Privacy in the Age Of Information (and algorithms)*

Bipin C. Desai
Concordia University
Montreal, Canada†

Nov. 2019

Abstract

This paper raises the privacy issues related to information that is accessible about individuals from their mobile devices and that which is collected when they interact with and use so called "free" services provided on the web. The importance of privacy has been ignored by most legislation and any laws passed have no teeth. The only exception is the privacy protection that is embedded in the EU's General Data Protection Regulation(GDPR). GDPR gives control to individuals over their personal data and requires any organization which collects and controls personal information to have in place appropriate measures both technical and logistic, to implement the data protection principles. In this paper, we propose a technical solution to provide a personal email and web server with complete control of all correspondence and contents. This would liberate users from fake free services and provide privacy and security.

Keywords: Privacy, security, online social networks, free email service, warrant-less constant surveillance, Heimdallr

1 Privacy its rise and fall

According to some, privacy was the result of the growth of the middle class who could afford better housing and their abode, even though humble, became their castle. Liberalization of laws such as the one that took the state out of the bedrooms recognized the right of people to be left alone. However, this was only at the governmental level since it had supreme power but the corporations were left to regulate themselves. At the end of the first gilded age, the need was felt to regulate the robber barons and their corporations. This was done by the emergence of the workers unions and the need to share the riches with the worker. The latter was implemented with a progressive tax system that supported the common good by taxing the haves to transfer to the have-nots. This afforded the luxury of privacy to the not so rich! It must be noted that recently, the Supreme Court of the largest functioning democracy in the history of humankind has ruled that privacy is

*This is a corected/updated version of an article presented during IDEAS 2019, Athens, Greece, 10-12 June 2019

†BipinC.Desai@concordia.ca ORCID: 0000-0002-9142-7928

a human right [44]: this in spite of an inane pronouncement of a kid who became fabulously rich and influential[53].

The tools and technology that are the roots of the privacy exploitation required many developments: quite a number of these occurred in the mid 20th century. The first of these was the introduction of computers and the development of semiconductors, its miniaturization and increase in computing power. The interconnection of computers and hence people was made possible with the introduction of the Internet. In the early days, access to the internet was limited to the academic communities, some businesses and government agencies. The introduction of the web and the development of the graphical browsers opened up the internet to an increasing number of users.

The offer of web based free email service by start ups fuelled by venture capitalists allowed these companies the continuous access to all email communications of an increasing number of users worldwide! The undeclared charge for this free service was and continues to be the contents of their messages and these users who in turn attracted more users and more contents; there being no laws to protect the privacy of the contents of these messages, which are in plain text. This clear text is the raw material for tailoring targeted publicity to the users of this service thus monetizing the 'free' service.

The graphical web browser also opened up a new method of communicating with family and friends. However, since the majority of users were seduced by the allure of setting up a free web presence without the need to be tech-savvy, this was the start of what we now call online social networks(OSN). The OSN attracted not only friends and family but complete strangers. This attraction of becoming a celebrity has been the force that pushed up the number of such users to billions. To this date, instead of recognizing themselves as publishers, these OSN claim to be simple platforms and take no responsibility for the content they provide which has created many problems, including bullying, extreme self-harm, fake news, genocide and terrorist act co-ordination[95].

The web opened up the internet to the non-tech savvy user. Instead of creating tools to make the Internet service such as email to be used privately, securely and easily accessible to the non-tech savvy or offering it via the national postal service, the unimaginative politicians let it be provided by venture capitalists.

A system such as the web robot and allowing any robot to be volunterily restrictes by a simple text file and hence served freely by most web servers was one of the biggest blunders made by the web community. The other blunder was to include third party contents and introduction of state by cookies and thier derivatives. The taking over of the web by the commercial players and facilitating tracking in the web browser are other blunders driven by monetizing the web. It is reported that there is an attempt to undo the harm in the new web but again, some of the players are the same as in the first web, and the same commercial pressure would jeopardize this solution.

The cell phone which started out as a bulky device profited from the miniaturization of semiconductor circuits and started getting smaller, lighter and more popular. The addition of a screen and more computing power and better and better networks transformed the cell phone from an emergency device to a personal communication device. The tech giant companies made sure that the new 'smart' cell phones have access to their services and the cell phone replaced the personal computer and the land line. The cell phone system also allowed bypassing the need of setting up an extensive telecommunication infrastructure and the need for laying and maintaining cabling and relay stations. This was replaced by cell phone towers and relay stations. The mobile

system speed-ed up communication in emerging economies as well as the developed ones.

With the growth of the internet and the mobile communication infrastructure, the opportunity of gathering data on individuals from their communications and interactions became relatively easy. The set up of the Global Position System(GPS) in the early seventies by the USAian government [46] along with the worldwide free access to the Standard Positioning Service (SPS) provided precise location information. A system to use the GPS location is built into the current generation of mobile hand sets. The many applications available for the mobile phone made it possible to introduce services many of which require SPS. The use of the global positioning system allowed the various applications running on cell phones to keep abreast of the location of the user. Some of these, useful to the user for applications such as directions and maps, allowed the marketing of nearby businesses to the cell phone user.

Furthermore, the applications on the mobile system allowed their developer to precisely know the whereabouts of the mobile device and hence its owner. These locations are recorded by the application developer and the supplier of the mobile operating system. Along with the web and the cell technology, the access to users data in their communications and by tracking their use of the web and applying the advances in computer science including data management and algorithms for machine learning etc. created what Zuboff calls Surveillance Capitalism[99]. The exploitation of personal data by private corporations is finally drawing the attention of scholars, and columnists and it is finally reaching the masses. The addiction to the cell phone means that one is constantly looking at it even when out in company with friends and family for a meal or just walking around.

The recognization of corporations as legal entities made it possible to put in power politicians which reversed the progressive nature of the taxation in the wrong belief that there would be a trickled down effect from the haves to the have-nots. Unfortunately, this effect has not occurred and the growth of the middle class has been halted and reversed. Competition by having another company provide similar, privacy oriented service, seems hardly possible. Because of the large share of the market another similar OSN, even one such as Google+ did not succeed.

1.1 Exposure to Privacy in the Computer Science Curriculum

Many of the current tech giants are headed by people who may have followed a computer science program and/or are "tech-geeks", while some of them are drop outs. One can safely assume that the majority of the coders could have had a computer science related education. However their exposure to humanities and social sciences would have been very limited if null as it is in many CS programs. The curriculum recommendation from ACM/IEEE includes the following: "A computer engineering curriculum must include preparation for professional practice as an integral component. These practices encompass a wide range of activities including management, ethics and values, written and oral communication, working as part of a team, and remaining current in a rapidly changing discipline." However not much is said about issues of privacy and security except that it is not ethical. However, with the recklessness shown by the robber barons of the late 20th - early 21st century who go ahead like bulls in a china shop and seem to have no regards for a person's privacy.

The sample curriculum for Computer science which runs into hundreds of pages[3] includes exposure of the student to Social Issues and Professional Practice and the documents point out that "Graduates should recognize the social, legal, ethical, and cultural issues inherent in the dis-

cipline of computing. They must further recognize that social, legal, and ethical standards vary internationally. They should be knowledgeable about the interplay of ethical issues, technical problems, and aesthetic values that play an important part in the development of computing systems. Practitioners must understand their individual and collective responsibility and the possible consequences of failure. They must understand their own limitations as well as the limitations of their tools." In the section SP/Privacy and Civil Liberties which is two 2 Core-Tier1 hours wherein the philosophical, legal aspects, privacy tools and implications and related issues are presented. This hardly seems adequate and is likely to run off the proverbial duck's back. Since some of the aspects of this responsibility are not encouraged to be practiced in the rest of the program the final impact is almost nil. What is puzzling is that in Appendix C of this document where course exemplars are given, there is not a single one just for SP/Privacy and Civil Liberties. One, given on page 304 on Social Issues and Professional Practice, is part of a course which includes Human Computer Interaction and Graphics and Visualization. Another example is Ethics & the Information Age [3], (p436) which however does not touch on the philosophical issue of property, person-hood and the right of a person to privacy. In Stanford university's CS program the course CS181 – Computers, Ethics, and Public Policy allocates a scant 1.6 hours to Privacy & Civil Liberties [3] (p501).

