2019 IEEE International Symposium on Technology in Society (ISTAS) Proceedings
Miriam Cunningham and Paul Cunningham (Eds)
ISBN: 978-1-7281-5480-0

Privacy, Data Rights and Cybersecurity

Technology for Good in the Achievement of Sustainable Development Goals

Katina Michael [1], Shannon Kobran [2], Roba Abbas [3], Salah Hamdoun [1]
[1] School for the Future of Innovation in Society & Computing, Informatics and Decision Systems Engineering, Arizona State University, Tempe, United States, email: katina.michael@asu.edu, shamdoun@asu.edu
[2] SDG Academy, Sustainable Development Solutions Network, New York, United States, email: shannon.kobran@unsdsn.org
[3]School of Management, Operations and Marketing, Faculty of Business, University of Wollongong, Wollongong, Australia, email: roba@uow.edu.au

***Abstract*— When technology is used for good in addressing sustainable development goals, fundamental human rights are adhered to. In the context of technology, we can discuss privacy, data rights and cybersecurity as three areas that are integral in maintaining the freedom and dignity of the individual. In a rush to bring developing nations on par with developed nations, the rapid deployment of technology is often seen as the answer to the achievement of all 17 sustainable development goals. We have seen, for example, biometric systems deployed in India through the Aadhaar biometric ID system versus the adoption of basic mobile technologies in Africa, providing e-payment capabilities. How can we know whether the deployment of new technology will help or inhibit the liberation of peoples, for example, to conduct mobile commerce? This paper emphasizes the need for three ethical elements- privacy, data rights and cybersecurity- in the deployment of new technologies and provides examples throughout history that demonstrate positive or negative applications of technology.**

Keywords*— privacy, data rights, cybersecurity, sustainable development goals, technology, ethics, values

I. Introduction

Technology can be an enabler, an implementer, a means of "achieving innovation, business opportunities and development, trade of environmental goods and services, finance and investment, and institutional capabilities" [1]. It is a holistic mechanism, that provides a means for realizing all the Sustainable Development Goals (SDG) set out by the United Nations (UN). However, technology is often hindered by external factors in facilitation and transference. On the one hand, technology is an enabler if used appropriately, and on the other hand, it may well be perceived as an oppressive instrument if used subversively to topple human rights [2]. It is in this context where *The Means of Implementation of the Post-2015 Development Agenda* and the *Addis Ababa Action Agenda* become vitally important.

Technologies are not neutral; they come laden with inherent values and features. The very same technology can be used to segregate or bring together. We have seen examples throughout history of positive and negative social impacts of technology. While each context is different, peoples have suffered and remain marginalized as a result of deliberate system design meant to oppress (e.g. [3]) or systems designed to liberate (e.g. open access). Without the appropriate conditions, technologies can fail in their execution because they do not adequately protect the citizen from misuse, abuse, manipulation, or misapplication by those in power [4]. The design of adequate technology policies will enable institutions to function and serve communities more effectively and permit stable and secure online and offline infrastructures that can attract adequate investments as risks are mitigated. In order to avoid some of these risks presented particularly by complex technologies, it is crucial to understand what privacy, data rights, and security mean in the context of *technology for good*. Often this can be conveyed by presenting what has been demonstrated in the past to be poor practice, or even in some rarer cases, malicious practice. We acknowledge, that the achievement of the Sustainable Development Goals hinges on a positive role of technology. And here, we can relate the SDGs as being inexorably linked to the emergent concept of *public interest technology* [5]. Adequate designs will, therefore, allow for policies that protect humans, improve economic prosperity, and consider the common good. Our hope in this paper is to begin to highlight representative sustainable development goals and targets that require technological intervention, and to demonstrate the importance of technology policy that will see privacy, data rights and cybersecurity embedded in the design process [6].

The IEEEXplore database was searched for the term "Sustainable Development Goals" and 102 individual papers were returned, including 87 conference papers, 10 magazine articles, and 5 journal papers. A high-level paper title analysis demonstrated that a large proportion of the papers were concerned with: the role of geographic information systems datasets; open data; energy systems; learning environments; supply chains; and advanced information technologies and systems, such as the internet of things (IOT), big data, artificial intelligence (AI), and virtual and augmented reality. The papers were situated primarily in a developing nations context, in Africa and the Asia Pacific, and did not address the significant considerations of privacy, data rights, or cybersecurity as integral design features of technology deployments for achieving SDGs.

This paper is broken down into three sections, privacy, data rights, and cybersecurity, to demonstrate the importance of each in sustainable user-centered solutions. Each section will provide an elaboration of the concept and present examples that are centered around communities, institutions and agencies of large-scale ICT deployments affecting citizenry. These three sections will provide insights into possible social implications of technology, that will be deliberated briefly in the discussion section, in the context of future research on the achievement of sustainable development goals and targets.

II. Privacy

This section will focus on the role of privacy concerning Information and Communication Technology (ICT) and the Sustainable Development Goals and emphasize why establishing trust between stakeholders, particularly between governments and citizens, is a critical aspect of any ICT intervention.

