Committee: Special Conference on Technological Advances and their Impact

Topic: User privacy and access in the digital world

Student Officer: Daphne Loupa

Position: Deputy President

PERSONAL INTRODUCTION

Dear delegates,

My name is Daphne Loupa and I am an IB2 student at the Moraitis School. In the 7th session of CSMUN, I will be serving as the deputy president in the Special Conference on Technological Advances and their Impact, which will be my first time chairing.

The purpose of this study guide is to equip delegates with information on the topic at hand, i.e. user privacy and access in the digital world, which will assist in their proper understanding of what is to be discussed during the conference. That being said, I hope it is of help to you and should you have any questions, feel free to contact me at daphneloupa@gmail.com.

I wish you all an enjoyable and productive conference and I am looking forward to meeting you all.

Sincerely,

Daphne Loupa

INTRODUCTION

With the emergence and popularization of new digital technologies, it is evident that new issues to address arise as well. Hence, a pressing matter as of recently is the way in which data can be protected and accessed online.

The internet has become a vast network containing data from millions of users, which, without the proper regulation, is easily available. Therefore, it is important to take the appropriate actions so as to ensure its protection.

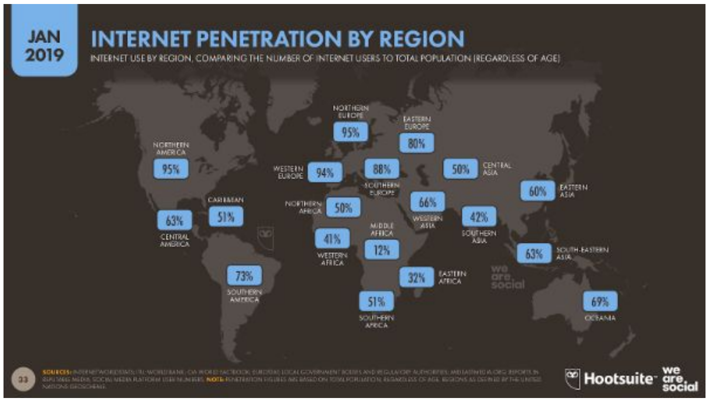


Figure 1: Internet users compared to population 2019[1]

DEFINITION OF KEY TERMS

Information privacy

One of the four classes of privacy, along with territorial privacy, bodily privacy, and communications privacy. The claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others. [2]

Information security

[1] "Digital 2019: Global Internet Use Accelerates." *We Are Social*, 30 Jan. 2019, wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates.

[2] "International Association of Privacy Professionals." *Glossary*, iapp.org/resources/glossary/.

The protection of information for the purposes of preventing loss, unauthorized access and/or misuse. It is also the process of assessing threats and risks to information and the procedures and controls to preserve confidentiality, integrity and availability of information.[3]

Authorization

When referring to digital privacy, authorization refers to the process by which the end user allows for the use of certain information.[4]

Outsourcing

The contracting of third-parties for certain business processes. An example for outsourcing is the collection of privacy information by advertising agencies through website such, but not limited to, Facebook and Twitter.[5]

Data breach

The unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a data collector. Breaches do not include good faith acquisitions of personal information by an employee or agent of the data collector for a legitimate purpose of the data collector—provided the personal information is not used for a purpose unrelated to the data collector's business or subject to further unauthorized disclosure.[6]

[3] Ibid.
[4] Ibid.
[5] Ibid.
[6] Ibid.

BACKGROUND INFORMATION

Computer Privacy vs Internet Privacy

Computer privacy entails the protection of a computer's hardware, software and information from potential attack or harm. However, with the emergence of the internet and online networks, the issue has transformed completely and become much more complicated. Due to the increasing reliance on online networks, information stored in computers is much more susceptible to attacks and the general safety of such data is largely compromised since it is now possible to access a computer's database without physical contact. Hence, if an operator has given way for a "loophole" in a system (e.g. poor configuration, weak passcodes, etc.), it is much easier for data to be accessed.[7]

Privacy vs Profit

It is evident that internet data collection is highly prevalent among businesses. Businesses retrieve data mainly by three means. Namely, by asking consumers to share their information directly, by tracking them, and by supplementing the data they have collected using other sources. For example, producers make note of their customers' activity on social media, or even location activity. Another emerging source of personal data collected by corporations is the "internet of things", which allows them to instill stricter surveillance on consumers.