The privacy and security framework[19] of the Canadian Institute for Health Information (CIHI), an independent, not-for-profit organization provides essential information on Canada's health systems and the health of Canadians. Most engineers and software designers are not very well exposed to privacy and may have been exposed minimally to security. However they and the marketing people would likely ignore most of the issues in such frameworks.

The privacy and security page of the USAian Federal Trade Commission(FTC) has the following about data security: "Many companies keep sensitive personal information about customers or employees in their files or on their network. Having a sound security plan in place to collect only what you need, keep it safe, and dispose of it securely can help you meet your legal obligations to protect that sensitive data. The FTC has free resources for businesses of any size"[39]. The guidelines are only for self regulation and the penalty is fairly small; as reported recently, about 22 million USD[35]. The issue addressed by FTC is based on the agreement it had with Facebook for privacy but the FTC claims that the company "deceived consumers by telling them they could keep their information on Facebook private, and then repeatedly allowed it to be shared and made public" [35]. Compare this paltry sum with the one in the guidelines for the EU which call for maximum penalties or 20 million Euros or up to 4% of the world wide revenue for a single breach which can add up to billions of Euros[7]. In the USAian system the privacy issues are being handled by a trade commission, not a human rights agency.

Even though there is so much concern about security, there have been some large breaches in recent years. Many systems store sensitive information such as passwords in clear text. The fact that the tech giants share information with third parties is enough for one to opt out of any system that needs third parties to carry on their central tasks.

2 Source of Privacy Violations

The biggest sources of privacy violation are invisible. On-line shopping requires passing valuable personal information to big as well as small retailers. Some of them are fly-by-night ones while others are multi-billion dollar enterprises. Many small fries are on the coattails of specialized

shopping portals. Many of these retailers, to increase their revenues, turn around and sell the personal information to data aggregators. The portals also could have access to such data and can use it to direct publicity for products and service to the users and with the use of cookies and trackers all this data goes into many different data repositories to be exploited, ad infinitum.

While shopping or doing any operation on line,, one is tracked by a myriad of trackers. A case in point is a session with one's own bank. If one has a tracker reporting add-ons in the browser, e.g., Privacy Badger, one sees the trackers used by these banks to track their own costumers and share the data with these third parties! A question sent to the bank of why this is being done is never responded to!

2.1 A Typical privacy agreement

When a person signs up as a user of most of the 'free' on-line services or to services such as mobile phone supplier, she accepts, unread much less with a clear understanding of what it implies, their privacy policy which is linked to equally unread and not understood data policy. These policies may be updated without the users' consent. As an example if one considers the privacy policy [34] and the data policy [33] of Facebook, which runs to, in the version currently accessible, 7 and 9 pages respectively; it is no wonder no one reads these and assumes that these privacy policies mean that the site will keep her personal information private and would not share it without her permission[84]. Little does the unsuspecting person knows that she is giving away a free license to persons and organizers who believe that privacy is no longer a social norm[53].

The user is required to let the supplier of the service reserve the right to process, sell, trade or rent aggregated or the users information which is anonymized. It is well known by now that most anonymizing schemes can be thwarted by combining information from multiple sources. The information that is up for grabs includes.[1]

Personal information: including name, mailing(postal) address, email address, telephone number, IDs of accounts, device identifiers, PIN, service provider information, account including credit card credentials, passwords, records of all communications as well as details of contacts.

Applications: All providers of applications have access to not only their own application data but also may share this data with other applications on the device. This looks like a modus operandi of all applications and as Zuboff says, anything that is not guarded would be claimed by these new pirates.

Back-up data on cloud: Could have access to users' personal information including contacts, email addresses, calendar, memo, tasks, display pictures, status messages, photos, audio, videos – the stated reason is to be able to restore this information.

Cookies: These were introduced in the web space to overcome the stateless nature of the web protocol. The reason for a stateless nature of the web was due to the philosophy of free sharing of knowledge. However, cookies and their derivatives have morphed into a nefarious form to facilitate surveillance.

Financial Information: Any transaction through the system may require credit status checking etc. any or all of which could be recorded and shared with other parties.

[1]The following is based on the privacy/data agreement of a number of organization including - Apple, Blackberry, Google, Facebook, etc.

Third party information: The service provider may combine your information with ones obtained from other sources.

Retention of Personal information: Even after the expiry of any direct association with the service provided it could be retained perhaps in an anonimized form and may be used perpetually.

International operations and onward transfers: The service provider, would require you to consent that your personal information may be collected, used, processed, transferred or stored in multiple jurisdictions.

Communication: The service provider may communicate information, surveys, marketing materials, advertisements or personalized content. The service provider may share your personal information within the service provider and with their service providers, financial, insurance, legal, accounting or other advisors.

Here are some of the things these systems have your permission to lay claim on! Any information and content you provide or they collect from creating or sharing content, contents of messages or communications with others. and all information provided while using any of their products including information of the account. They collect details about your connections, address books, logs, meta-data and contents of all communications including all SMSs and emails; pattern of usage including what, when, where, who (and use their algorithms to try to figure out why!). All transactions made which includes purchases which would include the details of the credit/debit cards used, authentication information, addresses and contact information about the transaction. In addition they have access to actions taken by your contacts and the information they provide. Your location information is used to determine where you live, where you go, what events you attend and where you are at any point in time. All this information is used to create targeted publicity which is tailored to influence you, using your foibles determined by their unknown algorithms.

The proliferation of the internet via the medium of the web to offer all types of services requires a user to sign-up using a user name and a password. Since more and more services (e.g., news, financial, Governmental, social and commercial) are now offered through the web a typical user may have scores of user IDs and passwords. The tech giants, to increase their presence, have offered to enter into an agreement with many of these services to let the users employ these tech giants credentials to log into these services. Thus the tech giants can trace the user not only on their own platform but can have access to what other services are being used and whatever other information the target service may provide the tech giant. What and how the information these giants would glean besides associating yet more data points in the profiles for these users is not advertised or communicated to the user.

3 Privacy violation at any level of sharing

One of the culprits in the current loss of privacy is the USAian system, its constitution and the outlook of its capitalistic system. Whereas there are some forms of restraint for the USAian governments collecting and using personal information in its constitution and amendments, the private sector is left alone to do as it pleases with a laissez faire self policing attitude. What the citizens do not trust the government to spy on is allowed to the private corporations. That self regulation does not work is amply illustrated in the recent Boeing 737 Max's design flaws which

led to two deadly crashes. An optional display that showed the disagreement of the angle of attack sensors on the Boeing Max required additional cost in the millions for the plane.

Furthermore, the fact that Boeing was able to get away with not having the Federal Aviation Agency(FAA) really act as an independent quality control shows that self regulation is unreliable. According to [31], [28]. "The problems were apparently compounded by FAA rules allowing manufacturers to essentially self-certify aircraft. Boeing reportedly tried to speed up the process in order to catch its rival Airbus A320neo, and pushed the FAA to give it more responsibility. There wasn't a complete and proper review of the documents," a former Boeing engineer said. "[The] review was rushed to reach certain certification dates." [31]. The failure to provide the correct software and the required equipment for a high priced air-frame leads one to conjecture the type of security employed by many of these tech giants who have no regulation, no oversight and no competition and pay little taxes. They fail to reveal a breach of security or the lack of it for months and years. According to the press, Google did not reveal a security breach for fear of regulations[29].

With current internet and wireless technology, people actually pay to use the free services in the form of internet connection monthly charges, buy and pay the connection fees for 'smart' devices that allow them to be tracked. Unlike criminals who are tracked by a tracking device imposed on them most consumers now carry a tracking device and pay for it handsomely, every month including for the bandwidth used for tracking.

