Data Privacy: Current Events and Policies

Tenzing Rither
Computer Science
Portland State University
Portland, Oregon, USA
rither@pdx.edu

He Wang
Computer Science
Portland State University
Portland, Oregon, USA
hw6@pdx.edu

Jiacheng Zhao
Computer Science
Portland State University
Portland, Oregon, USA
jiacheng@pdx.edu

ABSTRACT

Nowadays, people are trying to get deeper into the virtual world. A large amount of data for users is being collected by more and more databases of companies. Automation tools and applications that updating people's life are created. Nevertheless, they also bring instability and insecurity to people initially. There has been growing public discussion about data privacy around issues such as data privacy police. This paper focuses on data protection, methods, and policy of data privacy. These items have made the most primitive guidance for the development of the digital age in the future. Plus, they are the foundation for the steady development of the digital age. Analysis of the policy of current data privacy not only reveal the current rule in the new virtual world, but also promote the improvement of legislation that could benefit in the future.

CCS Concepts

- **Data Privacy→Current Events in Data Privacy**
- **Data Privacy→5G network technologies and security**
- **Data Privacy→Proposed Legislation and Policies**

Keyword

Digital age, Data privacy, Collection of data, Policies of data privacy, Legislation, Mechanism, Security, Virtual, Edward Snowden, Facebook, Uber, Technology, Kenya, Human right, Internet Governance Forum, IGF, WhatsApp, Encryption, Adblock, Apple IOS13, 5G, 5G networks, SDN, NFV, Network Slicing, HetNet, General data Protection Rights(GDPR), Right To Be Forgotten, IEEE, California Consumer Privacy Act (CCPA).

1.INTRODUCTION

With the development of society, people have entered the information age. The process of information virtualization has become more widespread. Everyone not only has a sense of reality, but also feels the presence in the virtual world. People take the advantages of computers to collect, calculate and analyze data and committed to building a better society. However, due to the troubles of virtualization, people realize that they need to make rules and policies in the virtual world to constrain behavior, just like the legislation in reality. As the old saying goes - no rule, no standards. Thus, this paper will focus on current events and policies of data privacy.

Our discuss was pushed by a set of exploratory research: What makes data protection important? What are the major events related to data protection? What are the technologies for data privacy? What are the requirements for different technologies for information security? What are the existing legal regulations related to data privacy? What are the challenges for better management of data privacy and data protection for the US and the world?

We will cover materials from research and study. First parts related to events of collection of data, and the mechanism of protection of data. Then, second parts related to 5G technology, the device to device connection, virtualization of the network, network slice, heterogeneous network. Discussion of information security requirements of different technologies. Last main parts list a series of existing policies and laws on data privacy: Right to be forgotten, General Data Protection Regulation(GDPR), IEEE Core Principles, and some proposed legislation

We found that data privacy is now becoming more and more enforced or talked about as a popular topic in congress. We need policies and laws of data privacy to constrain people's behavior. Although a lot of these acts are vague and unclear, we think states or governments are trying to set up a foundation of guidelines in regards to data privacy and where it should go before they jump into the details. We conclude with the policy of data privacy. Because this is so important to the lives of many. We think the debate on privacy laws will go on for a long time before we have a strong set of guidelines.

2.1. Collection of Data

In the digital age, data plays a huge role in our everyday lives. It's present in lots of obvious ways. When we are shopping online for example and have to type in our name and address. Data collection can also be less visible. Take data brokers, for example. You've probably never heard of them, but these businesses specialize in creating in-depth profiles of individuals for advertisers. A single profile may draw on up to 1,500 data points. This can include a person's sexuality, browsing history, political affiliation, and even medical records. In 2013, Edward Snowden [1] uncovered a vast regime of mass government surveillance programmers, opening a global conversation which is still unfolding today.

CHI 2019, May 4–9, 2019, Glasgow, Scotland UK

ACM ISBN 978-1-4503-5970-2/19/05. . . $15.00
https://doi.org/10.1145/3290605.3300410

The digital age has created new ways to collect, access, analyze and use data, often across multiple borders and jurisdictions. Unsurprisingly, this poses challenges for human rights. One challenge relates to the way companies use our data. The internet's business model depends on people sharing their data in exchange for access to content, services, and social media platforms. While you might not pay anything upfront to go on Facebook, they still make money from you by selling your personal information to advertisers. It also creates an opportunity for misuse. For example, "Long Island man billed nearly $1,900 in fraudulent Uber charges" which reported by ABC11 [2] shows " a hacker had taken over Bill's account and changed the email associated with the account." Plus, not only the man is charged from Uber, but also many credit cards have been charged at different price.

Another challenge relates to the collection of personal data by governments. Technological developments now enable governments to monitor our conversations, transactions, and the locations we visit. In some countries - including Russia, Australia, and South Korea - companies are legally required to store this data locally for long periods, making it easier for governments to get information on their citizens. These measures are often introduced in the name of fighting cybercrime and terrorism. But without adequate protections, data can easily be abused to target dissidents and activists and other bad ways. Emerging technologies - like the Internet of Things, wearables, and artificial intelligence - are likely to pose new challenges to human rights.

2.2. Events

First, let's look at the Apple vs. FBI case [3]. After the 2016 terrorist attacks in the US city of San Bernardino, the FBI asked Apple for the information stored on the iPhone of one of the suspects. However, Apple's operating system is encrypted and only accessible through a pin code. The FBI asked Apple to modify the system to let them in. Apple refused - opening a lively debate on the right to privacy versus security needs. The case was almost taken to court - but in the end, the FBI found a vulnerability to crack the phone. In privacy terms, this was a legal setback. If the case had gone to court, it could have helped popularize the risks of weakening encryption for society, and establish what constitutes a legitimate limitation on privacy by the state.