Once the mass of information has been collected, it is filtered out through the use of A.I. After it is refined, it is used in a myriad of ways. Besides improving business strategy or refining the customers' experience with the company and its products, businesses tend to convert such information into direct revenue. More specifically, it is often sold to advertisers. This has given way to a multi-billion dollar industry called "AdTech", which allows advertisers to profile users

[7] 2019, https://www.researchgate.net/publication/298807979_Computer_Security_and_Mobile_Security_Challenges. Accessed 10 July 2019.

and target ads. These advertisements tend to be highly discriminatory (e.g. based on gender) and manipulative (as advertisers personally target one consumer based on their user data).[8]

Privacy vs Security

However, it is not only businesses that want to collect such data. Governments tend to pressure tech companies to share such information and it is evident that the demand from governments for data is increasing drastically.

In certain cases, governments are willing to go to extreme lengths to retrieve information. For example, they might be inclined to steal information from the private sector, as seen in Wire's 2013 report on the NSA's taps on the data links used by Google and Yahoo.

For the most part, user data is useful to governments for the purpose of maintaining security. For example, they intend to collect information on terrorist organizations. Another use is in elections. For instance, user information is used in order to determine where to hold rallies, where to focus resources and how to profile voters.[9]

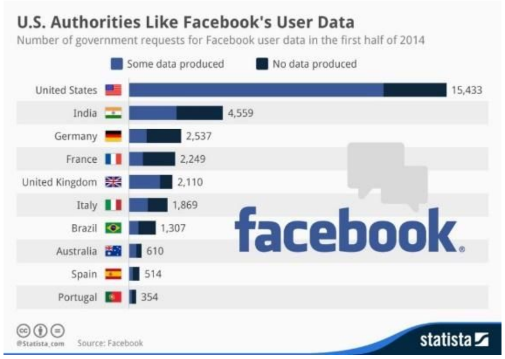


Figure 2: Government requests for Facebook data[10]

[8] Uzialko, Adam C. "How and Why Businesses Collect Consumer Data." *Business News Daily*, 3 Aug.

[9]"AdTech." *Privacy International*, privacyinternational.org/topics/adtech., Ijaz, Rehan. "Government Agencies Are Gaining New Data Collection Tools in 2018." *SmartData Collective*, 27 Apr. 2018, www.smartdatacollective.com/government-agencies-gaining-new-data-collection-tools/.Rubinstein, et al. "Systematic Government Access to Personal Data: a Comparative Analysis †." *OUP Academic*, Oxford University Press, 1 May 2014, academic.oup.com/idpl/article/4/2/96/734798.

[10] Facebook Infographics. "U.S. Authorities Like Facebook's User Data." *SiteProNews*, 18 Nov. 2014, www.sitepronews.com/2014/11/20/u-s-authorities-like-facebooks-user-data-2/.

Cybersecurity

No matter how secure a network may be, it is still susceptible to breaches. Such breaches are possible for multiple reasons. For instance, weak or stolen access codes and simple errors may give way for hackers to access significant sensitive information. Considering the amount of personal user data online, it is evident that a data breach could be detrimental for user privacy.[11]

This is especially important in the case of national cybersecurity. For this reason, states have adopted certain strategies that ensure a nation's digital data's safety. For instance, certain states choose to strengthen and secure infrastructure or to create collaborations with the private sector so as to ensure digital security to a larger extent. Examples of such strategies include the EU's NCSS[12], or the United States' Cybersecurity Strategy.[13]

TIMELINE OF EVENTS

Date	**Description of event**
November 2005	Eruption of Sony XCP scandal
August 2006	AOL search word leak
June 2013	Edward Snowden's documents on the NSA published
August 2013	Yahoo data breach with 1 billion accounts accessed
Summer 2014	JPMorgan data breach with 76 million accounts accessed
Late 2014	Yahoo data breach with 500 million accounts accessed
March 21, 2018	Zuckerburg's confession concerning Facebook's data collection
November 2018	Marriot data breach with 500 million reservation details accessed

[11] "8 Most Common Causes of Data Breach." *Sutcliffe Insurance*, 8 Oct. 2018, www.sutcliffeinsurance.co.uk/news/8-most-common-causes-of-data-breach/.