A. History of the Right to Privacy

In July 2015, the UN Human Rights Council appointed its first Special Rapporteur on the Right to Privacy [7]. The motivation for doing so, were issues pertaining to security and surveillance, big data and open data, health data, and personal data processed by private corporations. The focus was really on the efficacy and proportionality of intrusive measures made possible by advances in ICT. As governments across the world undergo digital transformation, privacy issues abound in the secure storage and secure communication of citizen's personal information. Consider this in the context of Sustainable Development Goal 3 "Ensure healthy lives and promote well-being for all at all ages." Whether sensitive information pertains to one's health status, criminal records, race or religious affiliation, or home address, citizens expect privacy [8]. However, before the discussion about the right to privacy, as it relates to the digital age, understanding history related to this right as an issue of international concern is essential. Article 12 of the Universal Declaration of Human Rights [9] identifies the right to privacy as a key principle that ensures freedom. It states: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation."

The Universal Declaration of Human Rights was established in 1948 after universal crimes were committed by the Nazis in World War II and evidenced during the Nuremberg International Military Tribunal. The Reich Government kept copious and meticulous hand-written records on a variety of minority groups who were discriminated against based on race, religion, sexual orientation, mental health, and more. Although computing power was then in its nascent stage relying greatly on the tabulation of punch cards, it was later discovered that the Hollerith machine was used by the Nazis to process census information [10]. This process facilitated the identification of individuals who were later sent to the concentration camps and gas chambers, or at the very least, made to wear specific badges identifying them as belonging to a particular group of people. This demand for individuals to wear identification badges sewn onto their clothing- or even have numbers branded onto their forearm- had nothing to do with identity and everything to do with dehumanization.

This narrative is a bleak way to start a discussion of the right to privacy, but it is important to establish why privacy was included in the Universal Declaration of Human Rights after people's personal identifying information was used against them. On the other hand, if we are to examine other acts of dehumanization that have taken place in the 20th and 21st centuries, they often begin with the removal of nationally-recognized identification documents, such as passports [11]. Governments can deny the rights of people in the absence of documented identity, as individuals are unable to provide evidence of citizenship. This can strip whole communities from any agency. At times these individuals can be considered refugees, forced to leave their country in order to escape persecution or war.

B. Privacy in the Digital Age

Privacy, as defined in 1948, was the right to be left alone. However, classical definitions of privacy do not account for the complexities associated with advanced technologies. As ICTs began to permeate government and business, information privacy came to refer to the interest an individual has in controlling, or at least significantly influencing, the way data about themselves is handled and used [12]. This might include sensitive information like: name, date of birth, age, sex, and address; current contact details of family and guardians; bank details; medical records; personal care issues; service records and file progress notes; individual personal plans, assessments or reports; guardianship orders; or even personal correspondence. Other information considered confidential includes ethnic or racial origin, political opinions, religious or philosophical beliefs, health, or sexual lifestyle should also be considered confidential, as it could be used against individuals [13]. But beyond privacy being a personal, individual interest alone, it is now more than ever a collective interest. For example, we see the potential for facial recognition systems, coupled with machine learning to encroach on the rights and freedoms of minority groups.

In an age of mobile devices, social media, and online platforms that consistently leave behind digital footprints, it appears difficult to maintain privacy [14]. This is a particularly important issue when websites do not disclose whether or not they are sharing information with third parties. Default sharing settings or unclear terms and conditions can place individuals at risk of disclosing private information that they may prefer to be confidential. First of all, it is essential to know who holds the consumer's information. Most governments store electronic records on their citizens- things such as tax records, electronic health records, even student identification records. The open data movement, which advocates for the free flow of data, sees value in making available data that has been funded by taxpayers so it can contribute to the public good. Governments are considering opening up some of this data so that it may be accessed by third parties who wish to create innovative services using de-identified information. Deidentification aims to allow data to be used by others without the possibility of ascertaining the identity of individuals.

Consumer data rights - the idea that a consumer should control the collected data - are supposed to change the potential for individuals to have their data locked to a legacy or incumbent provider [15]. The consumer data right will improve consumers' ability to compare and switch between products and services. These rights, in theory, offer individuals data portability between stakeholders of choice- for example, service providers such as energy or electric companies. In the context of the banking sector, the notion of an open banking framework has emerged, so that consumers will be able to access and safely transfer their banking data to trusted parties [16]. Open banking initiatives might include spending information, including deposit and credit account transactions.

Some NGOs are suspicious of the consumer data rights movement, claiming that these rights could be used to manipulate consumers [17]. Energy companies, for example, can monitor household activity by determining the types of household appliances in use, time of day data, for instance when someone is not at home or when someone chooses to sleep or rise. This behavioral analysis can develop further when information about consumers is available publicly online, and big data analytics can draw from these various sources to make inferences about an individual's pattern of life [18]. This process is known as predictive profiling and may be used to on-sell more products [19]. On the other hand, this is the first time in history that we can gather and share information so quickly and, in such quantities, and it can undoubtedly be used for good. By harnessing the power of ICT, by crowdsourcing information from stakeholders around the world and gathering data from sensors embedded in smart devices, collective awareness can be used to improve people's lives and achieve sustainable development [20].