In Kenya, a combination of invasive surveillance measures and a lack of adequate data protection facilitated a crackdown on civil society in 2013, which was documented by Peace Brigades International [4]. Many human rights defenders had their offices raided, computers hacked and phones tapped by the government. One of the ways human rights defenders have been fighting back is by pushing for the ratification of Kenya's first data protection law, long-stalled in Parliament. Kenya is by no means the only country to bring in surveillance legislation justified by security concerns. This event is a good demonstration of how seemingly abstract restrictions on online privacy can have physical consequences in the offline world.

2.3. Mechanisms

On the one hand, there are mechanisms at the international level. Following a UN resolution [5] on the right privacy in the digital age, the Human Rights Council has established a new Special Rapporteur for Privacy. And various internet policy forums, like the Internet Governance Forum (IGF), the Council of Europe, the Organization for Economic Cooperation and Development, and conferences, like CyFy [6], also contribute to shaping the scope of privacy in the digital age. On the other hand, we have company. The decisions of companies can also have a huge impact on data protection and privacy rights. For example, by building end-to-end encryption into their software, as WhatsApp did in early 2016 [7]. They claimed that "the encryption and decryption of messages sent on WhatsApp occurs entirely on your device. Before a message ever leaves your device, it's secured with a cryptographic lock, and only the recipient has the keys."

An easy step is taking digital security measures yourself. This can be as simple as using encryption and anonymity tools. People can also advocate for alternative digital business models, which aren't based on the extraction and sale of data. To illustrate, over the last few years, the number of users using Adblock software [8] globally has exploded. There is evidence that this is already pushing companies to less invasive advertising practices. Engagement in debates at the national and regional level is, of course, crucial. We also need to make sure legislation is keeping up with new technological developments- like the Internet of Things. Ultimately, if we want things to change, we need to make these issues accessible and relatable by being more creative about the way we talk about them. When people see how data protection and privacy affects them on a day-to-day basis, they may be more inclined to engage with these concepts.

3.1. Facebook vs FTC

he Internet has been linked to everyone with the entire world. We can communicate with people who are hundreds of miles away, we also can shop without step out of your room. Communication and convenience are not the only things which the worldwide internet brings to us. The Internet also exposes our personal information and secrets in risky. An article written by Jon Swartz and published in Barron`s says Facebook exposed at least 50 million user`s account information, and the fine will reach $23 million or 4% global revenue from the previous year regarding Europe `s General Data Protection Regulation Law. And 4% of the revenue fine will make Facebook lost $1.63 billion[9]. Information leakage does not damage companies, but also citizens. Your personal identification may be stolen. A record by Kelli B Grant says identity thieves stole $16 billion in 2016[10].

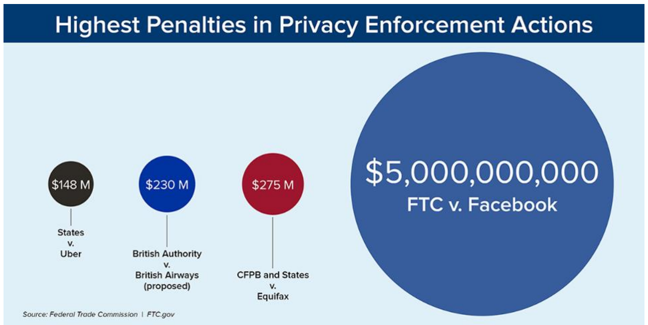

Figure: The Federal Trade Commission fined Facebook $5 billion for mishandling user's personal data.FEDERAL TRADE COMMISSION / FTC.GOV

This year 2019, Facebook was fined $5 billion for violating federal privacy, Figure 1 shows some companies` fines**.**

Internet is a part of our detail life. Without the internet, lives will run tough and barbarism. I do not even know how to finish this paper. We need Google to research, and we need Facebook to share or express our lives with friends. Information is not the binary digits you communicate will server ends. Information is the money that all companies are targeting. Companies such as Facebook or Google, they provide you free functional servers, and you will pay back by your personal information. We have these experiences while doing online shopping. You will keep receive advertisements after you purchase a headphone or a ticket of Portland Trail Blazers. Or you may just watch some videos on Youtube, then you will see the same product on your Instagram. The browser will continue post related products advertisements to you. Your information will be collected, organized and packaged. They will be traded as a product to other companies who will sell their service or merchandise. The information will be analyzed to help the decision-maker to set up targeting marketing strategy[11]. Companies share customers` information for the more targeted server, all companies announce to keep customers` information is protected.

3.2. Apple and IOS 13

Apple as one of the top multinational technology companies, provide various handy drives. iPhone, I suppose, is the greatest product in this century. It broke the 10-keyboard cellphone, and make smartphones smarter, and make all function possible on the device. Apple Worldwide Developers Conference(WWDC), brings new generations of devices every year, and also public new operating systems. In the Spring WWDC 2019, apple released IOS13 and macOS Catalina. In these IOS and macOS, the most significant optimization is data privacy. Apple makes Apple user stay in a more secure and private environment. Tim Cook introduced several new functions to make Apple safer.

I will summarize 3 functions most related to information privacy that we will have soon in September 2019. Firstly, the new feature is called Sign in with Apple. It is designed to against logging in websites or applications via your Facebook account or Google account. When you click log in with your Facebook or Google account, you are agreeing to share your information from your Facebook or Google account to the websites. These websites and applications will receive all your personal information. Under the protection of Sign in with Apple, you will log in a random pseudo-email. Your information will be hidden under the fake email. When you abort the service, pseudo-email will be abandoned with your traces as garbage. So those websites and applications can not track on you. Secondly, Find my is an optimized edition of Find iPhone. In the new edition, Find My, the lost Apple device will send a Bluetooth signal to all Apple devices, and the lost device location information will update to the Apple central server end. Those procedures will be processed without notification to both lost device and helper devices. The helpers will spend really tiny data to send the lost device location information. Also what is the most significant is the helpers' information will be kept in secure and private. Thirdly, HomeKit protection will collect and analyze house smart device data locally and sync to the cloud instead of sending all raw data to the cloud. This strategy can keep hackers away from raw data. We are entering a new stage of smart furniture. All furniture are getting more intelligent and fully-functional.

