Privacy in the Modern World: Challenges and Implications of Deploying Privacy-Preserving Technologies

Islam Faisal Abdelrasoul

900131607

Department of Computer Science and Engineering & Department of Mathematics and Actuarial Sciences

The American University in Cairo

Author Note

This paper was submitted for the graduating class of 2019's Ahmed Zewail Prize.

Abstract

Everyday, huge amounts of data are being generated and shared worldwide. With the recent advancements in computational sciences and with the rise of large-scale data analytics and artificial intelligence, the value of owning data has increased significantly. Privacy breaches on a large scale can even lead to influencing national decisions such as what the recent Facebook-Cambridge Analytica scandal did to politics in the US and the UK. Therefore, the privacy and digital immunity of data have been a hot topic of multidisciplinary research joining forces from researchers across the fields of computer science, social sciences, and law. Another dimension that is pertinent to that matter is national security and the future of secret messaging and secure communication. In this paper, we shed light on some of the main challenges pertaining to privacy, and its connections and effects on the modern world and how it resonates with the recent changes in the Middle East region.

Keywords: privacy, privacy law, multi-party computation, big data, digital rights, encrypted communication

Privacy in the Modern World: Challenges and Implications of Deploying Privacy-Preserving Technologies

Since the beginning of time, humans have realized the tremendous value of knowledge. Recently, this has been more evident in the race to acquire, maintain, and make use of digital data. Digital data help researchers study different phenomena, solve problems, and cure diseases. In the world of business and politics, digital data help decision makers make informed decisions based on complex models and risk analyses. The study of data privacy is a multidisciplinary field where the implications and challenges of privacy appear in many contexts such as computational sciences, social sciences, privacy laws, and even national safety and security.

The inherent sensitivity and the globally growing scale of data introduce several challenges. For example, health records in many countries are protected by laws and regulations such the *Health Insurance Portability and Accountability Act (HIPAA)* in the United States. These data need to be handled with care to ensure the rights of patients, and at the same time provide utility for medical researchers to generate models out of them. The other major challenge is the challenge of privacy at scale. Privacy breaches in many situations can lead to national crises or global complications. A notable example of this danger was the recent privacy breach known in the media as the “Facebook-Cambridge Analytica data scandal” where private data of Facebook users were used unwillingly to affect the public stance in historical political events such as the campaigns of the US politicians Ted Cruz and Donald Trump (Davies, 2015) as well as the 2016 Brexit referendum (Cadwalladr, 2017). This scandal raised the public awareness on the importance of privacy and made it a priority for lawmakers to secure the cyberspace in developed and developing countries alike.

The Middle East is no special to that arms race for digital knowledge. The region’s rapidly changing political climate, rising freedom of speech climate, and national security issues such as terrorism place privacy and digital democracy as two of the major challenges that have to be addressed. For example, should we allow secret messaging applications to ensure freedom of the press?, or should we ban them in favour of national security and fighting terrorism? Another question is: how can we make use of privacy-preserving technologies to provide help and immunity to people or humanitarian organizations (Le Blond et al., 2018) in distress or armed conflict? In fact, due to the topic's great influence and relevance to the region, The American University in Cairo have chosen the theme for the 2016-2017 common reading program to be "Big Data, Big Questions: From Data to Knowledge in the MENA Region". In this paper, some of these open questions and challenges are exposed and explained specially those pertaining to the Middle East region such as: terrorism, freedom of speech, and digital democracy.

Encrypted Communications, Terrorism, and Freedom of the Press

Cryptology, the science and craft of code making and code breaking, has been known to mankind ever since the ancient Egyptians invented the hieroglyphics (Whitman & Mattord, 2011). Later, the Greek used it to secure their communications in war (Damico, 2009). In today's world, we use it everyday to secure our internet browsing, credit card transactions, and even our chatting applications. In the early designs of encrypted communication systems, servers were trusted with the plaintext data. Therefore, when ordered by the authorities, messaging service providers such as WhatsApp or Messenger could hand in the original text of the messages. However, cryptology can offer beyond this model of trust. With the recent advancements of end-to-end encrypted communications applications such as Signal and Telegram, even when compelled by the authorities, these service providers cannot hand in the plaintext messages of the conversation because the way the system is designed makes this mathematically and computationally infeasible.