The result of the USAian system, where the tech giants are based, is that the private sector has laid claim on personal and private information of users of the myriad of devices that they own. Most of the smart devices are controlled by just two operating platforms again controlled by USAian tech giants. In addition, they control the application stores that users can download the 'apps' from and earn a percent of the fees for these applications. One wonders if this is not an example of a monopoly! Example of such laying a stake, like the one used in the gold rush of yore, is to claim all human experience as free raw material without any concern for individual rights and without any payment of any source[99]. As Zuboff compares these to the edict recited by the Spanish conquistadors and later the settlers of the west in what is now known as the U. S. A. This edict gave the conquistadors and the settlers some form of divine rights which allowed them to usurp the lands of the existing people and displaced them or wiped them out[99].

Google made six cooked up declarations which confer on themselves the right to translate the recorded experience of its users into behavioural data and own it, abuse, use and share it as they see fit and preserve these for perpetuity. They had no problem getting all this data since they had captured the search, the email and the the cell phone markets. They also are in control of the application market place for their cellphones. Another instance of conquest by declaration is the self proclaimed one by the Facebook founder which stated that privacy as no longer a social norm. This statement from a person with very little background in privacy was convenient since it was the basis of Facebook's business model[53] and this declaration, along with a changeable data/privacy policy has been used to mine the information entrusted to them by unsuspecting users. Facebook's usage of this data has been seen to violate the users privacy in many ways. This includes influencing them not only to buy products and services of questionable need but also to expose them to fake and biased news and help create targeted persuasive ads to influence a vote for doubtful candidates and proposals. It is no wonder, over the years Facebook has faced increasing scrutiny borne out by the number of times it has been cited by the privacy commissions, the courts and the popular press[30]. Facebook allowed phone companies [58] and other tech giants access to user data.[27]: they stretch and overstep privacy and competition laws and should be regulated

urgently[58]. Others have [23] and want to take Facebook to court[45].

According to the summary of the final report[72] of UK's Digital, Culture, Media and Sport Committee: "among the countless innocuous postings of celebrations and holiday snaps, some malicious forces use Facebook to threaten and harass others, to publish revenge porn, to disseminate hate speech and propaganda of all kinds, and to influence elections and democratic processes—much of which Facebook, and other social media companies, are either unable or unwilling to prevent. .....The big tech companies must not be allowed to expand exponentially, without constraint or proper regulatory oversight. But only governments and the law are powerful enough to contain them. The legislative tools already exist. They must now be applied to digital activity, using tools such as privacy laws, data protection legislation, antitrust and competition law. If companies become monopolies they can be broken up, in whatever sector. Facebook's handling of personal data, and its use for political campaigns, are prime and legitimate areas for inspection by regulators, and it should not be able to evade all editorial responsibility for the content shared by its users across its platforms"[89]. Even the people who were involved in the early days of Facebook and its mentor seem to agree with the findings of this and other reports[66], [48], After having collected millions of email addresses, Facebook says they would stop this practice and notify users[47].

Facebook has used parental influence to mould UE laws[40] and put pressure on politicians, around the world, by promising local investment such as installing data centers in exchange for lobbying for the company to block privacy laws and any forthcoming laws should be Facebook friendly[16], [90]. The fact that the earnings the companies make by their presence in a country is not being taxed is something that the tech giants have been successful in protecting and they continue to lobby for it[90]. Facebook allows governments to target individuals and groups to the extremes, e.g., Rohinga genocide[51], [55] The new virage of Facebook to privacy seems to be fake and meant to decrease their civil liabilities and in fact yet another business spin to try to protect their dominant position and keep at bay the regulations and any corporate breakup[13] [88]. Some demands for investigating the lobbying of tech giants are ignored by those in power who hope to benefit from their largess at election time[71].

3.1 Examples of privacy violations

Over the years, there have been many instances of violation of the common notion of privacy. Even the blanket surrender of privacy in the privacy agreements of the tech giants is often not honoured, much less the notion of privacy formed over the last few centuries. An overall view is recently reported in [93] that Google's street view violates privacy by taking videos of private homes spaces along with people therein and publishes them without any authority. When met with resistance, the recording operation was held off and the cameras returned when no one was looking.

Facebook Beacon published purchases made by users without their express consent. Facebook uploaded email contacts of 1.5m users without consent and when discovered says it was inadvertent. Actually it used a feature of a previous version. As usual the information mined from the user contacts and propagated into other databases may not be deleted but used. More of deny, deflect etc.

Google says a microphone in one of their products, which was not revealed to the buyers, was never activated; one has to take this with a grain of salt when the courts have to tell them to take down world-wide, search results of selling on the web products manufactured in violation of

trade secrets [18] There have been many instances of tech companies being warned about privacy. One such is the report by Denham, the Assistant Privacy Commissioner of Canada[26]. At that early date the report concludes "that Facebook did not have "safeguards in place to prevent unauthorized access by application developers to users' personal information, and furthermore was not doing enough to ensure that meaningful consent was obtained from individuals for the disclosure of their personal information to application developers"[26].

There is a class action suit against Facebook that has been going on for years in British Columbia and the company has used all its resources to keep this from being resolved. The case concerns the practice used by Facebook as of 2011 to feature, users' 'likes' in publicity without the explicit users' consent. The class action was filed in May 2014[23]. The company denied it saying that the consent was automatic and fought it all the way to the Supreme Court of Canada and after many years, the case was won by the plaintiff and the class action was returned to the BC courts after close to four years. It may take a few more years before the class action suit is decided and of course there would be appeals and likely trips back to the supreme court. In the meantime most people would give up and this is what companies, with deep pockets able to hire the best lawyers, count on. For not obtaining explicit consent from users to use their data, Facebook is facing a fine of up to 5 billion USD from the USAians Federal Trade Commission.

Companies claim that they protect your data; however, it seems that in fact they exploit it and are being hacked as reported in the popular press time and again. The number of breaches of data from companies is affecting more and more people since the early days when Apple stored passwords in the clear and had to grudgingly own up[93] to it

3.2 Childrens' Privacy

Children's Online Privacy Protection Act (COPPA) [38] this two decades old USAian federal act protects childrens' privacy by giving parents tools to control what information is collected from their children online. The personal information consists of: a first and last name; a home or other physical address including street name and name of a city or town; an e-mail address; telephone number; a Social Security number; any other identifier that could determine the physical or online contact of a specific individual; or information concerning the child or the parents of that child that the website collects online from the child and combines with other identifiers . A number of tech giants have been fined under the COPPA violation. TikTok is an OSN for video-sharing application and it is alleged to not seek parental consent before collecting information from children under 13 years old[87]. The company is banned by the governments in India and Bangladesh and has been fined in the USA[86].

Other on-line tech giants let children run up credit card bills using in application charges while playing games on devices such as iPad and iPhone. This kind of preying on children has been going on for a long time as illustrated in a story involving Farmville, a Facebook game, reported in 2010[52].

3.3 Legal Actions

The Privacy Commissioner of Canada had launched an investigation in 2018 to examine if Facebook's practices are in compliance with Canada's federal private sector privacy law, the Personal

Information Protection and Electronic Documents Act called PIPEDA)[69] However, this was not the first time: there were early warnings in 2009 about the privacy issues with OSN such as Facebook [63], [83]. Many of the complaints found Facebook to be in contravention of the Act and Facebook was to take corrective measures. However, as in the class action launched by Deborah Douez, the case has been going on over many years and is yet another example of the deny, deflect and defend mentality of these tech giants[23], [24], [25]. In a more recent report of joint investigation of Facebook by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia the conclusions drawn are that Facebook failed to obtain valid and meaningful consent of users nor their friends. Furthermore the company did not have adequate safeguards to protect users information and was not accountable for the information under its control[73]. The selective restriction used by Google for example in Google v Equstek Inc, was found to be not sufficient and the request for a worldwide ban was upheld.

The availability of free widely used OSN platforms allows anyone to post anything on it. The posters range from ignorant and zealot bigots, paid geeks and agents of governments to misinformed twitters. After many denials and deflections some of these OSN are finally admitting that their platform is a vehicle for fake news etc. [43] and making a feeble attempt to do something. However, the attempt is lack-lustre, for example a mere 40 people to fight millions of potential sources of fake news. The company is making sure to get as much spin out of it as possible by inviting dozens of journalists into the 'war' room to fight this fake news; there being a claim that these crews are backed by other unnamed and unseen experts and of course the unknown, unproven algorithms!