[12] "National Cyber Security Strategies". *Enisa.Europa.Eu*, 2019, https://www.enisa.europa.eu/topics/national-cyber-security-strategies.

[13] *Whitehouse.Gov*, 2019, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

UN INVOLVEMENT

The UN's first resolution on internet privacy was signed in 14 December of 1990, titled "Guideline for the regulation of computerized personal data files". Since then, the UN has approached the issue in various other resolutions. For example, GA3's resolution on internet privacy, adopted on 21 November 2016, which highlights the need to protect the right to privacy. Of course, the UN's HRC's work on the matter is notable. For instance, in April 2015, the HRC appointed the Special Rapporteur on the right to privacy, whose responsibilities included to protect the right to privacy in the context of new technologies.[14]

COUNTRIES AND ORGANIZATIONS INVOLVED

USA

The USA's NSA has been criticized for its violation of internet privacy to a large extent. Namely, the NSA's PRISM programme, exposed by Edward Snowden in 2013, which allowed the US government to track civilians' activity on the internet without a warrant, e.g. emails, calls, chats, was heavily scrutinized.[15] After this reveal, certain developments in favour of data protection have been made. For example, in 2015 a federal appeals court deemed the surveillance of phone records by the US government illegal, and hence the practice of service providers handing over records to the state was banned.[16] However, it is evident that, despite

[14] "A/RES/45/95. Guidelines for the Regulation of Computerized Personal Data Files." *United Nations*, United Nations, www.un.org/documents/ga/res/45/a45r095.htm. , "Right to Privacy in the Digital Age." *OHCHR*, www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx. , "Principles on Personal Data Protection and Privacy." *Principles on Personal Data Protection and Privacy | United Nations System Chief Executives Board for Coordination*, www.unsceb.org/principles-personal-data-protection-and-privacy. , "New UN Resolution on the Right to Privacy in the Digital Age: Crucial and Timely." *Internet Policy Review*, policyreview.info/articles/news/new-un-resolution-right-privacy-digital-age-crucial-and-timely/436.

[15] Toomey, Patrick. "The NSA Continues to Violate Americans' Internet Privacy Rights." *American Civil Liberties Union*, American Civil Liberties Union, 23 Aug. 2018, www.aclu.org/blog/national-security/privacy-and-surveillance/nsa-continues-violate-americans-internet-privacy.

[16] Abdo, Alex. "NSA, Unplugged: The Government Finally Stopped Vacuuming Up Our Phone Records." *American Civil Liberties Union*, American Civil Liberties Union, 30 Nov. 2015, www.aclu.org/blog/national-security/privacy-and-surveillance/nsa-unplugged-government-finally-stopped-vacuuming?redirect=blog%2Fspeak-freely%2Fnsa-unplugged-government-finally-stopped-vacuuming.

such policy changes, the NSA still collects a mass of data, as it continues to cooperate and exchange online data with its UK counterpart, GCHQ.[17]

Russia

In the Russian Federation, internet privacy is heavily restricted. Namely, internet companies are obliged to store at least 6 months of data and to be able to hand it over to the Russian government on demand. Hence, 175 sites have been asked to turn in data to the government, e.g. the dating app Tinder.[18] Furthermore, in April 2019, the Russian government signed a bill that would allow a system in which the country's internet users would be isolated from online international activity. This would make censorship much easier to achieve, as well as allow greater access to users' private information whenever the parliament deems it is necessary to activate the system.[19]

EU

It is evident that the EU has made significant attempts to protect user privacy in the digital world. The most recent example is the General Data Protection Regulation (GDPR), which came into effect in spring of 2018. In this way, the EU constructed a basic set of standards in order to ensure that EU citizens' data would be handled correctly.[20]

Privacy International

Privacy International is a charity organization whose sole purpose is to protect the right to privacy. Actions include campaigns and research and investigations in order to uncover

[17] "Why Do We Still Accept That Governments Collect And Snoop On Our Data?" *Privacy International*, privacyinternational.org/feature/1671/why-do-we-still-accept-governments-collect-and-snoop-our-data.