So, what is the bottom line? Your data is inevitably going to be collected by someone- the question is, do you trust that your data will be used *for* you and not *against* you by government agencies and private corporations or by hackers? In this age of data-driven decision-making, trust is just as important- maybe even more important- than privacy. You may be willing to give up control of your private data if you trust the person you are giving control to. Illustrating this point further; privacy requires security, and security enhances control. However, more control can serve to decrease trust in a provider, and having less trust can augment our privacy requirements [21]. It is possible to keep going around and around this cycle without reaching a point of harmony, but the aim is to strike an optimal point where all constituents are willing to form a social contract, setting out their expectations.

1) Case Example: My Health Record in Australia

Without trust, explicit consent, transparency, and accountability, even the most innovative ICT intervention will run into severe problems upon implementation. For example, in 2018 Australia decided to officially roll out an electronic health record scheme by automatically enrolling every Australian into the program. The government stored these health records in a centralized location, amplifying the risk of a single "big hack" by anyone wishing to have access to a rich honeypot of personal and sensitive information. The "My Health Record" system stores information about individual Australians' allergies, medical conditions, medications, test results, and anything else that is uploaded by a doctor. This information will be shared between medical providers, improving the efficiency of the healthcare system but it could also be used by law enforcement without a warrant.

Under section 70 of the My Health Records Act 2012, the Australian Digital Health Agency (ADHA) can disclose health information when it "reasonably believes" it is necessary to investigate or prosecute a crime, to counter "seriously improper conduct" or to "protect the public revenue". Moreover, if the information gets hacked, it puts vulnerable communities at risk of being discriminated against if the information becomes public – communities like HIV-positive people and people living with mental health conditions. It also is possible that such private health data could be linked with census data and other big data, which puts people's privacy at risk. Many people do not trust the Australian government to keep this information safe, given their track record [22], and as a result, civil society organizations are urging individuals to opt out if they have a criminal record or are a public figure; if they have lived with mental health issues, or if they have been or presently are a sex worker, have a lifelong transmissible condition or terminated a pregnancy prematurely [23]. More than 2.5 million Australians, incidentally opted out of the My Health Record [24].

Security breaches that occur from within governments, such as insider attacks by employees, or outside attacks, will have devastating impacts on people. Problems exist when there are weak privacy laws and controls in place. For instance, in February 2018, a notifiable data breach prompted a now mandatory requirement for various entities to report breaches of privacy [25]. However, at the same time, Australia does not make it possible for individuals to sue for damages as it does not have a common law tort for invasion of privacy. If a company with an annual turnover of more than AU$3 million fails to file a report, a maximum civil fine of $2.1 million to businesses or $420,000 to individuals is handed down. The flow-on effect of non-disclosure for a company is a significant loss of reputation. Even a leading state in cybersecurity, like Singapore, can have their systems penetrated. In July 2018, Singapore had to disconnect computers at public healthcare centers from the Internet after hackers compromised more than 1.5 million SingHealth patients' personal information [26].

Cyberattacks on national identity systems will become commonplace as more credentials are gathered and stored online [27]. If the citizen profiles make it onto the dark web, the implications of adopting emerging technologies before they have been tried and tested on large-scale populations will become apparent, and there will be significant backlash from citizens. The dark web refers to encrypted online content that is not indexed on conventional search engines. It is additionally part of the 'deep web', a more extensive collection of content that does not appear through regular internet browsing.

C. Privacy and Security By Design

The choice may be the adoption of new technologies to justly transform practices and reap the benefits of all this data or hang on to traditional systems that have known vulnerabilities and limitations and learn to live with them. Perhaps what is of the highest importance is to treat privacy and security as functional aspects of any new system. All too often, engineers do not incorporate privacy and security by design for a product that will affect hundreds of millions of people. The long-standing myths are that we need to give up our privacy for public safety; and that we need to sacrifice privacy for data analytics [28]. Function creep in services are also a concern, such as when tax file numbers become de facto national ID numbers, or biometric rollout systems are used retrospectively for unrelated aims [29]. Function creep is the gradual widening of the use of a technology or system beyond the purpose for which it was initially intended. "After the fact" privacy intrusions do not grant citizens an opportunity to consent to the mass-scale changes. Instead, they are imposed on them without a consultation process, and at times covertly.

The information gathered, whether through public or private means, has the potential to be used for good or ill, depending on the stakeholder and their motivation/agenda. However, we cannot deal in "what-ifs" if we are to adhere to the ethical principles of the Universal Declaration of Human Rights. At present, our laws are not keeping pace with information technology, so what may be considered *legal* might well be *unethical*. We are also witnessing transformative changes in state-society relations in many countries. Globalization and the associated range of economic, technological, social, and political developments have supported the rise of individualism, resulting in a shift from thinking in terms of the "public good." The 2015 Edelman Trust Barometer points to an "evaporation of trust" in institutions and leaders worldwide, inclusive of NGOs [30]. The annual survey finds a decline in trust overall, with more countries classified as distrusting than trusting. Globally, trust in business, media, and NGOs is at its lowest level since the 2008 financial crisis. What do we have to do to turn this around, especially if we are to achieve the sustainable development goals and targets? Governments need to lead open and transparent debate with all communities, about policy challenges and options. Expertise comes in many forms – technical, political, professional, and user expertise. All need to be included in policy debates, particularly in an era of budget constraint. Transparent accountability relationships are essential to secure public trust in the policy process. This suggests building accountability into the lifecycle of commissioning.

