



Committee: GA2: Human Rights Committee
Issue: Ensuring the protection of data privacy
Student Officer: Irmak Keleş (Deputy Chair)

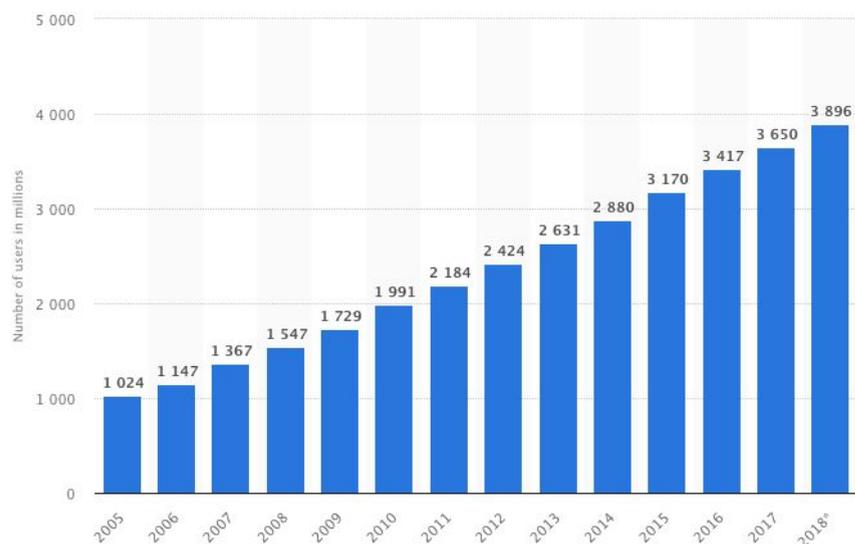
Introduction to the Issue

Protection of data privacy affects millions of people all around the world. In such a virtual oriented world, digital data is a mutual point for everyone. More than 50% of the world’s population has a digital fingerprint in the virtual world. The fact that there are approximately 4 billion users online as of 2018 elucidates the importance ¹

of data protection. Not to mention, every time a person creates an account, their information is collected and saved. Whenever you press the “I agree” button you trust the organization etc. on keeping your information protected and not misuse it. Data protection and privacy are two distinct topics. Data protection focuses on the security of the data from

unauthorized intervention. Data privacy is closely related to the technical part whereas data protection is concerned about the legal side. Simply put, we can say that data privacy is about authorized access to data. Even though the two concepts are not the same, having data protection ensures data privacy. Data protection is critical in the 21st century where identity theft remains to be one of the latest and pressing

Number of internet users worldwide from 2005 to 2018



¹ Image source: “Number of Internet Users Worldwide 2005-2017.” *Statista*, Statista, Dec. 2018, www.statista.com/statistics/273018/number-of-internet-users-worldwide/.