[18] Vasilyeva, Nataliya. "Russia Demands Tinder Shares User Data With Secret Services." *Time*, Time, 3 June 2019, time.com/5599925/russia-tinder-user-data-privacy/.

[19] Doffman, Zak. "Putin Signs 'Russian Internet Law' To Disconnect Russia From The World Wide Web." *Forbes*, Forbes Magazine, 1 May 2019, www.forbes.com/sites/zakdoffman/2019/05/01/putin-signs-russian-internet-law-to-disconnect-the-country-from-the-world-wide-web/#6ba82c781bf1.

[20] "What Is the General Data Protection Regulation? Understanding & Complying with GDPR Requirements in 2019." *Digital Guardian*, 15 May 2019, digitalguardian.com/blog/what-gdpr-general-data-protection-regulation-understanding-and-complying-gdpr-data-protection.

violations. For example, one of Privacy International's actions has been to uncover the so-called "Big Brother Inc", a set of technology firms investing in surveillance.[21]

Open Rights Group

Open Rights Group is a campaigning organization that specifically deals with protecting rights in the digital world. More specifically, they launch campaigns and lobbying, address to the media and deal with legal matters concerning digital privacy.[22]

POSSIBLE SOLUTIONS

Due to the severity of the issue and its implications for individual privacy, it is important to find the adequate solutions to resolve the issue.

Firstly, it is important to establish stricter regulation on corporations and governments that collect such data. For example, corporations could be required to set specific requirements for how data is handled and who is allowed to handle it. This could include creating a classification system and demanding for the appropriate handling based on the classification (e.g. where the information can be stored, whether it has to be encrypted, etc.). [23]Furthermore, it is important to establish an authorization system for the staff that handles and processes such data, which would check whether the person's access to the data is explicitly mentioned in business documents and if accessing such data is within their professional duties. Of course, it is vital to establish the appropriate accountability measures concerning data leaks and breaches for staff handling sensitive information.[24]

Secondly, it is evident that bringing about reforms such as the improvement of consent disclosures would allow users to have more control on their data. In the case of consent

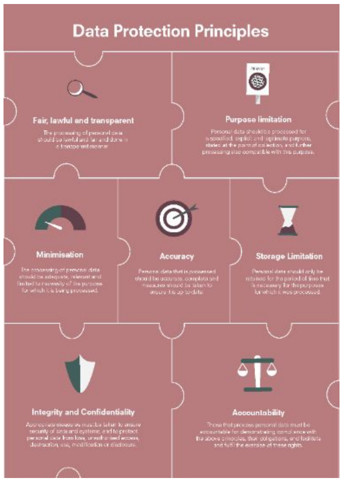
[21] "Uncovering Big Brother Inc." *Privacy International*, privacyinternational.org/impact/uncovering-big-brother-inc.
[22] "About." *Open Rights Group*, www.openrightsgroup.org/about/.
[23] "Guideline For Data Handling | Information Technology Services". *Itservices.Uncc.Edu*, 2019, https://itservices.uncc.edu/iso/guideline-data-handling. Accessed 9 July 2019.
[24] "INTERNAL RULES FOR THE PROCESSING AND PROTECTION OF PERSONAL DATA | Job Trust HR". *Jobtrust.Gr*, 2019, https://jobtrust.gr/en/gdrp/internal-rules-for-the-processing-and-protection-of-personal-data.

disclosures, as shown by research from Carnegie Mellon, if one were to read all website privacy policies in full, it would take 25 days out of a year.[25] Therefore, it is evident that users are highly unlikely to be informed about sites' privacy policies and consent disclosures as they are simply too extensive. Hence, it is vital in order to improve information amongst internet users to improve such disclosures and policies.

Thirdly, it could be beneficial to reconsider the legal age of broadcasting personal information online. In the fight for ensuring internet privacy, it is important to protect minors and their right to privacy. This is especially significant considering that minors and young users in general are the most avid users of social media sites and mobile networks and also considering that minors are especially sensitive groups when it comes to data protection.[26]

Fourthly, for the sufficient tackling of the issue, it is significant to establish a UN body specifically targeting the issue of digital user privacy. In this way, there would be sufficient focus on the matter from the international community. Of course, it follows that all nations should be encouraged to follow the guidelines set by the international community, for example guidelines in documents such as the EU's GDPR.