Thus, to summarize: in this section, we have reviewed concepts related to privacy in the context of human rights and the emergence of new ICT technologies and systems. Privacy should be considered in the design and implementation of any ICT system, particularly on large-scale government ICT projects rolled out to citizens. Greater emphasis needs to be placed on engaging civil society in order to develop ICT programs that are robust and trustworthy. This is the only way that the SDG targets will be achieved by 2030, if citizens are given a voice to participate in solutions building to meet their community's needs, and have control over their own data sets and future. No system is impenetrable, but we can reduce end-user vulnerability by working together to understand the social implications of technology better, being aware of the risks, and planning as much as possible to ensure that ICT works *for* us, and not against us.

III. Data Rights

This section will focus on data rights and the role of government in ensuring those rights. Statutory data rights, where they exist, require businesses to comply with laws to protect and empower consumers.

A. What are Data Rights?

Data rights are a question of *who* owns- and therefore has control over- certain types of information. They tend to fall into three categories:

- Government Data Rights,
- Business Data Rights, and
- Consumer Data Rights

In a government context, a "data right" is a way to refer to a government's right to use valuable intellectual property, such as software or certain types of technical or scientific data [31]. With respect to the business context, "data rights" generally refer to intellectual property, in addition to patents that are territorial, granted at the national or regional level. However, what is most germane to our discussion of data and sustainable development, is consumer data rights- that is, an individual's right to own and control the data collected about them, especially by businesses. Since data is such a valuable commodity- it fuels research, innovation, and other public service or private business needs- it makes sense that individuals should have a say in how their data is utilized and who profits from it.

For instance, consumers that upload data onto websites or social media platforms are often not aware of the default privacy settings or terms and conditions. Most people assume that data voluntarily submitted to the website is kept secure and is not shared with third parties or made publicly available, and yet this is *not* always true. Accordingly, large ICT companies and vendors have amassed personal information from subscribers from across the globe. To illustrate this, Facebook had approximately 2.23 billion active monthly users as of June 2018 and specializes in data collection and mining. Imagine a subscriber base on a social media platform that is twice China's population, and the corresponding datasets it stores and shares of text, image and multimedia messages and objects.

Since about 2006, people who have used a variety of online ICT platforms have demanded access to the data stored on them. Initially, big ICT firms (e.g. Google) hired paralegals to deal with these ad-hoc requests by consumers and organized customized data searches on their behalf. The issue first arose from the desire of individuals to "determine the development of their life autonomously, without being perpetually or periodically stigmatized as a consequence of a specific action performed in the past" [32]. This right later became known as the *right to be forgotten*, prevalent in the European Union. Importantly, some social media providers, like Facebook, now offer consumers a one-click option to download their archive of information if they want to see what Facebook knows, or if they want to leave the social network and take their history with them. As such, social media platforms have become a one-stop shop for intelligence-gathering for law enforcement. Certain telecommunications metadata laws also allow authorities access to content that a user has been looking at online via their Internet Service Provider (ISP). Many police officers consider this as the "cheapest investigative tool."

These trends in policing and data investigation are set to get even more pervasive as new technologies like Apple's Siri, Amazon Alexa, and other types of voice-recognition devices are capturing private conversations, converting these conversations into data, and storing the data in the cloud- ripe for big data analytics. This is particularly problematic given that organizations such as Amazon are looking to capture data before a 'wake word', which adds to the dangers in this context [33]. Location-based data, coupled with human condition data is a new form of data, that can be gathered near real-time or retrospectively to track and monitor individuals [34]. This kind of data can come from contactless public transport cards, GPS sensors embedded in smartphones, from fitness trackers worn on the body, and even from heart pacemakers. We also have CCTVs, and video cameras that are body worn by police officers (e.g. AXON) that are supposed to make people safer [14]. Citizens are becoming increasingly aware of potential data sharing with third parties, and the necessity to keep their data safe and secure.

B. Biometric and Biological Data Collection

The range of data that is being collected and stored is not limited to a consumer's online search history. The collection of biometrics, especially facial images and fingerprints, has become a common practice. It is conceivable that people's authenticated digital image will one day be stored on a smartphone rather than on a government ID card and that this, along with biometric data, will be how to authenticate individuals in everyday interactions. Authentication is the process or action of verifying the identity of a user, something that becomes vitally important in countries with significant population sizes trying to attain the Sustainable Development Goals. The very right to vote is a current topic of interest in many parts of Africa. Also, data innovation driven by government open data initiatives in the form of new services will drive growth in the future. However, this type of governance requires that stakeholders assume commensurate responsibility in addressing big data management issues.