While these tech giants claim not to be evil and want people to connect, they are in fact exploiting the recorded human experience to enrich themselves. By using the leverage of different kinds of equity(more than one vote for some types of shares, no vote for others and/or and not allowing some of the voting shareholders to vote against members of the board), they retain the majority voting rights and make sure that the reins of these tech giants are preserved in a dynastic fashion. The financial security system of their host country (USA) allows this type of capitalism. The USAians, who seem to not question such practices to encourage growth without much social good, are responsible for this dystopian status which continues to degrade human existence not only in their country but in most other countries. The exceptions are those countries who have put in safeguards and nurtured their own tech giants.

To challenge what these tech giants have usurped and now own via legal action, except for a few of us, is beyond[23] the economic means, personal energy, commitment and moral resources of the rest of us.

4 Waiting for a Solution

The protection of privacy, a human right, under threat from tech giants and goblins that they create requires some action. This could be either in the form of political and legislative and the form would be regulations and legislation with sizable penalties proportional to the income of the culprit, taxing the income etc. Another approach to be used is to set up national service for what now has become a way of many communications. The third approach, presented in the next section, is a technical solution to render the tech giants obsolete!

An opinion expressed in the press for handling the tech giants is to recognize the service they

provide as public service and either provide a national service under the control of an independent neutral organization and/or socialize them[82]. They have monopolized a number of services that they have usurped or re-engineered and made the population addicted to them. The addiction is evident in the homes, offices, public places and social get togethers where everyone constantly glances at their hand held devices[68]. These addicts are waiting for the next shot! No one seems to have recognized this addiction.

Waiting for a political solution is like "En attendant Godot" [14] but Godot never comes. The bent politicians are not in a hurry nor seem to have the moral strength to breakup these tech giants. The addiction that has been created with the so called free services has kept the politicians at bay. No thought has been given in any government to set up a national email service as an essential public infrastructure much as health, postal, road, school or train service. Even the tel-comm service is regulated in most countries. Since the internet depends on the tel-comm service it should be regulated with the tech giants at least held responsible for the contents. They should be taxed on their earnings in the jurisdiction where it is earned; there should be a penalty for the jobs that are shipped outside the country and for importing and exporting data. The tax should be at a progressive rate where the majority of the excess profit is taxed. This may encourage the tech giants to set up jurisdictional data farms to serve local emails, social contents.

Douthat[30] compares the western internet dominated by the USAian tech giants and the Chinese one dominated by the central government. The result in the western one is the addiction generated by the internet and the control of it by a few corporations which at times work with the government and mistakes made on it are magnified. Lies and fake news are spread by it and real news is, by repetition from the top, labelled as fake news[30].

Cryptocurrency has evolved much later than search engines. Its spread is liable to upset the financial sector and the basis for the support of the political system everywhere much as the so called open internet has done by concentrating the imperialistic nature in the hands of a few tech giants all under the USAian form of capitalistic protection. However, the move to regulate Cryptocurrency has already begun in the form of legislators in various parts of the world. Regulation of the tech giant to respect the privacy of its users and not exploit their personal information to manipulate them is missing.

4.1 A possible start

One of the principals of privacy in the European Union's General Data Protection Regulation(GDPR) is that a person is the owner of her data and she has the right to decide who can use it and how. Regardless of where and how the data is shared, it can be amended, deleted or she could determine who and how it would be accessed [32]. GDPR went into effect in the EU in May 2018[42]. Its objective is to give control to individuals over their personal data and requires any organization who collects and controls personal information to have in place appropriate measures, both technical and logistic, to implement the data protection principles.

Such organizations are required to disclose their legal basis and purpose of data collection operations and have publicized the period of data retention and and the sharing of it with third parties. The data collecting organization are required to provide, to any data subject on request, a portable copy of the data collected in a common format. The data subject has the right to have

their data corrected or even deleted. There are penalties for violation of this regulation, For a violation of this regulation, recently France has fined Google 5.7 Million USD[75].

In the few months of coming into force of GDPR[42], the USAian government is finally waking up to some form of legislation for consumer privacy[59], driven ironically, not due to concern for consumer privacy but as another component of high tech competition as outlined by Apple's CEO[21], [50]. In the meantime activists are filing an increasing number of complaints under the GDPR[6]. In spite of the protection afforded by GDPR, the legitimate business interest of the data processor still override the fundamental rights of the data subject!

GDPR applies only to the EU, but given the scale of the market, many companies are deciding it's easier – not to mention a public relations win – to apply its terms globally. The problem is that even if there is a directive, even from a court, tech giants seem to consider themselves immune to these. A very recent example of this concerns a ban put in by a New Zealand court to name an accused killer. The local media companies, against whom the court could take action, use resources to make sure such court bans are respected not only by themselves but also by their own social media channels. Google which does not apply bans globally and in line with this policy of geo-blocking (which is basically not being bound by local blackouts globally but only in the jurisdiction concerned) had emailed this information out to users, apparently not in New Zealand, who had signed up for "what's trending in New Zealand"[57].

The effect of GDPR[41] is being felt on this side of the Atlantic and accessing, for example a proper notice about cookies and use of analytics has to be given to EU citizens when they access USAian web sites: as usual there is an 'agree' or 'not agree' option! As usual it is too tempting to agree instead of looking at the privacy policy, third party partners or terms of service which are many pages long as pointed out earlier.

Competition by having another tech start-up to provide similar service seems hardly possible. Because of the large share of the market another similar OSN, even one such as Google+ did not succeed. Other avenues being used in the EU is to allow competition by blocking the tech giants from buying start-ups who may become a serious challenger some day. Such acquisitions have been allowed to proceed in the USA to date: buying of WhatsApp and Instagram by Facebook are examples. The European model where the dominant giants are forced to share the data [32] goes back to the conclusion of the Workshop A held in April 1995 which recommended search engines share information[9].

5 Way out of the privacy and security trap

The current situation where a small number of Usaian tech giants are controlling the web, all human knowledge and experience; they are manipulating awareness and beliefs to serve their aim of continued domination and maximizing profits. Their huge profits allow them to buy out any potential competition and are moving in new directions every day. This, after all has important elements in common with imperialism and totalitarianism. No surprise then that a country which experienced the latter most dramatically, Germany, has some of the strongest laws to safeguard privacy. Even still these efforts are merely corrective and merely polices the problem; not solve it. To actually overcome this system, a new solution is needed.

It is unlikely that many politicians who are heading governments or are part of the government

have much motivation to do anything about privacy. The existing laws have no teeth and the tech giants are happy to put up the three big Ds(deny, deflect, delay). Each year they can delay the action, they are more established, made a few more billions and were able to finance more elections and place their men(mostly) in the drivers seat.

There are many political ideas put forward by various aspiring politicians in the western world. This is so in the prelude to the USAian 2020 presidential election. They include breaking up the tech giants, giving more control to the users of their data, making the algorithms transparent etc. None of this may work; take for instance making the algorithms more transparent; most users who don't even read the privacy agreement would not be able to understand the working of the algorithms. It is also doubtful that the tech giants would ever be willing to make their algorithms transparent.

The other idea is to increase competition; however this is also a no starter. The tech giants have big market capitalization and have politicians in their pockets. They make all possible effort to influence politicians since they have direct lines to the ministers and presidents. As a result we are proposing here a method to turn the clock back and bring home all communications and the data that is shared.

5.1 Lifting the cloud

Most users of the 'free' services would not have read the privacy or the data-use policy when they sign up for these services. Reading these policies which are many pages long would be confusing with all their exceptions, and fighting any of its effect leads to years of battle in courts as is evidenced by the case cited earlier; such drawn out cases would exhaust the emotional energy of most users.

