The Right to Privacy in the Digital Age

April 9, 2018

Dr. Keith Goldstein, Dr. Ohad Shem Tov, and Mr. Dan Prazeres

Presented on behalf of Pirate Parties International Headquarters, a UN ECOSOC Consultative Member, for the Report of the High Commissioner for Human Rights

Our Dystopian Present

Living in modern society, we are profiled. We accept the necessity to hand over intimate details about ourselves to proper authorities and presume they will keep this information secure- only to be used under the most egregious cases with legal justifications. Parents provide governments with information about their children to obtain necessary services, such as health care. We reciprocate the forfeiture of our intimate details by accepting the fine print on every form we sign- or button we press. In doing so, we enable second-hand trading of our personal information, exponentially increasing the likelihood that our data will be utilized for illegitimate purposes.

Often without our awareness or consent, detection devices track our movements, our preferences, and any information they are capable of mining from our digital existence. This data is used to manipulate us, rob from us, and engage in prejudice against us- at times legally. We are stalked by algorithms that profile all of us. This is not a dystopian outlook on the future or paranoia. This is present day reality, whereby we live in a data-driven society with ubiquitous corruption that enables a small number of individuals to transgress a destitute mass of phone and internet media users.

In this paper we present a few examples from around the world of both violations of privacy and accomplishments to protect privacy in online environments. The examples provided are not exhaustive, representative, nor the gravest examples. Further research is necessary that will incorporate a systematic review to categorically identify universal values of digital rights and promote policies to thwart perpetrators of them. We conclude with a recommendation that the UN host free, open-access, digital platforms that will promote transparency among organizations that collect users' data and assist everyone to safeguard their identities. We must recognize the violations of human rights that are taking place in digital environments and engage in pragmatic steps as an international community to ensure the right to privacy.

I. Violations of Privacy

a. Search and Seizure of Digital Property

Governments and militant organizations utilize internet censorship to shape the public's beliefs and curb dissent. From the most developed countries to the least, examples are prevalent of bloggers, activists, and political opponents being harassed and silenced [1]. In the name of internet security, users are analyzed for characteristics that predict problematic behaviors. Data is saved, which can be used to profile individuals or groups who appear rebellious. During major protest movements around the world, such as the Arab Spring, Occupy protests, and the Umbrella Movement, governments were able to extract data from mobile phone users. Social media and other online correspondence were routinely blocked or tracked to dissuade protesters. While laws exist in most nations to protect search and seizure of physical property, such laws often do not abide for digital property. As a result, without a search warrant, it becomes permissible to insist that individuals forfeit access to social media accounts to gain services such as a visa to visit another country. Repressive regimes scrutinize specific individuals as a method of discrimination.

b. Profiling of Marginalized Groups

Police in the modern age can target specific ethnic, gender, and age groups. The Chicago police department implemented a "Strategic Subject List", which predicts potential perpetrators and victims of gun violence [2]. Individuals can be intimidated or arrested based on characteristics about them or those they associate with. There is a dangerous potential for big data mining to be used to repress minorities. Online profiling enables police to invade the digital property of strategic subjects [3]. These policing practices broaden disproportionate incarceration of marginalized groups. China has started a "Police Cloud", which appears capable of tracking social and ethnic groups [4]. Not only the police profile marginalized groups, legal and illegal organizations do so as well. Some of them aim to exploit, such as by luring women into prostitution rings or refugees into forced labor. Disadvantaged groups are easy targets of financial scams and more easily taken advantage of.

c. Biometric Dangers

We have an overarching concern for the fate of the free world in a computer, cloud-driven society that preserves biometric data. Such data will develop the capability to penalize vast amounts of the population for minor infractions, especially those that lack the technological and financial means to protect their privacy. The discrimination of Nazi Germany reminds us how dangerous it can be for countries to collect registries that track minorities. Biometric data is a centralized command that pretends to have complete control, but in reality unlocks a door for data to be hacked and abused. In Brazil it is now obligatory to be included in the biometrical database, which also enables voting in elections [5]. In an example of how biometric data is abused, the Brazilian Federal Police in 2017 made a deal with the Electoral Court for sharing this database without announcing the practice previously [6].

d. Censorship

It was more difficult for autocracies to track down and burn books than it is for modern governments to remove content from the internet. In Turkey, China, and many other countries the internet is censored to such a point that self-censorship takes place. Individuals willing to express themselves online are exposed to reciprocity. In most countries, some level of censorship exists. In Israel a bill was introduced recently that would provide the court with automatic access to remove content from online platforms [7]. Such actions are justified as a defense against conflicts with organizations such as Hezbollah in Lebanon that use internet platforms to initiate violent actions and recruit agents among Arabs who hold Israeli citizenship [8]. However, the Israel Democracy Institute (IDI) argued against the law, as it is liable to create disproportionate censorship in an improper legal process that has no precedent in other countries [9]. Governments attempt to restrict social media, but companies themselves also censor content. The internal rules of such censoring also deserve oversight [10].