4. 5G network and key Technologies

Technology will secure us from information breaches, also new technology can bring problems. Apple implements new functions to guard us. Huawei is working on constructing the new generation of networks. 5G is coming soon. In a Chinese article 5G and communication engineering management, written by Junli Sun and his team mention that the transfer speed can reach to 10 gigabytes per second. 5G network is the next network generation. It not only provides enhanced transfer speed but also scalability, connectivity and energy efficiency[12]. In Mirtra`s article, the team predicts there will be 50 billion devices will be linked to the global IP network. Device-to-Device(D2D) as a significant feature of 5G network, contribute to form a smaller local network and allows a device to communicate to other devices with high-speed data transportation[13]. As a result of this, 5G D2D communication is facing the threats of jamming, data modification, free-riding, and privacy violation, says Zhang in his article[14]. D2D challenge to the authorization of data entity, availability of communication., and also in the privacy preservation. Meanwhile, 5G network has a feature of low latency. Under the coverage of 5G network information transfers fast, the data will be huge and devices will respond to those data simultaneously after we update our hardware system to fit the enormous size of data.

Xiaoyu Li and Hong Shen published an article talking about the 5G network security development trend. They say 5G has to achieve all security ability similar to 4G networks, and also has to secure small cells and femtocells.Ahmad lists out reasons of why different generations of networks can be risky. For example, he says, the communication was based on IP, and that type of communication will enable the migration of internet security vulnerability in 3G network. And in the 4G network, the system faced to the increment of smart devices and new servers. He also expounds the security threat vectors will be a big challenge to solve[15]. High speed and high capacity of 5G can carry more small networks which have more flexibility, but also those small cells are beyond the protection from previous network generation. 5G networks request NFV security, networks Slicing security and Hetnet security[16]. How the network builds and how the new technologies secure system, are good problem to study. There are few countries in the world have the ability to construct the 5G network. China is one of them. Unfortunately, the 5G is too new to have deep understanding. We are going to introduce the core technologies and the security requirements related in this section.

4.1.NFV/ SDN and security recruitment

NFV is the short form for Network Function Virtualization. It is a key technology for the 5G network architecture, which has the function of transforming the system from hardware to software.SDN, which is the short form for Software-defined Networking, is dynamical network management that will improve network performance[17]. SDN was designed by Stanford University. It is a new type of network architecture, also it achieves virtualize internet. It will get full access to network behaviors. SDN has three major functions, centralized control, OpenFlow protocol, and network virtualization. Centralized control helps to manage the source from the system. It will dynamically control the network source allocation and optimization. Openflow protocol allows exclusive companies to develop customized functions for WAN. Network virtualization blocks the otherness from low-level hardware[18]. NFV combined with SDN replace physical ICD （Industrial Communication Device） with visual supplies. SDN contributes to data flow control flexibility and NFV contribute to the function deployment flexibility. They are two isolated systems, but they supply each other[19].

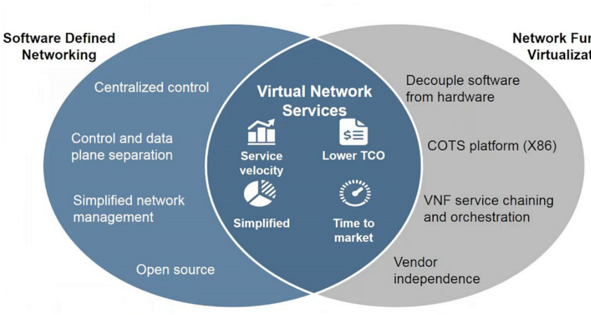

Figure 2: SDF functions and NFV functions.
They overlap at Virtual Network Services.

These technologies make 5G networks more efficient, more flexible and more adaptable[20]. In this article, the team analyze the requirements of NFV, SDN and network slicing which I am going to talk about later.

MANO(Management and Orchestration) is the new management system. The traditional networks will run on NFVI(Network Function Virtualization infrastructure) via VNF(Virtualized Network Function). NFVI is composed of a hardware device, Hypervisor, and virtualization source. MANO manages NFVI by assigning virtualization source to VNF, monitoring NFVI, updating virtualization source, hardware source and bugs. NFV security requests VNF management, data protection, VNF communication security, and bi-directional recognition. MANO requests device and software security optimization and reinforcing. SDN security requirements applied in four different layers. Firstly, in the application layer, the ID recognition between application and controller requests protection. Secondly, controller security requests the SDN controller has DDos/Dos attack defense mechanism and speed limit capability. Thirdly, the forwarding layer requests closing unnecessary services and ports. Forth, in South and North interface, bi-directional recognition and communication request powerful protection.

4.2.Network Slicing and security requirement

Network Slicing is another significant compose in 5G networks architecture. Slicing cuts a single network into multiple isolated small cells or networks, and small networks are verticals and they can achieve different functions to meet the requirement of various use cases. Network slicing a great technology with many different areas related. The following figure shows aspects with maturity levels of 5G network slicing[21]. Network slicing relies on the technologies of SDN and NFV. it can solve the problem of end-to-end(E2E) networks. Zhang rises up with a new type of network authorization protocol, PCHS(PKI-CLCHeterogeneous Signcryption) . This protocol satisfies bi-directional authorization, anonymity, non-repudiation, and fairness[22]. Yan mentions that function sharing and isolation between slices will cost security risks. The security requirements of network slicing apply on the protection of isolated small networks, the communication between slices, and slice security of the third party, and data management.