This notion of security is a double-edged weapon that can be used for both good or evil intentions. One evil use case is that it can serve as a communication channel for terrorists. In fact, in a recent report published by *The Middle East Media Research Institute (MEMRI)* (Stalinsky & Sosnow, 2015), it was shown that these encrypted communication technologies were heavily used by different terrorist organizations such as ISIS and Al-Qaeda. It is an established fact that eliminating terrorism is a common goal the world is striving to reach, and specially the Middle East to achieve stability. This may lead us to jump to the conclusion that securing our everyday communications should not come at the expense of risking people's lives by exposing them to terrorist attacks. However, encrypted communications could also save lives on the other hand. As much as this technology is desired by terrorists, it is also desired by journalists and reporters (Laskow, 2014) who may be working in conflict zones or working to expose corruption in governments and would like to avoid prosecution. Moreover, it could be used by whistleblowers to disclose important information to the public, while avoiding prosecution. One prominent example was the 2013 Snowden disclosures on global surveillance. Edward Snowden was working for the *National Security Agency (NSA)*, and he was able through encrypted communications to communicate with the journalists (Maass, 2013) Glenn Greenwald, Laura Poitras, and Ewen MacAskill to arrange for this disclosure.

Another problem facing the Middle East nowadays is the problem of refugees and victims in areas of armed conflict. They represent another category of those who can make use of such apps when in distress or requesting help (International Committee of the Red Cross, 2017). Humanitarian organizations such as the Red Cross need to have technological foundations so that they can operate in regions of armed conflict. Encrypted communications along with other technologies help provide these organization with the digital immunity they require (Le Blond et al., 2018).

Having seen both sides, it has become apparent how this dilemma is indeed challenging. It is hard to decide on the threshold between freedom and security. Should we sacrifice some freedom to ensure our security? or should we make the authorities' task harder so that we could gain more freedom? Finding the right balance is indeed a hard task that requires the collaboration of researchers, technology developers, legislators, and policymakers to research the future of secure communications in the new era.

Towards achieving Digital Democracy

The internet and social media had a great influence on the rise of the Egyptian Revolution in 2011 and the wave of the Arab Spring in the region. This has marked the start of a new era in the region where freedom and coping up with the world were two of its pillars. One aspiration of the revolution was to achieve true democracy, and in this article, we expose a certain aspect of democracy, *digital democracy.*

E-voting

One topic that arises whenever digital democracy is mentioned is *e-voting.* Although some countries are adapting e-voting at scale such as Estonia (Maaten, 2004), building secure verifiable e-voting systems is still an open topic of research. The complexity of such systems doesn't rely on just the sophistication of the technologies used, but rather the complexity of the sophistication of these systems, the unpredictable user behavior, and the legal and technical concerns of deploying such systems at scale. E-voting is not restricted to public polls, but it can be also used to manage polls in decision making institutions such as the Parliament. One misconception about e-voting is that it is merely a tool to "make voting easier". While this is indeed a desired functionality, it is not the only reason why e-voting is desirable. E-voting can enable us to *mathematically verify* the integrity of the election process and generate verifiable proofs that a certain election process was not forged that can be checked by the public in a process called *end-to-end verifiability* (Benaloh et al., 2015). In addition to developing the maths behind these systems, it is essential to pass clear regulations that would make such systems usable in critical elections.

Multi-Party Computation (MPC): Achieving more by knowing less

The sensitivity and importance of certain categories of data introduce a challenge and a compromise that needs to be addressed between privacy and functionality. One example mentioned in this article's introduction is the category of medical data. In this example, there is a desire by users and an obligation by law to keep the data private.

On the other hand, there is a desire by medical researchers to collect as much data as they can to support their research and investigate their hypotheses so that they are able to find new cures, or help eliminate diseases. A typical question that arises is how can we enable a certain medical researcher in hospital X to access the *aggregate* medical records of patients in 10 hospitals including hospital X? The word "aggregate" here is key, because the interest is in the aggregate of the records (average or other statistics) not in the individual records. Cryptology enables us to achieve this task through what is called *multi-party computation (MPC)* where multiple parties, in our case the 10 hospitals, own private data, and they are interested in computing a shared functionality while maintaining the privacy of each individual record and only exposing the final results. As it is clear from the examples, this will have tremendous effects on the healthcare system when used properly. MPC can also be used in research in the social sciences such as assessing and addressing economic inequalities (Lapets et al., 2018). In their research, Lapets et al. created a system for multi-party computation where data pertaining to work conditions and salaries are collected to identify from the aggregates (without looking at individual salaries) disparities in pay based on gender or other possible sources of economic inequalities. This kind of research will have a huge impact on a multitude of fields such as economics, gender studies, and social sciences in general.

This powerful model of computation enables us to perform more computations by caring less about the small dots that create the bigger picture. While the maths and science that drives the technologies for enabling this powerful tool is already available, the privacy laws, and legislation is still lagging behind. There is much to be done in regards to passing legislation that would make the rights and expectations of such systems clear. From the user end also, it is essential to make users aware of how these technologies operate, and what assumptions they operate under. For example, the properties of the system in the 10 hospitals network rely on the assumption that a certain number of the hospitals are not compromised, and once this threshold is exceeded, the system properties fall apart.