e. Business Surveillance

Facebook today has over two billion users. It enables people to share private data about themselves with others they know and trust. The company protects a large amount of user data. However, owing to unclear consent and sharing of data with third-party applications, many have discovered that detailed information about them, such as contacts, phone numbers, and likes, was being collected and shared without their consent or awareness [11]. Furthermore, Facebook provided administrative staff controls to erase messages, while users do not have the same controls over their own information [12]. Facebook is not alone in being accused of violating users' privacy. Agencies such as Equifax, which collected credit ratings for millions of people allowed its systems to be breached. Health insurance companies purchase big data from health care facilities to create predictive formulas for identifying risk pools and determining rates [13]. More and more businesses are utilizing big data for customer analytics. The USA, once a leader of restricting invasions of privacy, adopted regulations in 2017 that will remove the tradition of net neutrality. The ramifications of this decision will reduce freedom of expression [14] and increase the power of big data businesses to conduct mass surveillance and sell information about users' viewing content, purchases, and other personal information. Google and other large internet search sites already engage in such practices. They sell our information to advertisers, insurers, and lobbying groups, crafting the world that we are exposed to with almost no external ethical oversight.

II. Efforts to Protect Privacy

a. Multinational Efforts to Protect Privacy

Despite negative trends in the digital age, the right to privacy is still championed as an ideal by most of us. Multinational collaboration to protect digital rights is on the rise. Nations are bonding together to establish privacy-by-design controls that will protect data according to commonly agreed fundamentals. Governments, businesses, and criminal organizations have profited by invading our privacy, and supranational bodies are a potential buffer- a last line of resistance. The European Union recently adopted the General Data Protection Regulation (GDPR), which will go into effect in 2018. The regulation demands that individuals retain control of their data, that they can see the information about them that is being collected and ask to remove this information from internet platforms [15]. Organizations that collect data must employ a data protection officer, who will oversee that privacy standards are upheld and personal data of those who request to be forgotten are removed. A variety of multinational organizations aim to protect our digital rights, including the organization that we represent, Pirate Parties International [16]. Multinational initiatives are made possible by member states who participate. The International Conference for Data Protection and Privacy Commissioners (CDPPC), for example, has been bringing together government stakeholders since 1979 to assist them fulfill their mandates [17]. Each member state sends data protection officers to collaborate, which furthers our goal of harmonizing data protection. The present UN Resolution on the Right to Privacy in The Digital Age also exemplifies a positive multinational effort to protect privacy.

b. Government Efforts to Protect Privacy

While governments are demonized as infiltrators of our privacy, they are also guarantors of our digital rights and can reprimand those who violate them. Legislation that safeguards sensitive data is important, and many countries are struggling to keep pace with innovations in information technology that have expanded the realm of digital rights. Governments must both protect privacy and promote transparency, tasks that may seem at odds with one another but often function in tandem [18]. Governments can ensure that citizens are made aware of private information that is collected about them, as well as displaying information about what it does with that data and its own work. Medical data, for example, is private data that governments often enact legislation to protect. Otherwise, individuals could be discriminated against for employment and insurance. An important question that has been posed on the right to privacy is whether to provide people with access to medical records that show genetic dispositions to disease, as this information may not provide positive assistance when preventative precautions do not exist [19]. Governments must debate the levels of privacy and transparency that are in the best interests of its citizens. Voter rights to privacy are also important in democratic nations, as they guarantee the free choice underlying the spirit of elections. Cybersecurity is also a national responsibility as international conflicts between nation-states often spill over into digital environments. Recent examples of government legislation to provide greater transparency of privacy practices, include the Canadian

Parliament's Privacy Commisioner's Guidlines for Online Consent [20] and Brazil's "Internet Bill of Rights" [21]. Such legislation often seeks to regulate user consent and establish oversight into the interactions of individuals with internet providers and platforms.

c. Business Efforts to Protect Privacy

Effective online businesses realize the importance of customer trust, and they often provide their users with data protection and transparency about how they collect and use data. Single-sign-on frameworks present a challenge and opportunity for protecting individuals' privacy. Users are accused of a "privacy paradox", whereby they are willing to give up their rights to privacy for the sake of convenience but are nonetheless outraged to learn their data was utilized [22]. By allowing users to opt-in, companies are mitigating some privacy invasion, but they must carefully weigh the advantages and disadvantages of trading customer data with external services [23]. Data-driven technology is an important phenomenon, which can assist us in our lives. Standardizing the privacy policies for single-sign-on frameworks helps to ensure that user data is not misused by secondary service providers [24]. Privacy enhancing technologies assist us to protect our data, and such services are often provided free of cost. Facebook, which has already been utilized as a negative example of violating privacy, has also made positive efforts to protect our privacy by allowing users to delete accounts [25] and promising to enable users to also be able to delete specific data in the future [12]. The development of encryption services has also expanded the right to be "out of the system", providing individuals with a digital platform to congregate without fear of government interference. Furthermore, blockchain technology is expanding the right of individuals to establish financial networks that are not government regulated. Efforts by businesses to protect digital privacy must provide mutual benefits for individuals and organizations.