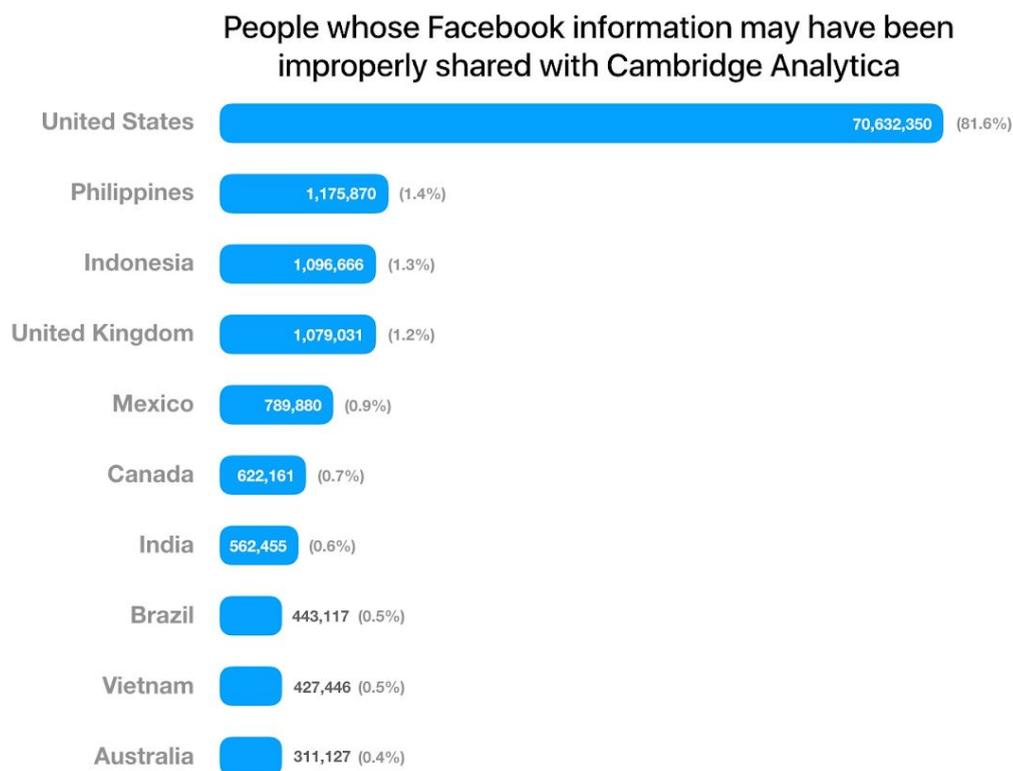


problems. So, the technology alone is vulnerable and inadequate since it can be accessed by authorized individuals. Therefore, it comes down to legislation regarding data protection and less about data privacy.

Involved Countries & Organizations

The United States Of America²

Being one of the leading powers of technology, the US has had many publicly popularised lawsuits regarding protection of data privacy. For example, the trial in April 2018, Mark Zuckerberg confessed that they had been sharing personal information. Many US citizens' personal data privacy was shared illegally through Facebook. The USA has been working to better the current state of chaos.

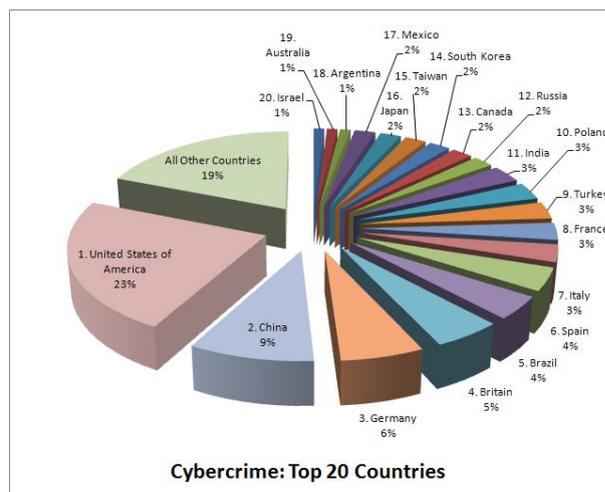


We do not know precisely what data the app shared with Cambridge Analytica or exactly how many people were impacted. Using as expansive a methodology as possible, this is our best estimate of the maximum number of unique accounts that directly installed the thisisyourdigitallife app as well as those whose data may have been shared with the app by their friends.

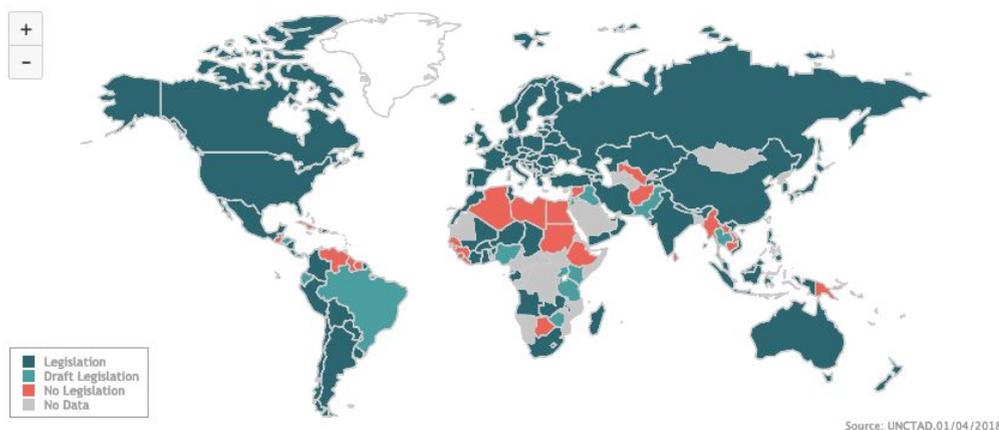
² Image: “The Power of Machine Learning – Lessons Learned from the Recent Facebook and Cambridge Analytica Scandal.” *ENTERPRISE TRADE VIEWS*, 10 Apr. 2018, www.google.com/url?sa=i&source=images&cd=&cad=rja&uact=8&ved=2ahUKEwja8dnr9M_gAhUM16QKHWxABUAQjhx6BAGBEAM&url=https://www.enterprisetv.com.my/the-power-of-machine-learning-lessons-learned-from-the-recent-facebook-scandal/&psig=AOvVaw3RuHbC3Sovouzh-nOAn7tZ&ust=1550944529563707.