Web is a relatively recent way of doing things and as in many facets of human existence the way to do things swings from one way to another like a pendulum. Computing is no exception. We started with the idea of a 'one of computing system' which would have been used to produce useful mathematical tables to be printed and shared. In reality, this is not what happened. Computers were developed as a proof of concept and from there went to become what was called "main frames' - expensive and bulky systems. They were time shared by many users locally or remotely using dedicated telecommunication lines.

In the nineteen-sixties there were two trains of developments. A family of main frames were affordable enough to be used by many organizations to have their own computer systems and software development teams. At the same time mini-computers were developed to be used by smaller organizations and labs. The mini-computers evolved into the micro-computers and personal computer(PC) in the late 1970s and many people were able to have a personal desktop to do their own processing. The personal data was housed in the hard disk of the PC. Development of the hard disk technology allowed increase in speed and capacity. It was possible to store all personal information locally.

The development and the spread of internet in the 1980s and then the world wide web starting in the early 1990s along with the graphical browser allowed the non-tech savvy person to be connected. The misdirection of the web by mainly commercial interests and the opportunity to claim uncharted territories prompted many tech buccaneers and geeks of the "dot.com" craze to

start violating unwritten traditions and using and introducing surveillance tools, and thereby were able to amass huge troves of information.

The lack of the postal services to see electronic mail as a new public postal service, the ignorance and self-interest of politicians allowed the lack of regulation in the new domain transferring ownership of personal information of hundreds of million of individuals. The first incursions of private venture capitalists were in the domain of web search and email and the early companies included: Altavista, Yahoo, Excite, Lycos. Even though web search engines started appearing in 1993, it was a later entry which captured the search market with a distinguishing appeal which has disappeared in the avalanche of paid positional publicity. Even though most search engines produce similar results, the habits and default setting in browsers tend to prioritize this one!

As pointed out in [99] the concentration of data by such organizations is making it difficult for competition to be effective. The EU has ruled against Google many times in recent years; all of these are fought in the courts and the monopoly continues. The habits of people to flock to a system where others are and hence believe to be a better system has worked against titans as Google was forced to shutdown Google+ their social network. Not waiting for the breakup of these tech giants and believing that less is better we propose here for users to take back control of their data, lives and privacy by offering them a system to host their own email and web server and setting up their own social network.

In a previous work we have pointed out the privacy issues with the increasing number of IoTs which transmit personal information to the servers of the makers of the IoTs. The key there was Heimdallr and the setting up of a Software Assurance Agency(SAA) [1]. This agency, is an independent one and requires that any device manufacturer must submit all software and updates to it for verification. It is independent and hence not run by a tech giant. Software, if it is not sound and suitable would not be certified and distributed. Unlike the 'stores' run by tech giants, SAA does not get a percent of the revenue for the software; however it charges a fee based on the size of the corporation and the number of certification requests. It is felt that there is a need for an independent organization such as SAA for the software industry much like the certification authorities CSA and UL. Here we propose to extend Heimdallr to not only monitor the IoTs but also act as a server for a personal email system and the web.

There are many systems that allow users to create their own web pages: an example is Facebook! Considering the number of articles, and litigations it has generated it is time that instead of giving away all this information to a corporation and sharing it with strangers, a personal web server could be used to allow the personal web page accessible only to the immediate family and friends.

The fact that a micro processor such as Raspberry is very affordable and is suitable for driving a personal email and web server with very little load and bandwidth needed; that solid state memory and drives are now very affordable and could provide sufficient secure storage for the family server. The system would have its own storage and backup system; hence all storage of the family data, emails, web pages, comments etc. would be stored locally and there would be no need to use a cloud and thus deprive tech giants of the free raw material(data) and an opportunity to mine this information for their own profit. The proposed system, hence, includes processing and storage. With a cheap processor such as Raspberry 2, SSD and the modem functionality required in private homes to connect to the internet through the intermediary of an ISP takes on the function not only of a sentry but also of a data vault.

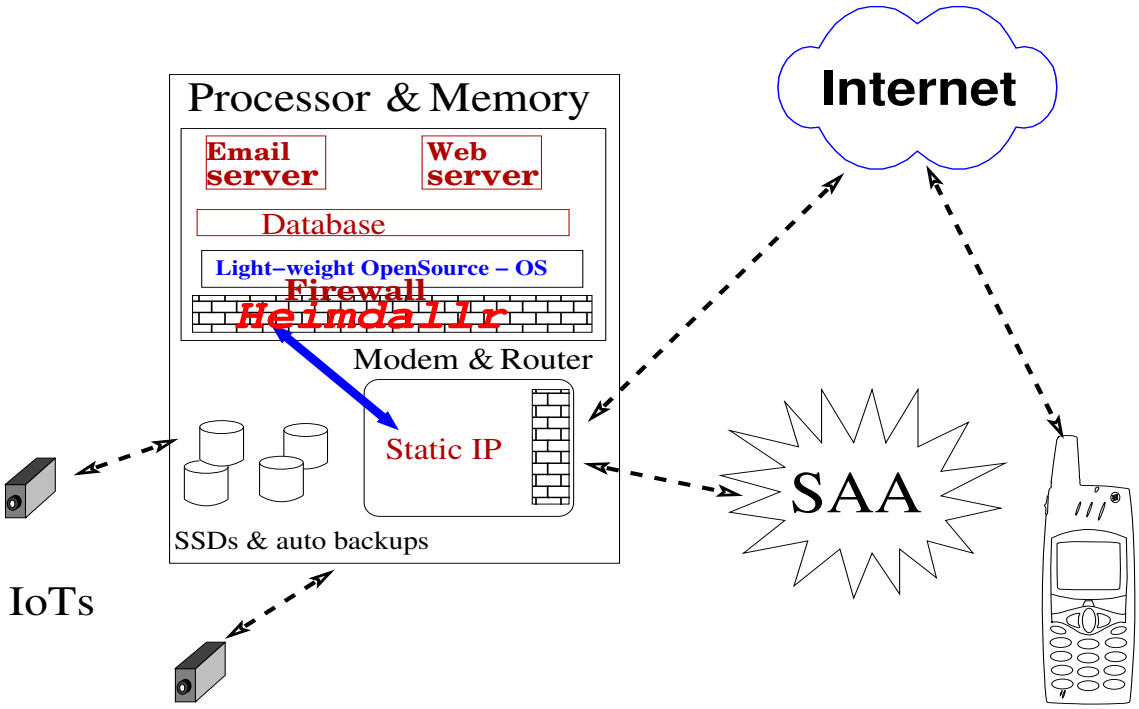

Figure 1: Proposal for a Technical Solution to address the tech giants privacy violation.

Arendt [5] in her chapter on Imperialism, while talking about Cecil Rhodes, quotes the words of Millen: "expansion is everything"[67]. Rhodes, looking at the stars and planet fell into despair since he wanted to annex all the planets for the British empire that he adored. Much like Rhodes some of the tech giants consider growth to be the good thing regardless of the collateral harm it does[66]. For instance Facebook knew that its platform could expose someone to bullying and coordinate terrorist attacks, This blunt memo by Bosworth recognizes that and noted that "The best products don't win. The ones everyone use win."[66]. With products like his, more users are attracted and they invite yet more!

5.2 Proposal for a Technical Solution

Breaking up the tech giants is not going to happen soon nor would an alternate commercial service start with the monetary power of the existing tech giants. They have the resources and staying power to bankrupt, buy and squash competition[98]. They have hundreds of lawyers working for them and connections to the highest level of the governments. The proposed system includes a modest processor, an email and web server,a light weight database, and a new generation of modem router. The system addresses the biggest source of privacy violation: email and web presence.