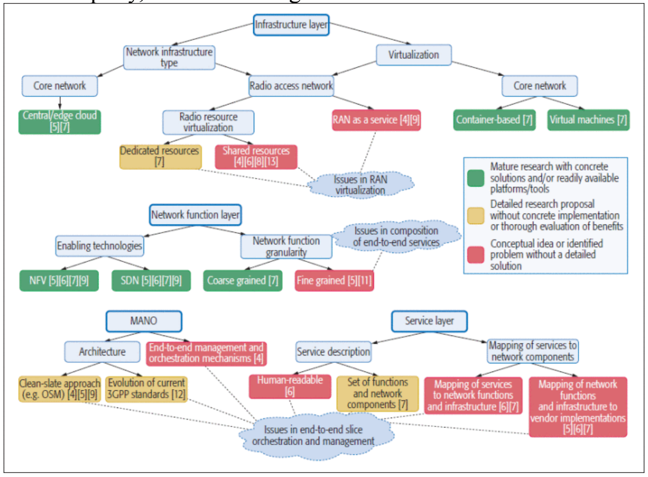
Infrastructure layer
Network infrastructure type
Virtualization
Core network
Radio access network
Core network
Central/edge cloud [5][7]
Radio resource virtualization
RAN as a service [4][9]
Container-based [7]
Virtual machines [7]
Dedicated resources [7]
Shared resources [4][6][8][13]
Issues in RAN virtualization
🟩 Mature research with concrete solutions and/or readily available platforms/tools
🟨 Detailed research proposal without concrete implementation or thorough evaluation of benefits
🟥 Conceptual idea or identified problem without a detailed solution
Network function layer
Enabling technologies
Network function granularity
Issues in composition of end-to-end services
NFV [5][6][7][9]
SDN [5][6][7][9]
Coarse grained [7]
Fine grained [5][11]
MANO
Service layer
Architecture
End-to-end management and orchestration mechanisms [4]
Service description
Mapping of services to network components
Clean-slate approach (e.g. OSM) [4][5][9]
Evolution of current 3GPP standards [12]
Human-readable [6]
Set of functions and network components [7]
Mapping of services to network functions and infrastructure [6][7]
Mapping of network functions and infrastructure to vendor implementations [5][6][7]
Issues in end-to-end slice orchestration and management

Figure 3: Network Slicing related area.

4.3.Heterogeneous Network security requirements

Hetnet(Heterogeneous Network) can be understood as multiple types of devices connection within a network, which is composed of different physical and link-layer technologies and topologies[23]. Hetnet supports all types of devices join in the networks, and communication among all other devices in the same networks via Bluetooth, Wifi, NFC, etc. All technologies talked about, SDN, NFV, slicing are all applied to create the Hetnet.

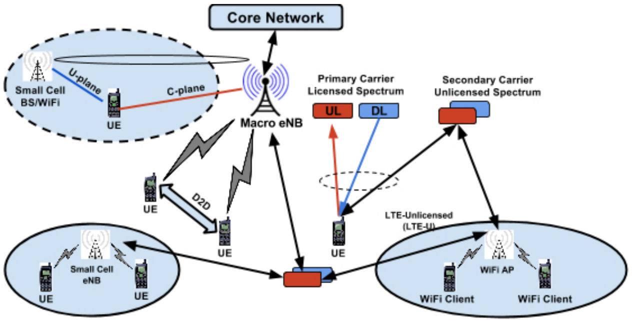

Figure 4: HetNet Structure, there are multiple small cells connecting to the core network, each of the small networks can have different connection mechanisms, or have different purposes.

Virtualization break the hardware barriers between devices[24]. The protection to each small cells, the communication security of between each small cells, and the connection security of small cells to the core networks are security of Hetnet. All security problems from SDF, NFV and slicing will be applied in the HetNet

5.1.Summary of Technologies and Security Requirements

Summarizing all technologies and the requirements of those technologies, 5G networks security focus on the protection of the macro network and the small networks, the communication between devices and the data management of separate devices and the central control, also focuses on the availability and the reliability of virtualization of the networks[25]. The author provides a more detailed analysis of the security requirements of the 5G network.

As 5G is running in the environment of VNF, the isolation technology should provide an efficient strategy. Hetnet is not only facing multiple devices but also the ways they connect to the system. The recognition and authorization, access technology are tough problems to deal with. Those technologies make 5G faster efficient, more creative, and more controllable. In this article, he mentions to hide users location information, users can non-periodically change user IP, to hide the mapping of location and user IP. To hide identity information, when user access to an untrustable internet, real location vectors can be generalized to as many as k indiscerptible positions, and the possibility of getting the real position is 1/k, then the ID will be secured k more times.

5.2. 5G Technology Summary

Data privacy is a serious problem. People more focus on keeping their location information, ID recognition, banking information, contextual information in private. IT companies are not only working on providing more functional service but also considering how to keep customers` information secure. There is a debate between targeting marketing and data privacy. 5G network brings high speed, high capacity, low latency, and D2D to us. The new generation network makes it happens that all data can be stored and processed in the cloud. There will be no need for a host computer. High speed will raise a similar experience or even faster than the process in your local device. 5G is making the smart city comes true. 5G will achieve smart furniture, and telesurgery will be reality. Of course, processing online, high-speed transfer speed and Device to Device communication will cause security problems, and data privacy challenges. Hardware updating and reinforcement, software optimization, and data encryptions are all efficient methods to protect our system and keep data secure.

6.1.Right To Be Forgotten

Due to the rapidly changing nature of how personal data is collected and used in an Internet-reliant world, digital privacy laws are disparate and largely untested. Currently, standards are very different around the world - a serious challenge when dealing with the Internet, where data flows freely across borders. The EU has probably the most advanced legal framework on this issue in the world, and its 28 member states cooperate together in a way that could provide a model for global standardization down the road. One issue on which the EU has led the way in terms of digital privacy laws is the so-called "right to be forgotten". In short, this is the right of an individual to have personal information about themselves removed from online data providers if that information is not of public interest. It requires a difficult balancing between the interests of companies that seek to profit off online data and the individuals about whom that data is collected.

In 2010, a Spanish man asked the courts to direct a local newspaper to delete articles about him from 12 years prior, which he argued were no longer relevant. He also asked for Google Spain to remove links to those articles from search results. The newspaper argued that the articles were newsworthy at the time and part of the historical record, so it was under no obligation to remove them - and the court agreed. It directed Google to comply with the request, however.