Conclusion

We hope that the situation might improve for the right to privacy, but the future appears bleaker. Since the advent of a digital society with online accounts, organizations that harvest user data have amassed tremendous powers. While certain merits can be argued for collecting user data, an equivalent responsibility remains to regulate and secure any stored personal data. Our identities are the most valuable thing we own. They are a form of wealth: identity capital. We should expect our identities to be protected from embezzlement and exploitation.

Unfortunately, both staggering breaches of privacy take place and personal data is used for corrupt purposes. We would like to believe that infringements are rare and negligible, but we have all been victims of privacy invasion. Our identities are abused by companies who track customers to sell products, interest groups who manipulate social media to shape elections, and governments that seek omnipotent powers. Online businesses are often multinational and can hide between borders. Neither small organizations nor large governments can be trusted to restrict themselves. The right to privacy in the digital age demands a united, multinational alliance that will ensure all individuals in the world share an inalienable right to protect their identities.

We urge the United Nations High Commissioner for Human Rights and international community to enforce accountability measures that ensure privacy invasions are monitored according to universal regulations. We must admonish governments who conduct indiscriminate mass surveillance and curtail their abilities to collect and utilize private information about individuals. We must penalize companies and individuals who steal our information or use it for illegitimate gains. While there are valid utilitarian reasons to enable minimal surveillance to enforce protective and punitive laws against heinous criminal activity, we must not allow individuals to become slaves of an oppressive system akin to George Orwell's Big Brother [26].

The UN must be proactive and provide a forum for those whose privacy is threatened. It is the responsibility of the international community to foster privacy-enhancing technologies that will protect all individuals equally. Regulations must restrict online entities from accessing all of our personal information. Unwitting users should not be compelled into giving up their privacy or not having access to a technology. We must ensure that our data is not used without our knowledge or consent, nor for purposes that were not explicitly stated. Positive efforts are being made, but we are playing a game of catch-up.

References (all urls were accessible on the date of submission, April 9, 2018)

[1] Flock, Elizabeth. "What Internet censorship looks like around the world". Washington Post. April 5, 2012: https://www.washingtonpost.com/blogs/blogpost/post/internet-censorship-what-does-it-look-like-around-the-world/2012/01/18/gIQAdvMq8P_blog.html?utm_term=.d0ebce509827

[2] Asher, Jeff and Arthur, Rob. "Inside the Algorithm That Tries to Predict Gun Violence in Chicago". The New York Times. June 13, 2017: https://www.nytimes.com/2017/06/13/upshot/what-an-algorithm-reveals-about-life-on-chicagos-high-risk-list.html

[3] Patton, D. U., Brunton, D. W., Dixon, A., Miller, R. J., Leonard, P., and Hackman, R. (2017). Stop and Frisk Online: Theorizing Everyday Racism in Digital Policing in the Use of Social Media for Identification of Criminal Conduct and Associations. Social Media+ Society, 3(3), 2056305117733344: http://journals.sagepub.com/doi/full/10.1177/2056305117733344

[4] Human Rights Watch. "China: Police 'Big Data' Systems Violate Privacy, Target Dissent" November 19, 2017: https://www.hrw.org/news/2017/11/19/china-police-big-data-systems-violate-privacy-target-dissent

[5] Tribunal Superior Eleitoral. "Biometria". Setor de Administração Federal Sul (SAFS): http://www.tse.jus.br/eleitor-e-eleicoes/eleicoes/biometria

[6] Tribunal Superior Eleitoral. "Parceria entre TSE e PF visa maior eficiência da gestão pública". Setor de Administração Federal Sul (SAFS): http://www.tse.jus.br/imprensa/noticias-tse/2017/Novembro/parceria-entre-tse-e-pf-visa-maior-eficiencia-da-gestao-publica

[7] The Israeli Knesset. “הצעת חוק להסרת תוכן שפרסומו מהווה עבירה מרשת .מאגר החקיקה הלאומי האינטרנט, התשע"ז-2016” [A bill to remove content whose publication constitutes a crime on the internet, 2016]: http://main.knesset.gov.il/Activity/Legislation/Laws/Pages/LawBill.aspx?t=lawsuggestionssearch&lawitemid=2011567