Our proposal is simple; add the functionality of an email server and a web server to the modem-wireless router that most people now have in their homes or small offices. This requires

the adding of simple interfaces to allow even the most non-tech savvy user to mange these servers. All emails will originate in the user owned system; the personal web server would host the person's web pages and all the contents would be stored locally. Access to the web server would be limited and the data could be shared as appropriate with various levels of security. Only invited persons would be able to access any contents and since the user is in control of the web server and all its contents, she has the full control. Heimdallr is the gate keeper and all interaction of the Internet and IoTs including those coming from the users and the IoT maker goes through the gatekeeper. All software updates, have to be submitted to the SAA which verifies them and if they pass the tests of functionalities, it is certified and accessible to Heimdallr. Only SAA verified software could be installed in the system

There would no longer be the need of any tech giants to provide email or web service. Technology has progressed to such an extent that these services could be incorporated in a device many home owners already have and its cost would be no more than that of the latest mobile device. The system would provide, each family in their own home an email server, a web server with their own family pages where they can post their news and share it with family and friends. The web server and the user interface would be such that expertise in making web pages would not be required. It is expected that the basics of internet usage, emailing, on-line chatting etc. would become programs in school. By including encryption in both the email and web contents, the leak of contents by eavesdropper is avoided.

The above development would mean that the not-really free services offered by the tech mammoths would not be required. So instead of waiting for a political solution from bent politicians, we are proposing a technical solution which would be created and maintained by the volunteer open source community and financed by required contributions from corporations making devices or software and donations by users.

6 Conclusion

The current practice of tech giants can only be neutralized by a technical solution where, their service would not be required. Once each family and business have their own static IP address and a hardened connection to the internet with a server that provides email and web service one becomes independent.The web server would not allow any robots and the gatekeeper, Heimdallr would not allow any untrusted/uncertified software to be installed in the system. The development of such a system is the next challenge of the academic community!

Acknowledgement

The author is indebted to scores of commentators and op-ed writers who have been able to see privacy being attacked by the tech giants and are bringing this to the attention of the general public.

Appendix: The web from an early participant

Soon after the so called official inauguration of the world wide web(WWW) in the form of the first WWW meeting in Geneva, a flurry of activities were held in U. S. A. This included a rushed announcement by the National Center for Super-computing Applications(NCSA) of 'Mosaic and the Web' conference, which was renamed WWW II, and was held in Chicago. Whereas the first was announced by Robert Cailliau the second was spearheaded by NCSA Mosaic[78]. One of the early resolutions of these two meetings was raised in the Navigational and Priority workshops held during the first world wide web meeting (WWW-1) in Geneva in 1994. Other activity in the first days of the web was one in July 1995: it being a forum held by the USA National Science and Technology Council's Committee on Information and Communication in Lister Hill Center (Bethesda, MD) entitled America in the Age Of information. A number of White Papers were presented[8]; looking through the list one finds that none of the white papers had touched on the issue of privacy. There was, but one, presentation on security.

During the subsequent early WWW meetings, some of the people involved in the navigation priority workshop devised various mechanisms for search in the new web. This included the Web-Jouornal [10] the support of robots and soon thereafter the early search engines. During WWWIII, in Darmstadt, the pioneers of the early search engines felt that to provide for the financial needs of the search engines, a side panel to display paid publicity would be appropriate. This way the paid publicity would be separated from the search results. This was the method used until a late search-engine arrival: initially, this new system was idealistic but soon became, under pressure from the venture capitalists, one of the leaders of the what has been termed the digital gangsters. All these systems are based on collecting huge amounts of personal information about the users, be it from free emails, or postings made on one of the online social networks (OSN)

References

[1] Aksoy, Ayberk, Desai, Bipin C., 2019. Heimdallr: A system design for the next generation of IoTs In Proceedings of International Conference on Industrial Control Network and System Engineering Research (ICNSER2019) ACM, New York, NY, USA, 10 pages https://doi.org/0.1145/3333581.3333590

[2] ACM, CE2016: Computer Engineering Curricula 2016, https://www.acm.org/binaries/content/assets/education/ce2016-final-report.pdf

[3] ACM, CS2013: Curriculum Guidelines for Undergraduate Programs in Computer Science, https://www.acm.org /binaries/content/assets/education/ cs2013_web_final.pdf

[4] ACM, Curricula Recommendation. https://www.acm.org/education/curricula-recommendations

[5] Arednt, Hannah, The Origin of Totalitarianism, Meridian Book, 1951, p 124

[6] BBC, Amazon, Apple and Google face data complaints, https://www.bbc.com/news/technology-46944694 last accessed May 6, 2019

[7] BBC, Google hit with €4.3bn Android fine from EU, Jul. 18 2018 https://www.bbc.com/news/technology-44858238 last accessed May 6, 2019

[8] AAI, America in the Age of Information, July 6-7, 1995, Lister Hill Center, Bethesda MD, http://users.encs.concordia.ca/ bcdesai/Age-of-Information-July-1995.pdf

[9] Desai, Bipin C., Pinkerton, Brian, Workshop A: Web−wide Indexing/Semantic Header or Cover Page, Summary, April 10, 1995, http://users.encs.concordia.ca/ bcdesai/web-publ/www3-wrkA/www3-wrkA-proc.pdf, also available from Spectrum Repository: https://spectrum.library.concordia.ca/985374/1/WWW-III-WrkShpA.pdf last accessed May 6, 2019

[10] Desai, Bipin C., Swiercz, Stan, WebJournal: Visualization of a Web Journey, June 1995, http://users.encs.concordia.ca/~bcdesai/web-publ/WebJournal.pdf, Last accessed, May 7, 2019

[11] Desai, Bipin C., IoT: Imminent ownership Threat. In Proc. of 21st International Database Application & Enginnerring Symosium, Bristol, UK, July 2017 (IDEAS 2017), 8 pages. https://doi.org/10.475/3105831.3105843

[12] BELL CANADA AND LYCOS ANNOUNCE JOINT VENTURE, Feb 2, 2000, http://www.bce.ca/news-and-media/releases/show/bell-canada-and-lycos-announce-joint-venture

[13] Bell, Emily Mark Zuckerberg's Facebook mission statements hide his real aim, The Guardian, Mar.10, 2019, https://www.theguardian.com/media/commentisfree/2019/mar/10/markzuckerberg-facebook-mission- statements-hides-his-real-aim

[14] Beckett, Samuel En attendant Godott, Les Èditions de Minuit, Paris, 1952

[15] CBC Radio Facebook has become one of world's 'most dangerous monopolies, https://www.cbc.ca/radio/thecurrent/the-current-for-may-10-2019-1.5129874/friday-may-10-2019-full-transcript-1.5131529

[16] Cadwalladr, Carole, My TED talk: how I took on the tech titans in their lair, Guardain, Apr. 21, 2019, https://www.theguardian.com/uk-news/2019/apr/21/carole-cadwalladr-ted-tech-google-facebook-zuckerberg-silicon-valle

[17] Cadwalladr, Carole, Campbell, Duncan Revealed: Facebook's global lobbying against data privacy laws, The Guardain, Mar. 2. 2019, https://www.theguardian.com/technology/2019/mar/02/

[18] Chisick, Chris Supreme Court of Canada Upholds BC Decision to Grant Worldwide De-Indexing Order Against Google, June 28, 2017 https://www.casselsbrock.com/CBNewsletter/Supreme_Court_of_Canada_Upholds_BC_Decision_to_Grant _Worldwide_De_Indexing_Order _Against_Google, https://www.canlii.org/en/ca/scc/doc/2017/2017scc34/2017scc34.html

[19] CIHI, Privacy and Security Risk Management Framework , h ttps://www.cihi.ca/en/about-cihi/privacy-and-security

[20] Confessore, Nicholas, Rosenberg, Matthew, Damage Control at Facebook: 6 Takeaways From The Times'sInvestigation, New York Times, Nov. 14, 2018, https://www.nytimes.com/2018/11/14/technology/ facebook-crisis-mark-zuckerberg-sheryl-sandberg.htm

[21] Cook, Tim, You Deserve Privacy Online. Here's How You Could Actually Get It, http://time.com/collection/davos-2019/5502591/tim-cook-data-privacy/

[22] Duffy, Andrew Trudeau and Liberals win majority in historic return to power Ottawa Citizen, Oct. 20, 2015 https://ottawacitizen.com/news/politics/justin-trudeau-and-liberals-stage-historic-return-to-power

[23] CBC, B.C. court approves class-action lawsuit against Facebook, May 30, 2014 https://www.cbc.ca/news/canada/british-columbia/facebook-class-action-lawsuit-launched-by-vancouver-woman-1.266046, Last accessed, May 6, 2019