China

China is one of the countries that has the highest rates of cyber-crime.³ Not to mention, the digital data flows are recorded to end in Chinese territories. China had inadequate attributes to data privacy in some parts of the laws. However, on 1 May 2018, China put the Personal Information Security Specification (the *PI Security Specification*) into force. the *PI Security Specification* is a set of complementary laws setting the new national standard to eradicate the issue.



Data Protection and Privacy Legislation Worldwide



Russia⁴

Russia has put great importance into the development of data protection and privacy laws since 2005. Taking into consideration the effect of General Data Protection Regulation

(GDPR) this is no surprise. “From 1 July 2017, the administrative sanctions for different privacy violations were increased substantially. For example, data processing, which is not in line with legal

³ Image: “Top 20 Countries Found to Have the Most Cybercrime.” *Remove Spyware & Malware with SpyHunter - Enigma Software Group USA LLC*, 21 Apr. 2017, www.enigmasoftware.com/top-20-countries-the-most-cybercrime/.

⁴ “Data Protection and Privacy Legislation Worldwide.” *UNCTAD | Investment Country Profiles*, unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx.



requirements for the volume of data provided in the written consent of the data subject, may result in a fine of RUR 75,000.”⁵

United Nations Development Group (UNDG)

The UNDG released a guidance note regarding data privacy, implementations and transparency. The report has been accepted and it appeals to to all UNDG entities which are: FAO, IFAD, ILO, IOM, ITU, OHCHR, UNAIDS, UNCTAD, UNDESA, UNDP, UNECA, UNECE, UNECLAC, UNEP, UNESCAP, UNESCO, UNESCWA, UNICEF, UNIDO, UNFPA, UNHABITAT, UNHCR, UNODC, UN OHRLLS, UNOPS, UN OSAA, SRSG/CAC, UN Women, UNWTO, WFP, WHO and WMO. The “GUIDANCE NOTE ON BIG DATA FOR ACHIEVEMENT OF THE 2030 AGENDA” explains the methods that can be undertaken to protect data privacy.

Detailed Analysis of the Issue

Citizen safety

Data privacy closely ties to citizen safety; therefore, is one of the most important topics in our age. Online data has become the perfect tool for hackers to gain information and later use it to attack. Critical national or personal information is stored in our virtual fingerprints on the internet. Protection of such information is the priority of the countries. The attacks show a drastic risk to public safety if, for example, the data concerning nuclear power station plants being stolen. The leading security present is called end-to-end encryption where only the authorized parties with recorded IP addresses uncover the privacy shield and access the data. We have to realize that from the legal view much more could be added to the current state. The standard usage of online bases to store information has become a playing-field for cyber-criminals. Big companies, governments, and media platforms should prioritize the security of current business on advanced security solutions. These solutions give the consumer’s data safety guarantee and help businesses gain adequate control. Data privacy is especially important when it comes

⁵ From the interview of Sergey V. Medvedev. “Russian Federation: Data Protection & Privacy Laws 2018 / Russian Federation.” *FDA Approves Pill With Sensor That Digitally Tracks If Patients Have Ingested Their Medication - Food, Drugs, Healthcare, Life Sciences - United States*, [www.mondaq.com/russianfederation/x/759522/Data Protection Privacy/Data Protection Privacy Laws 2018 Russian Federation](http://www.mondaq.com/russianfederation/x/759522/Data+Protection+Privacy/Data+Protection+Privacy+Laws+2018+Russian+Federation).



to retail. Customers expect to get recommendations based on their previous purchases and great command of data is needed to do so. At the same time customer loyalty is linked to security.

UNDG and The General Data Protection Regulation

The UNDG released the “GUIDANCE NOTE ON BIG DATA FOR ACHIEVEMENT OF THE 2030 AGENDA” which shows examples for implementations of data privacy protection. In Europe, The General Data Protection Regulation came into force on the 25th of May, 2018. This new bill aims to

modernize laws concerning protect one’s right to protection of personal information. It is said to be the most substantial change in data protection in every area imaginable. With the new regulation, the penalties are more severe, the consent concept is defined more clearly, and right to access to knowledge about the use of personal information is revised.⁶