Finally, another solution could be to promote personal choices that ensure to an extent data privacy. For example, users could be encouraged to install VPN programs and take other personal steps towards securing their personal information from data breaches or data collection. Such personal steps could be promoted through seminars directed to the general public, or more specifically targeted events (e.g. events in schools and education facilities). Such seminars and events could be an opportunity to raise greater awareness on the subject in


Data Protection Principles
Fair, lawful and transparent
The processing of personal data should be lawful and fair and done in a transparent manner.
Purpose limitation
Personal data should be processed for a specified, explicit and legitimate purpose, stated at the point of collection, and further processing also compatible with this purpose.
Minimisation
The processing of personal data should be adequate, relevant and limited to necessity of the purpose for which it is being processed.
Accuracy
Personal data that is processed should be accurate, complete and measures should be taken to ensure it is up to date.
Storage Limitation
Personal data should only be retained for the period of time that is necessary for the purpose for which it was processed.
Integrity and Confidentiality
Appropriate measures must be taken to ensure security of data and systems, and to protect personal data from loss, unauthorised access, destruction, use, modification or disclosure.
Accountability
Those that process personal data must be accountable for demonstrating compliance with the above principles, their obligations, and facilitate and fulfil the exercise of these rights.

[25] Madrigal, Alexis C. "Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days." *The Atlantic*, Atlantic Media Company, 1 Mar. 2012, www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/.

[26] *Mayerbrown.Com*, 2019, https://www.mayerbrown.com/-/media/files/perspectives-events/publications/2015/07/childs-play-protecting-the-privacy-of-minors-onlin/files/get-the-full-update/fileattachment/150720-hkg-privacy-tmt-socialmedia.pdf.

general and to ensure public information on the subject. The same principle could be adopted by companies so as to prevent data breaches which are a significant risk to the security of sensitive information of users.

Bibliography

"International Association of Privacy Professionals." *Glossary*, iapp.org/resources/glossary/.

Uzialko, Adam C. "How and Why Businesses Collect Consumer Data." *Business News Daily*, 3 Aug. 2018, w ww.businessnewsdaily.com/10625-businesses-collecting-data.html. , "AdTech." *Privacy International*, privacyinternational.org/topics/adtech

"AdTech." *Privacy International*, privacyinternational.org/topics/adtech.

Ijaz, Rehan. "Government Agencies Are Gaining New Data Collection Tools in 2018." *SmartData Collective*, 27 Apr. 2018, www.smartdatacollective.com/government-agencies-gaining-new-data-collection-tools/.Rubinstein, et al. "Systematic Government Access to Personal Data: a Comparative Analysis †." *OUP Academic*, Oxford University Press, 1 May 2014, academic.oup.com/idpl/article/4/2/96/734798.

"8 Most Common Causes of Data Breach." *Sutcliffe Insurance*, 8 Oct. 2018, www.sutcliffeinsurance.co.uk/news/8-most-common-causes-of-data-breach/.
"A/RES/45/95. Guidelines for the Regulation of Computerized Personal Data Files." *United Nations*, United Nations, www.un.org/documents/ga/res/45/a45r095.htm.

"Right to Privacy in the Digital Age." *OHCHR*, www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx.

"Principles on Personal Data Protection and Privacy." *Principles on Personal Data Protection and Privacy | United Nations System Chief Executives Board for Coordination*, www.unsceb.org/principles-personal-data-protection-and-privacy.

"New UN Resolution on the Right to Privacy in the Digital Age: Crucial and Timely." *Internet Policy Review*, policyreview.info/articles/news/new-un-resolution-right-privacy-digital-age-crucial-and-timely/436.

Toomey, Patrick. "The NSA Continues to Violate Americans' Internet Privacy Rights." *American Civil Liberties Union*, American Civil Liberties Union, 23 Aug. 2018, www.aclu.org/blog/national-security/privacy-and-surveillance/nsa-continues-violate-americans-internet-privacy. ,

Vasilyeva, Nataliya. “Russia Demands Tinder Shares User Data With Secret Services.” *Time*, Time, 3 June 2019, time.com/5599925/russia-tinder-user-data-privacy/.