1) Case Example: Citizenry DNA Collection by the State

To that extent, it is essential to discuss what the responsibilities and social implications are of the use of our DNA as a data source, arguably the most personal information. In the case of S and Marper v. the United Kingdom [2008], the European Court of Human Rights determined that holding DNA profiles or samples of arrested individuals that were later acquitted or discharged, is a violation of the right to privacy under the European Convention on Human Rights [35]. The collection, storage, and retention of DNA profiles and DNA cellular samples as well as biometrics, in general, remain to be ill-defined in many countries. A comprehensive and consumer-focused policy regarding this subject could incorporate the right for citizens to provide consent to the storage and use of their DNA profile and in addition to that include a periodical review, given the nature of DNA. The necessity to develop policies that guard citizens from misuse is also due to the commercialization of DNA data.

Companies such as 23andMe, AncestryDNA, Family Tree DNA, tellmeGen and Living DNA, collect DNA samples in exchange for a report of family genealogy and for example, their proneness to specific genetic diseases. Customers provide this DNA information voluntarily, but may not be aware that their DNA is then kept and stored by the DNA data processor. To illustrate, the economic value of DNA data, 23andMe, a company closely linked to Google, closed a cooperation deal worth $300 million in July 2018 with the pharmaceutical giant GlaxoSmithKline [36]. Commerce of this kind will further inform the trajectory of DNA data processing firms and therefore stretch the citizen's capacity to protect their data. Privacy is allegedly protected based on consent and data aggregation. For instance, 23andme claims "we will not share your individual-level information with any third party without your explicit consent" and tells consumers that "[they] choose how [their] genetic information is used and shared with others.” 23andme “tells [customers] how those choices are implemented and how [they] collect, use, and disclose [their] information” [37]. Such wordsmithing is not only smart, but it also discourages consumer awareness of the potential consequences, as related for instance to insurability.

The SANS Institute [38] defines a policy as a document that outlines specific requirements or rules that must be met. A privacy policy contains information about the collection of personal information, how that personal information may be used, and enforcement for deliberately being in breach of someone’s privacy. However, many of the privacy policies that consumers sign- often without even reading what they agree to- have provisions that allow companies to share customers’ data with third parties, including marketing companies whose primary business driver is the liquidity of data. Ultimately, this means that the owners of this data are the companies or organizations that collect it, not the people who supply it.

C. *Regulatory Landscape*

Governments, civil society organizations, technology companies, and multi-stakeholder partnerships around the world come together to expand individuals’ data rights. Such a movement requires a socio-technical-legal approach, as there is an acknowledgement that humans interact with technology in a variety of intended and unintended ways. And governments have a particularly important role to play in fair and accessible legislative processes. For instance, in Australia, the government initiates a public consultation process when new legislation is to be introduced [39]. This process allows for civil society to participate and share valuable knowledge that is used to assess the viability of a proposed change. When new legislation relates to issues of privacy and data rights, the Australian Privacy Foundation, among other NGOs, plays an essential role in presenting evidence to relevant Senate hearings and privacy impact assessment submissions for consideration by government. The state has a responsibility for protecting data, transparency, and accountability, in the face of corporations who intend to use data to enhance innovation and develop their businesses.

The Facebook-Cambridge Analytica scandal from 2016 to 2018 demonstrated the importance of laws that protect consumers from the misuse of their data and breach of their privacy. Alongside the now defunct London-based elections consultancy company Cambridge Analytica, Facebook became embroiled in a dispute over the alleged harvesting and use of personal data residing on their platform. The allegations have heightened concerns over whether such data was then used to try and influence the outcome of the 2016 U.S. presidential election and the Brexit vote through a process of social media microtargeting campaigns [40]. Additionally, Facebook used very vague language in its privacy policy, misleading consumers about their data-sharing practices. Cambridge Analytica had found a way through defenses to acquire more data than just that of a survey respondent using the Facebook platform. The result was a consumer backlash, as people deleted their Facebook accounts. In July 2018, in a single day of trading, Facebook shareholders wiped more than $130 billion off the company's market value. In 2019 Facebook paid 7% of its $69B dollar expected earnings in fines [41].

1) The General Data Protection Regulation

As the scandal played out in the media, the European Union officially published the General Data Protection Regulation (known by its acronym GDPR), and it came into force in May 2018 [42]. The GDPR has overhauled how businesses process and handle consumer data. The legislation is designed to "harmonize" data privacy laws across Europe as well as give greater protection and rights to individuals. In the full text of the GDPR, 99 articles set out the rights of individuals and obligations placed on organizations covered by the regulation. There are eight rights for individuals. These include granting people easier access to the data companies hold about them, and a new fines regime and a clear responsibility for organizations to obtain the consent of individuals from whom they collect data. In short, it is a set of rules that give users greater control over their online personal data. Businesses operating in the E.U. are now required to obtain consent to allow for the use of consumer data.

Companies covered by the GDPR are accountable for their handling of people's personal information. This can encompass data protection policies, data protection impact assessments, and relevant documents detailing how data is processed. A large part of this regulation for businesses is proving compliance. In recent years, there have been a score of massive data breaches, including hundreds of millions of Yahoo, Sony, LinkedIn, eBay, and Equifax account details. Under GDPR, the "destruction, loss, alteration, unauthorized disclosure of, or access to" people's data has to be reported to a country's data protection regulator where it could have a detrimental impact on those individuals that are impacted. This can include but is not limited to, financial loss, confidentiality breaches, damage to reputation and more. The Information Commissioner Office must be informed of a breach 72 hours after an organization becomes aware of it, and furthermore the people it impacts must be notified.