[24] CBC, Facebook wins appeal to stop B.C. class-action lawsuit over privacy, Jun 19, 2015, https://www.cbc.ca/news/canada/british-columbia/facebook-wins-appeal-to-stop-b-c-class-action-lawsuit-over-privacy-1.3120849, Last accessed, May 6, 2019

[25] CTV, Supreme Court clears way to B.C. class-action against Facebook, June 23, 2017, https://www.ctvnews.ca/canada/supreme-court-clears-way-to-b-c-class-action-against-facebook-1.3473026, Last accessed, May 6, 2019

[26] Denham, Elizabeth, Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. Under the Personal Information Protection and Electronic Documents Act, PIPEDA Report of Findings #2009-008, July 16, 2009, https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2009/pipeda-2009-008/ Last accessed, April 18, 2019

[27] Dance, Gabriel J.X., et.al, As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants, NY Times, Dec. 18, 2018, https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html

[28] Gates, Dominic Flawed analysis, failed oversight: How Boeing, FAA certified the suspect 737 MAX flight control system Seattle Times, Mar. 17, 2019 https://www.seattletimes.com/business/boeing-aerospace/failed-certification- faa-missed-safety-issues-in-the-737-max-system-implicated-in-the-lion-air-crash/ Last accessed, May 19, 2019

[29] D'Onfro, Jillian, Google did not disclose security bug because it feared regulation, says report, CNBC, Oct 8 2018, https://www.cnbc.com/2018/10/08/google-reportedly-exposed-private-data-of-at-least-hundreds-of-thousands-of-plus-users.html

[30] Douthat Ross, The Only Answer Is Less Internet, New York Times, April 13, 2019. https://www.nytimes.com/2019/04/13/opinion/china-internet-privacy.html, Last accessed April 23, 2019

[31] Dent, Steve Report: Boeing's crucial 737 Max safety analysis was flawed EnGadget, Mar. 18, 2019 https://www.engadget.com/2019/03/18/boeing-737-max-faa-certification-flaws/ Last accessed April 23, 2019

[32] The Economist, The future of big tech Why big tech should fear Europe, The Economist, Mar 23rd 2019, https://www.economist.com/leaders/2019/03/23/why-big-tech-should-fear-europe

[33] Data Policy - Facebook, https://www.facebook.com/ about/privacy/update

[34] Terms of Service – Facebook, https://www.facebook.com/legal/terms/update

[35] Fleshman, Glenn, FTC Considers Record Fine for Facebook Over Violation of User Privacy Agreement It Made in 2012, Report Says, http://fortune.com/2019/01/18/facebook-privacy-ftc-record-fine-considered/

[36] Frenkel, Sheera, et. al. Delay, Deny and Deflect: How Facebook's Leaders Fought Through Crisis NY Times, Nov. 14, 2018, https://www.nytimes.com/2018/11/14/technology/facebook-data-russia-election-racism.html

[37] COPPA, Children's Online Privacy Protection Act, https://www.ftc.gov/enforcement/statutes/childrens-online-privacy-protection-act

[38] FTC, Privacy and Security, https://www.ftc.gov/tips-advice/business-center/privacy-and-security

[39] FTC, Careful Connections: Building Security in the Internet of Things, https://www.ftc.gov/tips-advice/business-center/guidance/careful-connections-building-security-internet-things

[40] Goodwin, Bill , et al., Facebook asked George Osborne to influence EU data protection law, Computer Weekly, Mar. 2, 2019, https://www.computerweekly.com/news/252458229/Facebook-asked-George-Osborne-to-influence-EU-data-protection-law

[41] GDPR, What is GDPR and how will it affect you?, https://www.theguardian.com/technology/2018/may/21/what-is-gdpr-and-how-will-it-affect-you

[42] GDPR, General Data Protection Regulation https://gdpr-info.eu/

[43] Graham-Harrison, Emma, Inside Facebook's war room: the battle to protect EU elections, Guardian, May 5, 2019, https://www.theguardian.com/technology/2019/may/05/facebook-admits-huge-scale-of-fake-news-and-election-interference

[44] Guruswamy, Menaka India's Supreme Court Expands Freedom NY Times, Sept. 10, 2017 https://www.nytimes.com/2017/09/10/opinion/indias-supreme-court-expands-freedom.html?

[45] Guliani, Neema Singh, W Should Be Able to Take Facebook to Court, NY Times, Jan.. 6, 2019, https://www.nytimes.com/2019/01/06/opinion/facebook-privacy-violation.html

[46] GPS, Global Positioning System History, https://www.nasa.gov/directorates/heo/scan/ communications/policy/GPS_History.html Last accessed Apr. 7, 2019

[47] Facebook uploaded email contacts of 1.5m users without consent, The Guardian, Apr. 18, 2019, https://www.theguardian.com/technology/2019/apr/18/facebook-uploaded-email-contacts-of-15m-users-without-consent

[48] Hughes, Chris It's Time to Break Up Facebook, NY Times. May 9, 2019, https://www.nytimes.com/2019/05/09/opinion/sunday/chris-hughes-facebook-zuckerberg.html

[49] Hart, David, On the Origins of Google:, August 17, 2004, https://www.nsf.gov/discoveries/disc_summ.jsp?cntn_id=100660

[50] Hem, Alex, Apple chief calls for laws to tackle 'shadow economy' of data firms, Jan. 17, 2019, https://www.theguardian.com/technology/2019/jan/17/apple-chief-tim-cook-calls-for-laws-to-tackle-shadow-economy-of-data-firms

[51] Huish, Robert, Balazo Patric, Unliked: How Facebook is playing a part in the Rohingya genocide, The Conversation, Jan. 2, 2018, https://theconversation.com/unliked-how-facebook-is-playing-a-part-in-the-rohingya-genocide-89523

[52] Insley, Jill FarmVille user runs up £900 debt The Guardian, Apr. 7, 2010 https://www.theguardian.com/money/2010/apr/07/farmville-user-debt-facebook

[53] Johnson, Bobby, Privacy no longer a social norm, says Facebook founder , The Guardian, Jan 11, 2010, https://www.theguardian.com/technology/2010/jan/11/facebook-privacy

[54] Jacobsson, Andreas; Davidsson, Paul, Towards a Model of Privacy and Security for Smart Homes. Proc.: 2015 IEEE 2nd World Forum on Internet of Things (WF-loT), p. 727-732 URL: https://doi.org/10.1109/WF-IoT.2015.7389144

[55] Jenkins, Simon, Facebook is out of control and politicians have no idea what to do The Guardian, Feb, 18, 2019, https://www.theguardian.com/commentisfree/2019/feb/18/facebook-powerful-politicians-commons-abuse

[56] Lycos, https://en.wikipedia.org/wiki/Lycos

[57] Manhire, Toby, New Zealand courst banned naming Grace Millane'e accused killer,. Google just emailed it out 13 Dec. 2018, https://www.theguardian.com/world/2018/dec/13/new-zealand-courts-banned-naming-grace-millanes-accused-killer-google-just-emailed-it-out

[58] Madrigal, Alexis C. , What We Know About Facebook's Latest Data Scandal, The Atlantic, June 4, 2018, https://www.theatlantic.com/technology/archive/2018/06/what-we-know-about-facebooks-latest-data-scandal/561992/

[59] Meyer, David, In the Wake of GDPR, Will the U.S. Embrace Data Privacy?, Fortune, Nov. 29. 2018, http://fortune.com/2018/11/29/federal-data-privacy-law/

[60] Morozov, Evgeny, It's not enough to break up Big Tech. We need to imagine a better alternative, Guardian, May 11, 2019 https://www.theguardian.com/commentisfree/2019/may/11/big-tech-progressive-vision-silicon-valley

[61] Mullin, Joe Privacy lawsuit over Gmail will move forward Aug. 16, 2016 https://arstechnica.com/tech-policy/2016/08/privacy-lawsuit-over-gmail-will-move-forward/