“What Is the General Data Protection Regulation? Understanding & Complying with GDPR Requirements in 2019.” *Digital Guardian*, 15 May 2019, digitalguardian.com/blog/what-gdpr-general-data-protection-regulation-understanding-and-complying-gdpr-data-protection.

“Uncovering Big Brother Inc.” *Privacy International*, privacyinternational.org/impact/uncovering-big-brother-inc.

“About.” *Open Rights Group*, www.openrightsgroup.org/about/.

Madrigal, Alexis C. “Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days.” *The Atlantic*, Atlantic Media Company, 1 Mar. 2012, www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/.

Digital Security Risk Management For Economic And Social Prosperity OECD Recommendation And Companion Document. 1st ed., 2015, https://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf. Accessed 9 July 2019.

Mayerbrown.Com, 2019, https://www.mayerbrown.com/-/media/files/perspectives-events/publications/2015/07/childs-play-protecting-the-privacy-of-minors-onlin/files/get-the-full-update/fileattachment/150720-hkg-privacy-tmt-socialmedia.pdf.

Helimun.Com, 2019, http://helimun.com/sites/default/files/The%20Right%20to%20Privacy%20in%20the%20Digital%20Era%20ECOSOC.pdf.

"INTERNAL RULES FOR THE PROCESSING AND PROTECTION OF PERSONAL DATA | Job Trust HR". *Jobtrust.Gr*, 2019, https://jobtrust.gr/en/gdrp/internal-rules-for-the-processing-and-protection-of-personal-data.

Pagliery, Jose. "'Sony-Pocalypse': Why The Sony Hack Is One Of The Worst Hacks Ever". *Cnnmoney*, 2019, https://money.cnn.com/2014/12/04/technology/security/sony-hack/index.html.

"National Cyber Security Strategies". *Enisa.Europa.Eu*, 2019, https://www.enisa.europa.eu/topics/national-cyber-security-strategies.

Whitehouse.Gov, 2019, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

Marsan, Carolyn, and Network World. "15 Worst Internet Privacy Scandals Of All Time". *Pcworld*, 2019, https://www.pcworld.com/article/248811/15_worst_internet_privacy_scandals_of_all_time.html.

Jessica Silver-Greenberg, Matthew Goldstein and Nicole Perlroth. "Jpmorgan Chase Hacking Affects 76 Million Households". *Dealbook*, 2019, https://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/?mtrref=www.google.com&gwh=43EAE3486369568FEEA4F52D6C643BB1&gwt=pay.

"Https://Time.Com". *Time*, 2019, https://time.com/5467773/marriott-data-breach/.

2019, https://www.researchgate.net/publication/298807979_Computer_Security_and_Mobile_Security_Challenges. Accessed 10 July 2019.

Facebook Infographics. “U.S. Authorities Like Facebook's User Data.” SiteProNews, 18 Nov. 2014, www.sitepronews.com/2014/11/20/u-s-authorities-like-facebooks-user-data-2/.

Doffman, Zak. “Putin Signs 'Russian Internet Law' To Disconnect Russia From The World Wide Web.” Forbes, Forbes Magazine, 1 May 2019, www.forbes.com/sites/zakdoffman/2019/05/01/putin-signs-russian-internet-law-to-disconnect-the-country-from-the-world-wide-web/#6ba82c781bf1.

Abdo, Alex. “NSA, Unplugged: The Government Finally Stopped Vacuuming Up Our Phone Records.” American Civil Liberties Union, American Civil Liberties Union, 30 Nov. 2015, www.aclu.org/blog/national-security/privacy-and-surveillance/nsa-unplugged-government-finally-stopped-vacuuming?redirect=blog%2Fspeak-freely%2Fnsa-unplugged-government-finally-stopped-vacuuming.

“Why Do We Still Accept That Governments Collect And Snoop On Our Data?” Privacy International, privacyinternational.org/feature/1671/why-do-we-still-accept-governments-collect-and-snoop-our-data.

“Digital 2019: Global Internet Use Accelerates.” We Are Social, 30 Jan. 2019, wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates.

“Data Privacy Week: Working Towards Change.” Privacy International, privacyinternational.org/long-read/2666/data-privacy-week-working-towards-change.