Google appealed to the Court of Justice of the European Union. Google Spain (the specific entity named in the complaint) argued that since it had no hand in processing data when users entered search requests, as its sole function was to manage infrastructure and sell advertising space, it could not be ordered to change how that data was represented. Such complaints, it said, would be relevant to its parent company, Alphabet Inc., which is located in the US (a non-EU state). Google Spain further argued that even if it were to be regarded as responsible for the data it provides as a service, it does not meaningfully process that data, and instead acts as a passive repository of information. This, it argued, meant that it was not the proper party to receive this kind of request.

The court disagreed with Google's arguments in two important ways: first, it decided that since Google Spain sells advertising space in the EU, it is responsible for the data it offers as a service, even though the processing of that data occurs in the US, which is not an EU member state. Second, the court found that since a search engine organizes and prioritizes search results, it counts as a data processor and can be ordered to change how its results are retrieved.

The EU court largely based its ruling on a directive proposed in 1990 and passed five years later. At that time, of course, the landscape of the Internet was extremely different from today. When the Directive was written, the first World Wide Web browser would not be released outside a research facility for another year. The court cited both this 22-year-old directive, and the present-day ubiquity of search engines in our lives, in its ruling. This highlights the complexity in applying laws developed decades earlier to cutting-edge services: the nature of these questions of law is very different from what it was when the laws were written.

The court established a "right to be forgotten" in the EU, stating that "the data subject's rights override, as a general rule, that interest of internet users" to have free access to information and the desire of companies to profit off of data-providing services. However, it went on to say, "this balance may depend, in specific cases, on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information." But it didn't provide much guidance on how to decide between those concerns.[28] [5]

The Harvard Law Review, in a follow-up editorial, cautioned both sides of the argument not to read too far into the ruling, largely because of this limitation on the judicial review process: the courts can only judge whether current laws are being followed, not decide whether they're adequate or sufficient for current concerns [28].

6.2. General Data Protection Regulation(GDPR)

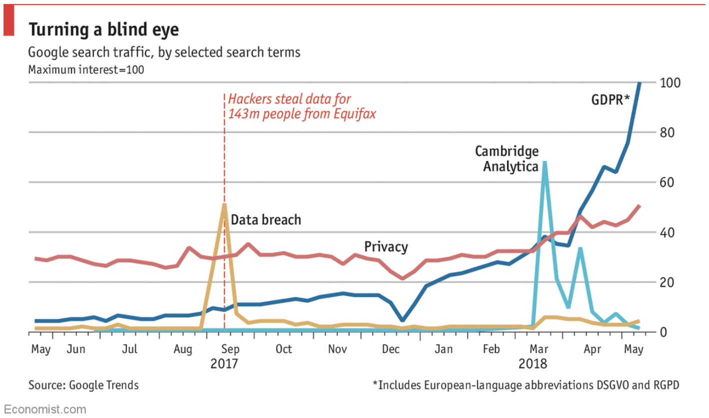

Figure 5: Google search trend graph showcasing popularity in keywords. GDPR significantly rises by 2018.

As you can see from the figure above GDPR was not quite popular in 2017. By 2018 GDPR became more widely searched and sought after. GDPR is becoming the forefront of data privacy and working its way towards setting a global standard.

The Google Spain case was a landmark ruling that brought the conversation on digital privacy to a head between corporations, governments, and privacy advocates. But other changes have been in the works as well. One of the most significant among these is the General Data Protection Regulation (GDPR), which was passed in 2016 and enacted in 2018, and is a binding regulation instead of a policy directive like that involved in the Google Spain case.

It requires online entities that collect identifying data about an EU citizen to get that user's explicit consent, and imposes fines if the consent agreements are long, complex, and difficult to understand. In January of this year, Google was fined €50 million for not fully complying with the GDPR in France. The law allows for even bigger fines though, up to 4% of the offending company's global revenue.[33]

Critics say it's too harsh, enacted too fast, and an undue burden on companies that are struggling to keep up with changing public priorities. Others reply that a 2-year delay in implementation is already slow given how fast the Internet changes, and smaller penalties will just be ignored by multi-billion dollar corporations.

Both sides are right in some ways. But the GDPR is exemplary in one way: it sought to update international law on an issue that has largely been left undirected, in a meaningful way and in a reasonable timeframe. Such laws can be updated; we don't have many examples yet of how such policies affect the websphere long-term. But starting points like this are necessary if any progress is ever to be made.

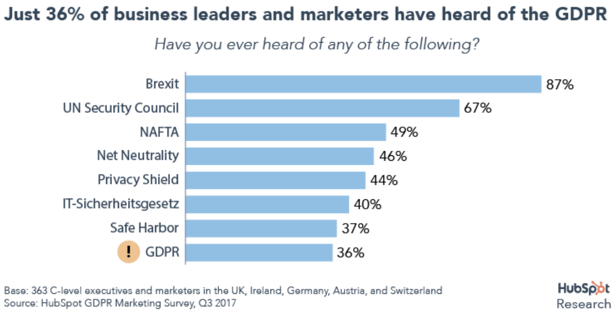

Figure 6: Here you can see how unknown GDPR is still today.

In Figure 6 you can see how widely unknown GDPR still is. You can see in the chart Brexit is more widely known. This graph showcases how leaders find GDPR insignificant. Data privacy is becoming more and more of a priority in politics, but it is still very much behind and will need a lot of time before any effective legislation gets addressed in regards to data privacy.

6.3. US and International Challenges

Cultural mores vary significantly across the world. This presents a challenge in setting standards for the Internet, where data flows freely across borders. Asia and Africa, with their rapidly expanding populations, will make up an increasingly significant portion of the online consumer base; with their voices largely absent from preceding conversations in the Western world about digital privacy, we need to be prepared for a wider set of perspectives as future solutions are sought.