For companies that have more than 250 employees, there is a need to maintain documentation detailing why people's information is being collected and processed, descriptions of the information that is held, how long it is kept for, and descriptions of technical security measures in place. Additionally, companies that have "regular and systematic monitoring" of individuals at a large scale or process a lot of sensitive personal data have to employ a data protection officer (DPO). For many organizations covered by GDPR, this may mean having to hire a new member of staff– although larger businesses and public authorities may already have individuals in this role. The DPO is required to report to senior members of staff, monitor compliance with GDPR, and be a point of contact for employees and customers.

There is also a requirement for businesses to obtain consent to process data in some situations. For instance, when an organization is relying on consent to use a person's data lawfully, it must explain that consent has been requested and provided. In addition to that, there has to be a "positive opt-in." When Facebook was under siege in April 2018, not only were they facing the allegations of the Cambridge Analytica scandal but, in preparation for the enactment of the GDPR in the same month, they moved 1.5 billion users out of reach of the new European privacy law relocating servers from Ireland to the U.S. where privacy laws are less strict. However, Facebook is not alone, as other ICT giants have purportedly done the same [43], [44]. How can we hope to achieve the SDGs using technology if we are constantly evading privacy regulations, there to protect the individual citizen? How will we achieve SDGs as a conscious community if our company practices are about evasion, rather than seeking to go beyond mere compliance, to active accordance.

Prior to the GDPR, privacy was operating under a 1995 EU Data Protection Directive. With the enactment of the GDPR the following rights for individuals were identified:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights concerning automated decision making and profiling.

Organizations will have to ensure that they have appropriate security measures in place to protect the personal data they hold on their customers.

2) *Frameworks for Ethical Data Collection*

High-level initiatives like the GDPR constitute a significant step in the right direction when it comes to recognizing and protecting people’s right to control their data. However, in an age when private companies have more data than government agencies, companies will need to lead the way in reforming business practices and restoring consumer trust. For transnational firms, especially, the GDPR might be complex to implement and will most definitely require a GDPR compliance team, usually within a broader policy group. Firms have begun by conducting a company-wide audit, documenting and publishing their transparency and disclosure of data practices, monitoring continuously, and restricting access where necessary to sensitive information.

Data Right campaigners such as the U.K’s Chartered Institute of Marketing are urging organizations to take action on the issue of responsible management of customer data. They are asking organizations to make a pledge to do four things:

- Be clear
- Show the benefits to consumers
- Show respect to customers
- Be in the know

The Chartered Institute of Marketing claims that 67% of consumers would share more personal information if organizations were more open about how they will use it [45]. By demonstrating that a business is open, honest, and championing best practices, organizations can show their customers the value-add of sharing their data in delivering a more personalized experience. The most crucial stakeholder in all of this, is the consumer, citizen, i.e., the individual, and a key consideration is consumer education. Children should learn about what happens when they go online or interact with a mobile device, how to interpret user agreements and detect websites that do not value privacy, how to avoid cyber-attacks, and so much more. Youth should be taught about protecting their personal information, and about what they can do if they suspect that their privacy and data rights have been violated. This is the road to empowerment.

People should also be aware of and advocate for the right to be forgotten- to eliminate the digital footprint they leave behind so that what they do online does not perpetually influence their lives or the lives of their families. Here, too, the European Union is leading the way, issuing penalties to any company that does not comply with the GDPR. The GDPR states smaller offenses could result in fines of up to €10 million or two percent of a firm's global turnover (whichever is greater). Those with more severe consequences can have fines of up to €20 million or four percent of a firm's global turnover (whichever is greater). People have a right to determine the development of their lives in an autonomous way, without being permanently or periodically stigmatized as a consequence of a specific action performed in the past. The Federal Trade Commission’s (FTC) fine to Facebook of $5B was 200 times larger than any previous fine handed down by them to any corporation [46], signifying the increasing importance of corporate responsibility with respect to technology’s impact on citizens.

Given that data can be used to support or inform any of the Sustainable Development Goals, privacy, and data rights underscore all of them. However, essential targets related to this matter are described in SDG 16, which promotes justice and strong, ethical institutions; and SDG 17, which stresses the importance of partnership and cooperation in achieving sustainable development. Fundamentally, we need stakeholders to come together to protect individuals’ data rights and create new standards, industry guidelines, laws, and even privacy-enhancing technology.

The U.S. Department of Homeland Security’s MENLO report, which was released in 2012, proposes a framework for ethical guidelines for computer and information security research [47]. This proposal was based upon the need to help clarify how the characteristics of ICT raise new potential for harm and to show how a reinterpretation of ethical principles can lay the groundwork for ethically defensible data usage. Among these ethical principles is a requirement to ensure that multi-stakeholder partnerships happen more vigorously, given the complexity of future sociotechnical systems that are semi or fully autonomous. Technologies such as driverless cars, industrial robots, brainwave technologies, automated medical implants- and the data collected by all of these devices- will require some kind of embedded ethical agent to ensure that the technology makes decisions that are ethically sound, protecting people's lives and privacy [48]. These examples show that it is vital to think of privacy during the design of the systems, not as a bolt on requirement after diffusion.