[8] Schwartz Eltsholer, Tehila. “תזכיר חוק הסרת תוכן המהווה עבירה מרשת האינטרנט .חוק הפייסבוק התשע"ו-2016” [The Facebook Law. A memorandum on the law for the removal of content that constitutes a crime on the internet]: https://www.idi.org.il/knesset-commities/12069

[9] The Israeli Security Agency. “Kalkilya Resident Linked to Hezbollah Arrested and Charged”. March 9, 2017: https://www.shabak.gov.il/english/publications/Pages/296.aspx\

[10] Hopkins, Nick. “Revealed: Facebook's internal rulebook on sex, terrorism and violence”. The Guardian. May 21, 2017: https://www.theguardian.com/news/2017/may/21/revealed-facebook-internal-rulebook-sex-terrorism-violence?CMP=share_btn_tw

[11] Sydell, Laura. “FTC Confirms It's Investigating Facebook For Possible Privacy Violations” NPR. March 26, 2018: https://www.npr.org/sections/thetwo-way/2018/03/26/597135373/ftc-confirms-its-investigating-facebook-for-possible-privacy-violations

[12] Constine, Josh. “Facebook retracted Zuckerberg’s messages from recipients’ inboxes”. Tech Crunch. April 5, 2018: https://techcrunch.com/2018/04/05/zuckerberg-deleted-messages/

[13] Thielman, Sam. “Your private medical data is for sale – and it's driving a business worth billions”. The Guardian. January 10, 2017: https://www.theguardian.com/technology/2017/jan/10/medical-data-multibillion-dollar-business-report-warns

[14] Miles, Tom. “U.N. freedom of speech expert concerned about net neutrality”. Reuters. December 20, 2017: https://www.reuters.com/article/us-usa-internet-un/u-n-freedom-of-speech-expert-concerned-about-net-neutrality-idUSKBN1EE2DA

[15] The EU General Data Protection Regulation (GDPR) Portal: https://www.eugdpr.org/

[16] Jääsaari, J., & Hildén, J. (2015). Piracy & Social Change| From File Sharing to Free Culture: The Evolving Agenda of European Pirate Parties. *International Journal of Communication*, *9*, 20.

[17] The International Conference of Data Protection and Privacy Commissioners Website: https://icdppc.org/

[18] Gutwirth, S. and De Hert, P. (2008). Regulating profiling in a democratic constitutional state. In *Profiling the European citizen* (pp. 271-302). Springer, Dordrecht.

[19] Tavani, H.T. (2004). "Genomic research and data-mining technology: Implications for personal privacy and informed consent", *Ethics and information technology*, 6(1): 15–28

[20] Office of the Privacy Commissioner of Canada. "Privacy and Social Media in the Age of Big Data: A Report of the Standing Committee on Access to Information, Privacy and Ethics". April, 2013: https://www.priv.gc.ca/media/2105/gl_oc_201405_e.pdf

[21] Arnaudo, D. (2017). "Brazil , the Internet and the Digital Bill of Rights" Igarapé Institute. Strategic Paper 25. April 2017: https://igarape.org.br/marcocivil/assets/downloads/igarape_brazil-the-internet-and-the-digital-bill-of-rights.pdf.

[22] Bashir, M., Hayes, C., Lambert, A., and Kesan, J. (2015). "Online Privacy and Informed Consent: The Dilemma of Information Asymmetry." *Proceedings of the Association for Information Science and Technology*, *52*(1), 1-10.

[23] Davenport, Thomas H. and Harris, Jeanne G. (2007). "The Dark Side of Customer Analytics." Harvard Business Review 85(5): 37–48: https://hbr.org/2007/05/the-dark-side-of-customer-analytics

[24] Hoven, J., Blaauw, M., and Warnier, M. (2016). "Privacy and Information Technology." Stanford Encyclopedia of Philosophy: https://plato.stanford.edu/entries/lawphil-nature/

[25] Curtis, Sophie. "How to Permanently Delete Your Facebook Account." The Telegraph. March 21, 2018: https://www.telegraph.co.uk/technology/0/permanently-delete-facebook-account/

[26] Orwell, George (1949). Nineteen Eighty-Four. New York: Harcourt, Brace & Co.

About the authors

Keith Goldstein is the General Secretary of Pirate Parties International and International Coordinator of the Pirate Party of Israel, Ohad Shem Tov is the Chairperson of the Pirate Party of Israel, and Dan Prazeres is Alternative Board Member of Pirate Parties International and General Secretary of the Pirate Party of Brazil. Questions regarding this submission may be sent to the lead author: keith.goldstein@pp-international.net