Public Awareness of Privacy Issues

Preserving an ecosystem of modern communications capabilities backed with proper privacy laws and guarantees would never be enough unless users were well-educated about the aspects, issues, and limitations of the services they use everyday online. Raising the public awareness on issues such as privacy and the digital footprint of the users online is essential so that all of these technologies and laws come into real effect and touch the lives of users. One approach for this is through intelligent and user-friendly human-centeric approach of developing applications. For example, all of us see that small “green lock” when surfing the secure internet in modern web browsers. However, how many of us really understand the dimensions and guarantees that this “security promise” offers? While simplifying the design may seem the ultimate goal at a first glance, it is not really the case. In a recent study (Darwish & Bataineh, 2012), it was shown that the oversimplified designs may lead to undesired results by leading users to undermine the importance of certain features. To achieve the task of finding the right balance between simplicity and utility is a hard task that requires the coalition of psychology, human-computer interaction (HCI), and computer science researchers.

Besides intelligent design, there should be a media interest in promoting the appropriate practices, digital rights and laws, as well as the limitations of the services offered online. This is an inherently hard challenge because of the wide spectrum of audience that need to be addressed and the different levels of education, technological literacy, and interest in these topics. Different organizations have been trying to conquer this challenge, such as the *Electronic Frontier Foundation* whose slogan is “defending your rights in the digital world”. The goal is to have more of these institutions globally and on a national level for each country.

Conclusion

Cryptology and modern computation advances have enabled us to do a lot of tasks that can provide us with different levels of privacy and digital immunity. The tuning of the level of privacy to be employed in a certain situation is a question of compromise between social, economic, safety, and data sensitivity factors. To be able to maintain a healthy ecosystem of privacy-preserving technologies, it is essential that researchers from different fields including computer science, social sciences, and law participate together to research all the factors before legalizing and deploying such technologies.

References

Benaloh, J., Rivest, R., Ryan, P. Y., Stark, P., Teague, V. & Vora, P. (2015). End-to-end verifiability. *arXiv preprint arXiv:1504.03778.*

Cadwalladr, C. (2017). The great British Brexit robbery: how our democracy was hijacked. Guardian News and Media. Retrieved May 23, 2019, from https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy

Damico, T. M. (2009). A brief history of cryptography. *Inquiries Journal*, *1*(11).

Darwish, A. & Bataineh, E. (2012). Eye tracking analysis of browser security indicators. In *2012 International Conference on Computer Systems and Industrial Informatics* (pp. 1–6). IEEE.

Davies, H. (2015). Ted Cruz campaign using firm that harvested data on millions of unwitting Facebook users. Guardian News and Media. Retrieved May 23, 2019, from https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data

International Committee of the Red Cross. (2017). Humanitarian Futures for Messaging Apps: Understanding the opportunities and risks for humanitarian action.

Lapets, A., Jansen, F., Albab, K. D., Issa, R., Qin, L., Varia, M. & Bestavros, A. (2018). Accessible Privacy-Preserving Web-Based Data Analysis for Assessing and Addressing Economic Inequalities. In *Proceedings of the 1st ACM SIGCAS Conference on Computing and Sustainable Societies* (48:1–48:5). COMPASS ’18. Menlo Park and San Jose, CA, USA: ACM. doi:10.1145/3209811.3212701

Laskow, S. (2014). Is communications security for reporters improving? Columbia Journalism Review. Retrieved May 23, 2019, from https://archives.cjr.org/behind_the_news/is_communications_security_for.php

Le Blond, S., Cuevas, A., Troncoso-Pastoriza, J. R., Jovanovic, P., Ford, B. & Hubaux, J.-P. (2018). On enforcing the digital immunity of a large humanitarian organization. In *2018 IEEE Symposium on Security and Privacy (S&P)* (pp. 424–440). IEEE.

Maass, P. (2013). How Laura Poitras Helped Snowden Spill His Secrets. The New York Times. Retrieved May 23, 2019, from https://www.nytimes.com/2013/08/18/magazine/laura-poitras-snowden.html

Maaten, E. (2004). Towards remote e-voting: Estonian case. *Electronic Voting in Europe-Technology, Law, Politics and Society*, *47*, 83–100.

Stalinsky, S. & Sosnow, R. (2015). Encryption Technology Embraced By ISIS, Al-Qaeda, Other Jihadis Reaches New Level With Increased Dependence On Apps, Software–Kik, Surespot, Telegram, Wickr, Detekt, TOR: Part IV–February-June 2015. *Inquiry & Analysis Series*, (1168).

Whitman, M. E. & Mattord, H. J. (2011). *Principles of information security*. Cengage Learning.