Right to protection of personal data

The European Union has been developing the GDPR for the past three years. In Australia and the US, similar laws are being developed. An average citizen is, now, more knowledgeable about the invasion of privacy. The scandalous news -concerning social network platforms, governments, and major companies invading privacy- appearing on the cover pages of the news and magazines have raised awareness about the issue. However, citizens are still vulnerable to attacks since an activity online has the chance of their personal information being stolen. Later, this information may be sold to social media platforms, tech companies or governments. It is known that about 20% of the data flow ends in China,

EU GENERAL DATA PROTECTION REGULATION
Enforcement starts on May 25th, 2018
Concerns organizations processing personal data of EU citizens

- **Increased Territorial Scope** (extra-territorial applicability)
- **Penalties:** fines of up to 4% of annual global turnover or €20 Million (highest of both)
- **Consent:** clear consent to process data (and ability to withdraw)
- **Breach notification duty:** within 72 hours of having become aware of it (if risk)
- **Right to access:** controller must answer whether personal data are processed; why + where; copy
- **The right to be forgotten:** Data Erasure (conditions)
- **Data portability:** right to transmit personal data to another controller
- **Privacy by design:** from concept to legal requirement
- **Data Protection Officers:** staff member or external service provider

<http://www.eugdpr.org/the-regulation.html>

Summary of some key changes with GDPR

⁶ Image: “General Data Protection Regulation: the Online Guide to the EU GDPR.” *i-SCOOP*, www.i-scoop.eu/gdpr/.



Russia and Ukraine (based on data collected by BlackFog). This information flow is undoubtedly the biggest problem we are facing today. This violation of the right to protection of personal data is one thing the UN has been struggling to get hold of for many years.

List of Important Events

Date (Day/Month/Year)	Event
10 December 1948	The Universal Declaration of Human Rights was adopted
4 November 1952	National Security Agency (NSA) was formed
25 January 2012	Reform of the EU's data protection rules to strengthen online privacy rights and boost Europe's digital economy was released
July 2014	Russian President Vladimir Putin signed the new bill regarding personal-data measures
30 June 2014	The right to privacy in the digital age resolution presented by Report of the Office of the United Nations High Commissioner for Human Rights
25 May 2018	The General Data Protection Regulation comes into force for the European Union
23 October 2018	European External Action Service (EEAS) presents a new set of regulations concerning the handling of personal data: Regulation (EU) 2018/1725
10 October 2018	"The European Union Delegation to the UN in Geneva, the Permanent Mission of Austria in Geneva and the Geneva Internet



	Platform organize a conference to discuss personal data protection and data flows.” ⁷
--	--

Past Resolutions and Important Documents

- “GDPR Key Changes.” *Key Changes with the General Data Protection Regulation – EUGDPR*, eugdpr.org/the-regulation/.
- The Right to Privacy in the digital age, 30 June 2014, (resolution 68/167) <https://icdppc.org/wp-content/uploads/2015/03/Letter-to-the-UN-High-Commissioner-for-Human-Rights-Right-to-Privacy-in-a-Digital-Age.pdf>.
- General Assembly resolution 71/199 and Human Rights Council resolution 34/7
- Rither, Andreja. “Protection of Privacy and Personal Data on the Internet and Online Media .” *Council of Europe*, Parliamentary Assembly, Report1 Committee on Culture, Science and Education , 12 May 2011, assembly.coe.int/CommitteeDocs/2011/RihterviepriveeE.pdf.
- *The State of Data Protection Rules around the World A Briefing FOR CONSUMER ORGANISATIONS*. Consumers International, www.consumersinternational.org/media/155133/gdpr-briefing.pdf.
- The Right to Privacy in the Digital Age (Panel), 15 April 2014 (A/HRC/DEC/25/117)
 - The Right to Privacy in the Digital Age, 18 December 2014 (A/RES/69/166)
- *Report of the Special Rapporteur on the Right to Privacy*. Human Rights Council Thirty-Seventh Session, 26AD. https://www.ohchr.org/en/hrbodies/hrc/regularsessions/session37/documents/a_hrc_37_62_en.docx
- “EUR-Lex Access to European Union Law.” *EUR-Lex - 52011DC0681 - EN - EUR-Lex*, OPOCE, eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2018.295.01.0039.01.ENG&toc=OJ:L:2018:295:TOC.

⁷ Intext citation: “EVENT: The EU General Data Protection Regulation and International Data Flows - EEAS - European External Action Service - European Commission.” *EEAS - European External Action Service*, 10 Oct. 2018, eeas.europa.eu/delegations/un-geneva/51004/event-eu-general-data-protection-regulation-and-international-data-flows_en.