In the US, where many tech companies are headquartered, freedom of speech is one of the highest-valued rights - much more so than in Europe; for example, hate speech laws are much more tolerant here. Further, states have their own regulatory agencies and legal initiative, complicating the equation when issues of digital rights are challenged in court. Corporate lobbying also tends to play a more influential role in the legislative process in the US than in Europe, meaning tech companies are likely to have more momentum behind protecting their interests here.

John W. Dowdell, writing in the Tulsa Law Review in 2017, took an expansive look at the history of privacy rights in America and abroad in order to comment on what an "American right to be forgotten" might look like. He advocates for a consolidation of America's fractured approach to privacy law - specifically, the creation of a fully empowered federal agency that is specially equipped to advise on new laws and enforce their implementation. Dowdell's thoroughness is beyond reproach, and the work he has put into compiling a legal background for this issue is impressive. However, his solution still largely assumes that Congress can self-organize to act with foresight and alacrity, in the best interest of all as opposed to that of their donors. [26]

In the aforementioned editorial in the Harvard Law Review, the editors offer insight into a key piece that will provide the cornerstone on which people like Dowdell can build a robust framework. They emphasize that putting out legal fires as they arise, the way most legal precedent on this matter has been bubbling up across the Western world, is a messy strategy that will lead to serious complications down the road: "the real debate is not on what has already been decided, but on what is yet to come," the editorial states; "if critics hope to change the substantive outcome, they must shift their focus from secondary legal and policy arguments to the fundamental values at stake" [28]. It is by having these conversations about fundamentals that a robust and enduring system can be established in our increasingly global society. So for digital privacy rights to have a consistent and robust future in America - and abroad - we will need to seek compromises between regulatory consistency, corporate interests, and privacy advocates.

6.4. Proposed Legislation

There are many legislations being proposed in Congress in regards to data privacy, here are just a few and their details. The first policy is the CONSENT Act (Customer Online Notification for Stopping Edge-Provider Network Transgressions). "The bill will require explicit opt-in consent from users of Facebook and other online platforms before these online platforms use, share, or sell any of their users' PII, as well as explicit notification any time data is gathered, shared, or sold to a third party, in addition to adding new reporting requirements in case of a data breach involving sensitive customer proprietary information." [30] This way, users know when data is being collected from companies and allows them to be more aware of activities regarding their personal information. The act would also give the FTC (Federal Trade Commission) jurisdiction to prosecute violators. Letting users be aware of data gathering is really significant in knowing what data is being used and providing users with the ability to decide what amount of info they would like to share. This act may be seen as more extreme to corporations, and more disadvantage to their business. The government would be given more power to manage what they believe is right or wrong. Perhaps if there was a compromise that could be met to benefit both sides of the market and government then more agreement could be met.

The second policy is the Social Media Privacy Protection and Consumer Rights Act of 2018. This act discloses privacy policies and obtains consent on privacy preferences for users. Examples of this act include: opting out of data gathering, notifications etc. This would give power to the consumers on controlling what data they would like to be shared publicly. Some people may be more comfortable with sharing personal information than others. Some people may want to keep most of their information as private as possible. The ability to customize privacy settings is a great way for corporations to ask users how much they are willing to share and get consent this way. Giving a certain amount of control to consumers would encourage them to educate themselves on privacy settings, and better inform themselves of the consequences and benefits of digital privacy.

The third policy is California's Privacy Bill. "The bill adds limits to selling data on users younger than 16 years of age and prevents businesses from denying service to users should they choose to exercise their rights under the bill." [30] This bill is aimed at protecting minors. Nowadays everyone is on social media. Teenagers are no exception. Be it Twitter, Instagram, Snapchat, or Facebook. Social media has such a massive impact on the daily lives of many that the state of California decided that something needed to be done to address the exponential growth in popularity of social media and the dangers it presents. This bill seems like a great way to inform young users on the dangers of sharing their information on the internet, and by informing them of their privacy rights, they can be more diligent about being aware.

6.5. California Consumer Privacy Act (CCPA)

From the legislation mentioned, none of them have actually passed in congress. There were over seven bills in 2019 that were introduced. Some of the bills introduced in 2019 were: The Information Transparency and Personal Data Control Act, The Commercial Facial Recognition Privacy Act, An update to the Children's Online Privacy Protection Act (COPPA) of 1998, The Digital Accountability and Transparency to Advance Privacy Act, and The American Data Dissemination Act. All of these bills touch on consent, transparency, making privacy easier to understand to consumers, being more aware of privacy, where the consumer's data is going, the purpose of using user's data, and more. Again none of the bills have passed. There is one state who was able to pass a state legislation on data privacy. California was the first state to pass a law on data privacy. California introduced the California Consumer Privacy Act (CCPA). It's a policy that at first glance seems similar to GDPR, but it is not. CCPA was signed into law on June 28, 2018. CCPA officially becomes effective on January 1, 2020. CCPA is an act that will allow Californian residents to know what data is being collected, where their data is going, who is receiving their data, will allows consumers to request corporations to delete their information, and more. The bill essentially aims to protect consumers, and their privacy. The downsides to this law is that it only affects California residents, the act does not officially protect users from data collection, corporations would not be required to ask permission from users to collect their data, and many more flaws and loopholes. Overall the act is a beginning step in data privacy and where it should go.

These were just a few policies concerning digital privacy, but there are lots more. Now more than ever, suggested policies discussing privacy is growing more and more with the ever growing concern, and politicians are realizing the importance of bringing up this topic to congress. Hopefully in the near future, there will be legislation that discusses the issues brought up in our paper today, and Congress and the market can work towards finding a balance to handle digital privacy.

7. Future Solutions in Data Privacy

Now we must look towards effective solutions to tackle digital privacy rights. One solution that could greatly help spread the importance of digital privacy to people would be for companies to educate consumers on privacy and what it really means. "The number of IoT devices grew from 500 million in 2003 to 8 billion in 2017 and is expected to grow to 50 billion in 2020, with that consumers should be informed about the products they are using."[30]. With the growth of popularity of these devices, it's crucial to let consumers know what they're buying and be upfront with the details and capabilities of the device they're buying. Someone's grandma or grandpa could go to Best Buy and purchase an Amazon Echo, but they may not be aware that their device is most likely listening to them even when not in use. Some people might find this offensive and an invasion of privacy, but they wouldn't know this was how they felt unless they had prior knowledge. So, it is the responsibility of corporations to take a step towards educating users and working towards providing better privacy for everyone.