[62] King, Mark Parents told to beware children running up huge bills on iPad and iPhone game apps Guardian, Jan. 12, 2013 https://www.theguardian.com/technology/2013/jan/12/parents-children-in-app-purchases

[63] McLaren Leah Is Elizabeth Denham the Only Person Powerful Enough to Take on Facebook? The Walrus, Apr. 18, 2019 https://thewalrus.ca/is-elizabeth-denham-the-only-person-powerful-enough-to-take-on-facebook/

[64] Martin, Nicole Was The Facebook '10 Year Challenge' A Way To Mine Data For Facial Recognition AI?, Forbes, Jan. 17, 2019. https://www.forbes.com/sites/nicolemartin1/2019/01/17/was-the-facebook-10-year-challenge-a-way-to- mine-data-for-facial-recognition-ai#4b56c3fe5859

[65] The history of Mobile phones, https://en.wikipedia.org/wiki/History_of _mobile_phones, last accessed April, 2019

[66] McNamee, Roger I Mentored Mark Zuckerberg. I Loved Facebook. But I Can't Stay Silent About What's Happening, The Time, Jan ., 17, 2019, http://time.com/5505441/mark-zuckerberg-mentor-facebook-downfall/

[67] Millen, Sarah Gertrude, Rhodes, London, 1933, p. 138.

[68] Nancherla, Aparna, Lee, Christopher, The Infinite Scroll, New York Times, April 13, 2019, https://www.nytimes.com/2019/04/13/opinion/sunday/the-infinite-scroll.html,

[69] Privacy Commissioner launches Facebook investigation. March 20, 2018, https://www.priv.gc.ca/en/ opc-news/news-and-announcements/2018/nr-c_180320/

[70] OSN, Why the UK is taking on social networks over child safety, https://www.theguardian.com/technology/2019/feb/06/why-uk-is-taking-on-social-networks-child-safety, Last accessed April 16, 2019

[71] Le NPD réclame à la commissaire au lobbying une enquête sur Facebook, La Presse, Mar. 4, 2019, https://www.lapresse.ca/actualites/politique/politique-canadienne/201903/04/01-5216953-le-npd-reclame-a-la-commissaire-au-lobbying-une-enquete-sur-facebook.php

[72] Pegg, David, Facebook labelled 'digital gangsters' by report on fake news, Guardian, Feb. 18, 2019, https://www.theguardian.com/technology/2019/feb/18/facebook-fake-news-investigation-report-regulation-privacy-law-dcms

[73] Joint investigation of Facebook, Inc. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia PIPEDA Report of Findings #2019-002, April 25, 2019 https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-002/ Last accessed April 30, 2019

[74] Paul, Kari, Facebook security lapse affects millions more Instagram users than first stated. Guardian, April 18, 2019, https://www.theguardian.com/technology/2019/apr/18/instagram-facebook-password-lapse-privacy-breach-data-exposed- Last accessed, April 18, 2019

[75] Price, Emily, France Fines Google $57 Million For GDPR Violation, Jan. 21 2019, http://fortune.com/2019/01/21/france-fines-google-57-million-for-gdpr-violations/

[76] Privacy Shield, Key New Requirements for Participating Companies, Informing individuals about data processing, https://www.privacyshield.gov/Key-New-Requirements

[77] Privacy Shield, https://www.privacyshield.gov/Program-Overview

[78] WWW1 First International Conference on the World-Wide Web, https://en.wikipedia.org/wiki/First_International _Conference_on_the_World-Wide_Web

[79] Rushe, Dominic Google: don't expect privacy when sending to Gmail Teh Guardian, Aug 15, 2013 https://www.theguardian.com/technology/2013/aug/14/google-gmail-users-privacy-email-lawsuit

[80] Ressa Maria, Facebook Let My Government Target Me. Here's Why I Still Work With Them, The Time, Jan. 17, 2019, http://time.com/5505458/facebook-maria-ressa-philippines/

[81] Ryan, Marc, Warzel, Charlie, Kantrowitz. Alex, Growth At Any Cost: Top Facebook Executive Defended Data Collection In 2016 Memo — And Warned That Facebook Could Get People Killed, Buzzfeed, March 29, 2018, https://www.buzzfeednews.com/article/ryanmac/growth-at-any-cost-top-facebook-executive-defended-data, Last accessed April 12, 2019

[82] Srnicek, Nick. The only way to rein in big tech is to treat them as a public service, The Guardian, Apr 23, 2019, https://www.theguardian.com/commentisfree/2019/apr/23/big-tech-google-facebook-unions-public-ownership

[83] Stueck, Wendy, Former information commissioner Elizabeth Denham was one of first to raise concerns over Facebook data, Globe and Mail, March 25, 2018, https://www.theglobeandmail.com/canada/british-columbia/article-former-information-commissioner-elizabeth-denham-was-one-of-first-to

[84] Turow, Joseph, Let's Retire the Phrase 'Privacy Policy', New York Times, Aug. 20, 2018. https://www.nytimes.com/2018/08/20/opinion/20Turow.html

[85] Turow, Joseph, Google Still Doesn't Care About Your Privacy Fortune, June 28, 2017 http://fortune.com/2017/06/28/gmail-google-account-ads-privacy-concerns-home-settings-policy/

[86] Tiktok: India bans video sharing app, https://www.theguardian.com/world/2019/apr/17/tiktok-india-bans-video-sharing-app, Last accessed April 16, 2019

[87] TikTok video-sharing app fined for collection of children's data , The Guardian, Feb. 28, 2019 https://www.theguardian.com/technology/2019/feb/28/ tiktok-video-sharing-app-fined-for-collection-of-childrens-data, Last accessed April 16, 2019

[88] Tufekci, Zeynep, Zuckerberg's So-Called Shift Toward Privacy, NY Times, Mar. 7, 2019, https://www.nytimes.com/2019/03/07/opinion/ zuckerberg-privacy-facebook.html

[89] Disinformation and 'fake news': Final Report, Digital, Culture, Media and Sport select committee, Feb, 2019, https://publications.parliament.uk/pa/cm201719/cmselect/ cmcumeds/1791/179102.htm

[90] von Scheel, Elise, Facebook pressured Canada to ease up on data rules, U.K. reports say, CBC News, Mar 03, 2019, https://www.cbc.ca/news/politics/facebook-canada-data-pressure-1.5041063

[91] Valentino-de Vries, Jennifer, Tacking Phones, Google Is a Dragnet for the Police, NY Times, April 4, 2019, https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html

[92] Vaidhyanathan, Siva Facebook's new move isn't about privacy. It's about domination, Guardain, Mar. 7, 2019, https://www.theguardian.com/commentisfree/2019/mar/07/ facebook-privacy-domination

[93] Warzel, Charlie, Thompson, Stuart A. Tech Companies Say They Care, NT Times April 10, 2019, https://www.nytimes.com/interactive/2019/04/10/opinion/tech-companies-privacy.html, Last accessed April 17. 2019

[94] Waterson, Jim, Obscure pro-Brexit group spends tens of thousands on Facebook ads, Guardain, Jan. 14, 2019, https://www.theguardian.com/politics/2019/jan/14/obscure-pro-brexit-group- britains-future-spends-tens-of-thousands-on-facebook-ads

[95] Waters, Richard, Murphy, Hannah, Stacey, Kiran, Social Media's Reckoning?, Financial Times, April, 13-14, 2019, p6

[96] Wu, Tim, How Capitalism Betrayed Privacy, NY Times, April 10, 2019 https://www.nytimes.com/2019/04/10/opinion/sunday/privacy-capitalism.html

[97] Weinberg, Zoe A. Y. Google Settles Buzz Lawsuit The Harvard Crimson, Sep. 7, 2010 https://www.thecrimson.com/article/2010/9/7/google-mason-privacy-settlement/

[98] Yglesias Matthew The push to break up Big Tech, explained Vox, May 3, 2019 https://www.vox.com/recode/2019/5/3/18520703/big-tech-break- up-explained

[99] Zuboff, Shoshana, The Age of Surveillance Capitalism, Jan, 2019, pp179, ISBN 97801-61039-564-4