D. Toward Consumer Data Rights

Protecting data rights is a real issue - but as we have seen with regulations like GDPR, the work of advocacy groups like Privacy International, and consumer movements like the one to #deleteFacebook, demonstrates that many people are committed to getting involved in reforms, and there is real reason to hope. For instance, blockchain technology- most often associated with cryptocurrencies and other financial technology, can actually be used to store any type of information securely- offering a huge amount of potential for ensuring that people can have more control over their own data. The blockchain facilitates smart contracts between stakeholders. These smart contracts may well be open agreements between consumers and businesses, determining how their data is or is not to be used.

In Australia, the government has decided to legislate a new "Consumer Data Right" to give Australians greater control over their data, empowering customers to choose to share their data with trusted recipients only for the purposes that they have authorized [15]. This is as a direct result of new emerging open frameworks in the banking sector, but will soon be rolled out to other sectors like energy, and telecommunications, and then economy-wide [49]. It is an example of how reforms in the private and public sector can reinforce and influence each other for the greater good, and- in theory- it will mean that individuals can feel confident that they are in control of their data.

With new consumer data rights and data protections set in legislation, consumers will negotiate how much personal information they want to share with service providers. Also, they will be able to choose if they want to open their private data for public access, making it available for research or other purposes. They may even be able to sell their data, and benefit from it the way companies are benefiting from it now. However, the infrastructure around such initiatives are first being enacted by legislation, then implementable frameworks, and then consumer awareness to utilize these open services. The movement around personal data rights is ongoing and will only become increasingly critical over time. Moreover, as new laws and standards emerge, there are still many questions about oversight and governance. It is, therefore, essential for the public to remain informed and involved in the data rights discussions within their communities.

IV. CYBERSECURITY

This section explores cybersecurity as a global issue in the context of the digital revolution, and how ensuring cybersecurity through greater awareness and strong multi-stakeholder partnerships are crucial for achieving the Sustainable Development Goals in a hyper-connected and digitized world. Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes. Cybersecurity is a global issue that knows no boundaries. It affects individuals and society, small and large organizations and transnational companies, critical infrastructure systems that we all depend on, and even our national security. Implementing effective cybersecurity measures is particularly challenging today because there are more devices than people, and attackers are using progressively innovative methods and techniques to compromise systems. The increasing move towards digital records for health, education, and government IDs means that the value of information has become attractive to those who wish to penetrate systems for financial gain, reputational gain, to cause instability, or who just want to demonstrate weaknesses that exist. The Internet was not built with security in mind, however, much of the world's dataflows are transacted over public networks that are vulnerable to attack.

A. CIA Model

It is, therefore, important that corporations and government agencies seek to secure the data they collect on behalf of consumers and citizens. To do this, they can use the CIA model, which stands for Confidentiality, Integrity, and Availability in the context of security. *Confidentiality* of data means that a client can trust that their personal information will not be shared with those that are not explicitly authorized to view it. This process can be achieved, in part, by implementing access control mechanisms, such as authorizing only certain people to access or manipulate information. Resource hiding is another important aspect. Organizations may not wish for people to know about specific equipment they are using, and so the very existence of this equipment must be kept confidential. With confidentiality, the data is either compromised or not. However, *integrity* includes both the correctness and the trustworthiness of the data. The integrity of data has become increasingly important as more sectors adopt data-driven decision-making. If the data underlying the decision is corrupted, the impacts of that decision may be devastating for governments, businesses, communities, and individuals.

In order to preserve integrity, prevention mechanisms are needed to block any unauthorized attempts to change the data or any attempts to change the data in unauthorized ways; and detection mechanisms that report when the data's integrity is no longer trustworthy. These types of integrity mechanisms are particularly important for controlling cyberphysical infrastructure in sectors such as telecommunications, water, and waste control, energy, oil and gas refining, and transportation. The reason is that these sectors affect large populations and significant outages can be harmful to highly urban communities in particular. Therefore, if a natural disaster occurs and the water control system is compromised, and data is corrupted, the flooding can have devastating consequences that could have otherwise been avoided.

Availability, as it relates to cybersecurity, is knowing that one can access or use a resource or data when needed. Someone may deliberately deny access to data or a service by making it unavailable, known as a denial of service attack. These types of attacks generally occur when a hacker overloads a system with superfluous requests, preventing some or all legitimate requests from being fulfilled. It generally means that computers cannot connect to a host machine on the internet, thus denying them the right to carry on with, for example, a retail transaction, a cash withdrawal from an automatic teller machine, or the accessing of vital government records. For example, it is suspected that Australia's 2016 online-only census survey suffered at the hands of unauthorized traffic from outside Australia, impeding people's ability to access the survey and, therefore, be counted in the census [50]. As more systems go online, enforcing the confidentiality of data, the integrity of data, and the availability of system access, it will be crucial to ensure that the systems function as intended, whether they are online government services, mobile banking, e-health records, educational tools, or fundamental infrastructure.

