
2007	US Congress passes and anti-terror surveillance bill, allowing the PRISM program
1975	First Personal computers are introduced, marking the beginning of the digital age
4th of November 1952	The National Security Agency of the United States (NSA) was founded
10th of December 1948	The Universal Declaration of Human Rights (UDHR) was adopted, stating the right to privacy as a fundamental human right

Previous Attempts to Resolve the Issue

The UN has until now not made any major steps towards the solving of this issue. Within the EU, however, there has made significant progress towards solving the issue. In March 2012, the European Court of Justice proposed the creation of the European Union General Data Protection Regulation (EUGDPR) that protects users from unauthorised data storage and tracking. It also ensures that all corporations follow the European data protection laws and are able to fine all non-compliant corporations. With this organisation instated, the EU is far ahead of the International community.

The United Nations General Assembly adopted resolution 68/167 in December 2013. This resolution expressed the possibility of the negative impact which interception of communications may have on human rights. In addition to that, the resolution expressed concern on negative consequences of surveillance. The General Assembly was of the opinion that people should have the same rights, whether it is online or offline. Upon that, the General Assembly urged all nations to respect the rights and protect the privacy in digital communication of their people.

Possible Solutions

A solution might be to educate people about their digital footprint, seeing that there still are a lot of people who are not aware that they are being tracked and their data is being stored. With knowledge, these people will be able to fully understand the Internet and take control and seeing the impact of their Internet use. A second solution might be an international variant of the EUGDPR that ensures that all organizations throughout the entire world will be forced to respect their user's privacy. Such an organisation must be a third party and should not be controlled by a group of member states. A third solution might be defining the legality of surveillance. Many nations already have digital surveillance in place, however, with regulations that will legalise some supportive forms of surveillance, delegates will be able to ensure that less privacy will be violated.

Appendices

Appendix A

http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/71/L.39/Rev.1

Appendix B

https://www.eugdpr.org

Appendix C

www.privacyinternational.org

Appendix D

https://theslot.jezebel.com/internet-privacy-explained-for-people-who-have-never-th-1794112859

Appendix E

https://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx

Appendix F

https://www.rollingstone.com/politics/news/edward-snowden-inspires-global-treaty-for-online-privacy-20150924

Appendix G

https://heinonline.org/HOL/LandingPage?handle=hein.journals/gwilr42&div=28&id=&page=

Bibliography

1. “Arthur W. Diamond Law Library Research Guides.” *International Internet Law* - Research Guides, library.law.columbia.edu/guides/International_Internet_Law.

2. “Edward Snowden: Leaks That Exposed US Spy Programme.” *BBC News*, BBC, 17 Jan. 2014, www.bbc.com/news/world-us-canada-23123964.

3. “Universal Declaration of Human Rights.” *United Nations*, United Nations, www.un.org/en/universal-declaration-human-rights/.

4. “What Is Internet Privacy?” *Techopedia.com,* www.techopedia.com/definition/24954/Internet-privacy.

5. “When It Comes to Internet Privacy, Be Very Afraid, Analyst Suggests.” *Harvard Gazette,* 24 Aug. 2017, news.harvard.edu/gazette/story/2017/08/when-it-comes-toInternet-privacy-be-very-afraid-analyst-suggests/.

6. Doctorow, Cory. “The Curious Case of Internet Privacy.” *MIT Technology Review,* MIT Technology Review, 30 Dec. 2013, www.technologyreview.com/s/428045/thecurious-case-of-Internet-privacy/.

7. Jeavans, Adam Blenford & Christine. “After Snowden: How Vulnerable Is the Internet?” *BBC News*, 27 Jan. 2014, www.bbc.com/news/technology-25832341.

8. “Media Censorship in China.” *Council on Foreign Relations*, Council on Foreign Relations, www.cfr.org/backgrounder/media-censorship-china.

9. Privacy International. “Cyber Security.” *Privacy International*, www.privacyinternational.org/topics/cyber-security.

10. Privacy International. “Data Protection.” *Privacy International*, www.privacyinternational.org/topics/data-protection.

11. Privacy International. “Government Hacking.” *Privacy International*, www.privacyinternational.org/topics/government-hacking.

12. Privacy International. “Identity and Privacy.”*Privacy International*, www.privacyinternational.org/topics/identity-and-privacy.

13. Privacy International. “Social Media Intelligence.” *Privacy International*, www.privacyinternational.org/node/55.

14. Theintercept. “NSA Deletes ‘Honesty’ and ‘Openness’ From Core Values.” *The Intercept*, 24 Jan. 2018, theintercept.com/2018/01/24/nsa-core-values-honestydeleted/.