A second solution to work towards fixing the issues regarding digital privacy would be to provide user control over data. Bret Swanson stated in an AEI article, "Sometimes the best solution for problems regarding technology is, well more technology." To address the issue of digital privacy, providing services that allow for the customization of one's privacy settings can allow for people to feel more comfortable and at ease with their products. These services should be user friendly, with an easy to use interface. Current services that exist include plugins like adblock, privacy badger etc. The creation of software to better protect users also supplies financial incentives for businesses, so there are benefits for everyone involved.

A third solution is to find a balance between legislation and the market on digital privacy. An example of problems arising without the help or interference of companies and government is the Cambridge Analytica scandal. "Facebook handed over personal information of more than 87 million users to Cambridge Analytica, so it is crucial that privacy policy laws be developed to prevent this from happening." [30] The lack of monitoring, and management on how data gets handled leaves room for critical mistakes to occur like Cambridge Analytica. This scandal caused a great outrage towards Facebook and a growing distrust to the companies policies and beliefs. Having privacy policy laws to prevent the exploitation of people's personal information is crucial, especially when it concerns controversial issues like politics. So having principles to guide the building of a system to protect and prevent these type of events from happening again is crucial . IEEE-USA has created core principles on data privacy and protection that includes: Public Transparency, Disclosure For Users, Control, and Notification. Public Transparency talks about the public being aware what data is being collected and what is being shared with third parties. This principle is mainly stating how companies should be as transparent as possible with the use of the data they're collecting. Disclosure For Users mainly talks about how users should be able to access information on what part of their personal information is being used. Control simply states how users should have the option not to be tracked, have personal info deleted if they wish to, and the ability to protect minors. Notification discusses letting users be informed about their privacy settings, being notified when their data is being misused or is lost, and having paid advertisers notify users that they are viewing paid content. [30] These principles are great rules to look at when discussing digital privacy laws. As you can see, the misuse of data is a fear expressed in the article about Cambridge Analytica, and one that should be at the forefront of confronting digital privacy rights.

These three solutions are just a few of the possible paths that digital privacy could take to reform privacy rights regarding technology. Now here are some current legislation that are taking the lead in digital privacy right now. These cases are being discussed presently in Congress, and are relevant to shaping the future of digital privacy. As Steve Jobs once said, *"Privacy means people know what they're signing up for, in plain language, and repeatedly. I believe people are smart. Some people want to share more than other people do. Ask them."*

8.Conclusion

In a consistent streak of the last 20 to 30 years, the internet, (previously designed to just be a research tool for universities), exploded in more ways that can be understood. In the last 10 years in particular, we've seen services such as banking, shopping, medical treatment and records, and a broad range of social media move onto the internet, making it a vital part of their respective services. What was once a simple and straightforward tool for public information and learning grew into a piece of technology heavily integral to life for those living in the first world. Brand new services would develop faster than fixes to issues regarding online property, data privacy, and/or general ethics for both users and companies. Particular questions such as "who owns the data I generate when I use a service?" come up and unfortunately, since businesses have already been utilizing the internet for decades to collect that data and provide whatever goods or services needed with it, the answer may not be straight forward. Many government attempts to fix issues have either been non-existent or too slow moving to be effective "protection" by any measures. Many third party companies have taken it upon themselves to set and follow their own rules and standards regarding what belongs to the user and what belongs to the company and the respective responsibilities that follow. Though once again, unfortunately, not all companies adhere to the same set of underlying moral principles which results in some companies fully neglecting their users for profit.

It would generally be ineffective and patently dangerous to start shutting down some or all of these services in order to restructure them because doing so could mean disruptions in the economy, banks, emergency services/hospitals all of which millions of people already depend on, as previously established. So the question then becomes: how do we begin integrating and balancing individual user rights and protections with a robust economic system in an interconnected age? To date, the solution has largely been piecemeal: as points of contention arise, existing law gets applied however seems best. This approach will not yield robust results long-term. In examining the fundamentals of privacy, existing protections under US law, international policies on digital privacy, the nature of potential future solutions, and proposed US legislation, it has become clear that legislatures, corporations, and private advocates must collaborate to establish a firm framework on which a solution can be found.

The authors of this paper want to stress, the solution does not necessarily lie on the side of more blanket regulation, blind and slow. Conversely, the solution also does not lie on the side of no regulation whatsoever, which becomes apparent when taking into context, for example, credit monitoring and bank keeping. Rest assured, a line must exist in the spectrum from no regulation to complete regulation. It will by no means be easy to implement and enforce but with time and thorough integration of tech-leaders and representatives, it could be achievable. Before we can suggest where a line may rest, we must first consider what can fundamentally constitute digital property and the implicit rights to privacy that follow. We can then further examine the laws that already exist based on the different interpretations of digital privacy and why. Finally, once we have examined the legislation that exists, we will be ready to propose a few solutions to active legislation as well as a few non-legislative based suggestions to better serve the interests of the people or consumer of services and the companies providing them.

9.ACKNOWLEDGMENTS

Our thanks to ACM SIGCHI for allowing us to modify templates they had developed.

We would like to thank Professor Kristin Tufte, the instructor for CS410: Explorations in Data Science, for providing advice, ideas, and resources for this project.