- “The Right to Privacy in the Digital Age.” *OHCHR | Freedom of Religion: UN Expert Hails Albania, but Notes New Challenges and Unresolved Issues from the Past*, www.ohchr.org/en/issues/digitalage/pages/digitalageindex.aspx.
- “PRIVACY AND DATA PROTECTION PRINCIPLES.” *United Nations Global Pulse*, www.unglobalpulse.org/privacy-and-data-protection.
- Smith, John. “Data Protection.” *European Data Protection Supervisor*, 11 Nov. 2016, edps.europa.eu/data-protection/data-protection_en.

All the included links and pdf documents have been written with data protection being the focal point. The past attempts to solve the issue are explained in depth in the resolutions. The countries and their part/side on the topic is explained in the Consumers International article. Current information and overview of the topic are defined specifically in the first two links. The Human Rights Committee of UN has had multiple panels, letter, and resolutions on the topic included in the list.

Past Attempts to Solve the Issue

There has been a lack of protection of personal data privacy until late 2013. Starting with the resolution submitted in 2014 by the Human Rights Committee the acceleration of improvement stated upon data protection and privacy issue. The efforts on Right to Privacy in the digital age was inadequate; therefore, the Human Rights Committee created the UN Special Rapporteur mandate in March 2015 (and renewed it three years later). Next, there were many improvements made through legislation. With the help of the United Nations, access now formed Data Security Helpline. Numerous policy publications were made about guidance on government hacking and data protection. Data Privacy Day has been successful at raising awareness and bringing people together about the issue. Yet, there are not many effective laws which clearly state the limit of authorized access on personal data. Similarly, the formation of the General Data Protection Regulation (GDPR) was a big leap from the previous regulations; nevertheless, with such active development, the GDPR has been incompetent.



Possible Solutions

Keeping in mind the previous sections we see that some actions were taken to eradicate the stealth and misuse of personal data; however, none has been truly effective. Even though the General Data Protection Regulation is one of the most significant actions taken in this manner, it lost its effectiveness after some years. In this case formation of a comprehensive organization that will have a greater force worldwide is more sufficient. On the other hand, legislation passed by the governments plays a key role in making such an organisation more effective. Countries should make sure that the laws discussed regarding privacy of citizens are in line with the UN guidelines. Not to mention, a lot of responsibility is on the users itself. The government or a non-profit organization can utilise various methods to better the user education and awareness. Big companies which have wide access to personal information of individuals could be made to obey more rigorous standards (standards should be set clear on how to handle data). Recognition of the rule of law from institutions/governments is a big step and can be made possible through the UN. Before accessing personal information the transparency of contracts can be revised. This is an important step to meet the rights of individuals. All members should acknowledge the importance of protection of the right to privacy. Lastly, data privacy access easiness could be redirected, relating to rigorous standards. Access to surveillance tools like software and such equipment should have binding laws concerning usage which will truly level the playground and address the cruciality of the issue.

Key Words

- Personal data: In this document personal data refers to any specific, private individual data an individual has, from credit card numbers to personal photographs.
- Encryption: It is used as a way to prevent unauthorized access to personal data. It involves the process of turning data into code.
- Digital fingerprint: Digital fingerprint is any activity and individual has online. Social media accounts, addresses entered, search history are some examples.
- Digital literacy: Digital literacy represents the understanding of virtual concepts and therefore being knowledgeable about information technology.



Bibliography

- “DATA PRIVACY, ETHICS AND PROTECTION GUIDANCE NOTE ON BIG DATA FOR ACHIEVEMENT OF THE 2030 AGENDA.” *UNDG_BigData_final_web.Pdf*, United Nations Development Group , undg.org/wp-content/uploads/2017/11/UNDG_BigData_final_web.pdf.
- “Defending the Right to Privacy Globally: 8 Key Recommendations for the Digital Age.” *Access Now*, 25 Apr. 2018, www.accessnow.org/defending-the-right-to-privacy-globally-8-key-recommendations-for-the-digital-age/.
- Edwards, John. *Letter from Chair of the Executive Committee*. International Conference of Data Protection and Privacy Commissioners , icdppc.org/wp-content/uploads/2015/03/Letter-to-the-UN-High-Commissioner-for-Human-Rights-Right-to-Privacy-in-a-Digital-Age.pdf.
- Rither, Andreja. “Protection of Privacy and Personal Data on the Internet and Online Media .” *Council of Europe*, Parliamentary Assembly, Report1 Committee on Culture, Science and Education , 12 May 2011, assembly.coe.int/CommitteeDocs/2011/RihterviepriveeE.pdf.