10.REFERENCES

1. Ed Pilkington. 2016. 'Edward Snowden did this country a great service. Let him come home'. (September 2016). Retrieved August 16, 2019 from https://www.theguardian.com/us-news/2016/sep/14/edward-snowden-pardon-bernie-sanders-daniel-ellsberg

2. Wabc. 2019. Long Island man billed nearly $1,900 in fraudulent Uber charges. (January 2019). Retrieved August 16, 2019 from https://abc11.com/technology/man-billed-nearly-$1900-in-fraudulent-uber-charges/5095741/

3. Electronic Privacy Information Center. EPIC - Apple v. FBI. Retrieved August 16, 2019 from https://epic.org/amicus/crypto/apple/

4. Peace Brigades International. Retrieved August 16, 2019 from https://www.peacebrigades.org/en/kenya

5. General Assembly backs right to privacy in digital age | UN News. Retrieved August 16, 2019 from https://news.un.org/en/story/2013/12/458232-general-assembly-backs-right-privacy-digital-age

6. CyFy. Retrieved August 16, 2019 from https://www.orfonline.org/cyfy/

7. WhatsApp FAQ - End-to-end encryption. Retrieved August 16, 2019 from https://faq.whatsapp.com/en/android/28030015/

8. AdBlock. AdBlock. Retrieved August 16, 2019 from https://getadblock.com/

9. Jon Swartz - https://www.barrons.com/articles/facebooks-big-data-breach-could-cost-it-over-1-billion-1538417905

10. Kelligrant - https://www.cnbc.com/2017/02/01/consumers-lost-more-than-16b-to-fraud-and-identity-theft-last-year.html

11. Negash S., Gray P. (2008) Business Intelligence. In: Handbook on Decision Support Systems 2. International Handbooks Information System. Springer, Berlin, Heidelberg.

12. Mitra, & Agrawal. (2015). 5G mobile technology: A survey. *ICT Express, 1*(3), 132-137.

13. Yilmaz, O., Zexian Li, Valkealahti, Uusitalo, Moisio, Lunden, & Wijting. (2014). Smart mobility management for D2D communications in 5G networks. *2014 IEEE Wireless Communications and Networking Conference Workshops (WCNCW),* 219-223.

14. Aiqing Zhang, & Xiaodong Lin. (2017). Security-Aware and Privacy-Preserving D2D Communications in 5G. *IEEE Network,31*(4), 70-77.

15. Ahmad, I., Kumar, T., Liyanage, M., Okwuibe, J., Ylianttila, M., & Gurtov, A. (2018). Overview of 5G Security Challenges and Solutions. *IEEE Communications Standards Magazine, 2*(1), 36-43.

16. 李侠宇,沈鸿.5G网络安全发展趋势研究[J].电信网技术,2016(12):42-44

17. Benzekki, K., El Fergougui, A., & Elbelrhiti Elalaoui, A. (2016). Software−defined networking (SDN): A survey. *Security and Communication Networks, 9*(18), 5803-5833.

18. 吴春德.基于SDN和NFV的5G移动通信网络架构的设计思路[J].信息通信,2019(06):218-219.

19. 黄睿. 面向SDN/NFV的安全服务链映射机制研究[D].战略支援部队信息工程大学,2018.

20. 严苗苗. 5G网络之切片安全[A]. 《建筑科技与管理》组委会.2018年9月建筑科技与管理学术交流会论文集[C].《建筑科技与管理》组委会:北京恒盛博雅国际文化交流中心,2018:2

21. Foukas, X., Patounas, G., Elmokashfi, A., & Marina, M. (2017). Network Slicing in 5G: Survey and Challenges. *IEEE Communications Magazine, 55*(5), 94-100.

22. 张俐欢. 5G网络切片中的异构安全通信研究[D].西安电子科技大学,2018.

23. Delphinanto, A., Koonen, T., & Den Hartog, F. (2011). End-to-end available bandwidth probing in heterogeneous IP home networks. *2011 IEEE Consumer Communications and Networking Conference (CCNC),* 431-435.

24. Li, Xu, & Zhao. (2018). 5G Internet of Things: A survey. *Journal of Industrial Information Integration, 10*, 1-9.

25. 苏洲.网络安全--5G的基石[J/OL].中兴通讯技术:1-5[2019-08-15].http://kns.cnki.net/kcms/detail/34.1228.tn.20190708.1630.006.html

26. John W. Dowdell. An American Right to Be Forgotten. Retrieved August 16, 2019 from https://digitalcommons.law.utulsa.edu/tlr/vol52/iss2/23/

27. 2019. Facebook hit with $5-billion federal fine for privacy violations. (July 2019). Retrieved August 16, 2019 from https://www.latimes.com/business/story/2019-07-24/facebook-ftc-facebook-5-billion-fine

28. Google Spain SL v. Agencia Española de Protección de Datos. Retrieved August 16, 2019 from https://harvardlawreview.org/2014/12/google-spain-sl-v-agencia-espanola-de-proteccion-de-datos/

29. Heterogeneous 5G Networks. Retrieved August 16, 2019 from https://www.openairinterface.org/?page_id=458

30. Retrieved August 16, 2019 from https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8436400

31. Kelligrant. 2017. Identity theft, fraud cost consumers more than $16 billion. (February 2017). Retrieved August 16, 2019 from https://www.cnbc.com/2017/02/01/consumers-lost-more-than-16b-to-fraud-and-identity-theaft-last-year.html

32. Michael Nuñez. 2019. FTC Slaps Facebook With $5 Billion Fine, Forces New Privacy Controls. (July 2019). Retrieved August 16, 2019 from https://www.forbes.com/sites/mnunez/2019/07/24/ftcs-unprecedented-slap-fines-facebook-5-billion-forces-new-privacy-controls/#1379a6965668

33. Jon Porter. 2019. Google fined €50 million for GDPR violation in France. (January 2019). Retrieved August 16, 2019 from https://www.theverge.com/2019/1/21/18191591/google-gdpr-fine-50-million-euros-data-consent-cnil.

34. SDN and NFV. Retrieved August 16, 2019 from https://nets-international.com/insights/sdn_nfv/

35. Jon Swartz. 2018. Facebook's Big Data Breach Could Cost It Over $1 Billion. (October 2018). Retrieved August 16, 2019 from https://www.barrons.com/articles/facebooks-big-data-breach-could-cost-it-over-1-billion-1538417905