B. Cybercrime

Many of the types of cybersecurity issues we have discussed thus far fall into the category of "cyber threats," which exploit weaknesses in infrastructure. Responses to these threats often involve technical rather than legal measures; as such, a variety of organizations ranging from NGOs to intergovernmental bodies are actively involved in cyber defense. In contrast, cybercrime refers exclusively to attacks on private entities with the intent of gaining profit or inflicting damage. It is estimated that cybercrime is costing us $600B-$1T annually. As more data is collected online, the consensus is that the cost of cybercrime will also rise commensurately. It also follows as the number of devices increase, the greater the number of avenues of attack for hackers to consider to penetrate systems.

At a personal level, hackers are interested in the identity and the credentials found on an individual's computer. Just as countries seek to reap the advantages of global reach through online business models, breaches in security can have a chilling effect on those starting to use the Internet. In countries in Africa, as consumer awareness about cybersecurity grows, cyberattacks have had a detrimental impact on development and growth. Most of the population have also been exposed to phishing attacks- the practice of sending fraudulent emails that resemble emails from reputable sources. The aim is to steal sensitive data like credit card numbers and passwords. It is the most common type of cyber-attack. People can help protect themselves through education on best practices or a technology solution that filters malicious emails.

At the national level, we have seen cyberterrorists stealing fingerprint records and claiming to have penetrated defense websites, making a mockery of defenses and attracting international attention as a result. In September 2015, the U.S. Office of Personnel Management admitted that 5.6 million permanent sets of fingerprints were stolen. The potential to hack DNA databases is also a real possibility. At the international level, multinational organizations have had login details and passwords stolen across jurisdictions. Although the potential for cybercrime can be mitigated by enhancing the security of Internet networks, only national governments possess the proper legal tools and jurisdiction to prosecute attackers. As a result, an effective response to cybercrime is largely restricted to governments. However, this is a genuinely multi-stakeholder environment, and we need to understand data sovereignty, the applicability of international humanitarian law, and the United Nations charter in order to create international standards for managing cybercrime that reach across national borders. One such example is the Council of Europe's 2004 Convention on Cybercrime, which has had some impact on international cooperation and data sharing between nations.

C. Regulating Cybersecurity

Ultimately, security is everyone's problem, not just IT groups tasked with protecting a government's or company's networks and data repositories. In 1992, the OECD produced security guidelines promoting a culture of security by leadership, an extensive participation by government and business stakeholders [51]. The main point raised by the OECD is that security has to be factored in during the design of any new technology system. Today, what we call privacy and security "by design" principles are being taught internationally as a way to emphasize the growing importance of cybersecurity [52]. The principles that the OECD identified were nine-fold, and include awareness of risks, timely responses to risk, ethical conduct, and continuous reassessment, among others. A successful cybersecurity approach has multiple layers of protection spread across the computers, networks, programs, or data that one intends to keep safe. In an organization, the people, processes, and technology must all complement one another to create an effective defense from cyber attacks.

TABLE I Relationship of Privacy, Data Rights, and Cybersecurity with the SDGs & Targets

ID	Definite Technological Intervention Required in the Achievement of Goal / Target	Privacy Impact	Data Impact	Security Impact
1.4	By 2030, ensure that all men and women, in particular the poor and the vulnerable, have equal rights to economic resources, as well as access to basic services, ownership and control over land and other forms of property, inheritance, natural resources, appropriate new technology and financial services, including micr2.1 By 2030, end hunger and ensure access by all people, in particular the poor and people in vulnerable situations, including infants, to safe, nutritious and sufficient food all year round			
2.c	Adopt measures to ensure the proper functioning of food commodity markets and their derivatives and facilitate timely access to market information, including on food reserves, in order to help limit extreme food price volatility			
3	Ensure healthy lives and promote well-being for all at all ages			
3.7	By 2030, ensure universal access to sexual and reproductive health-care services, including for family planning, information and education, and the integration of reproductive health into national strategies and programmes			
3.8	Achieve universal health coverage, including financial risk protection, access to quality essential health-care services and access to safe, effective, quality and affordable essential medicines and vaccines for all			
4.a	Build and upgrade education facilities that are child, disability and gender sensitive and provide safe, non-violent, inclusive and effective learning environments for all			
4.4	By 2030, substantially increase the number of youth and adults who have relevant skills, including technical and vocational skills, for employment, decent jobs and entrepreneurship			
4.5	By 2030, eliminate gender disparities in education and ensure equal access to all levels of education and vocational training for the vulnerable, including persons with disabilities, indigenous peoples and children in vulnerable situations			
5.b	Enhance the use of enabling technology, in particular information and communications technology, to promote the empowerment of women			
6.a	By 2030, expand international cooperation and capacity-building support to developing countries in water- and sanitation-related activities and programs, including water harvesting, desalination, water efficiency, wastewater treatment, recycling and reuse technologies			
7.a	By 2030, enhance international cooperation to facilitate access to clean energy research and technology, including renewable energy, energy efficiency and advanced and cleaner fossil-fuel technology, and promote investment in energy infrastructure and clean energy technology			
7.b	By 2030, expand infrastructure and upgrade technology for supplying modern and sustainable energy services for all in developing countries, in particular least developed countries, small island developing States and landlocked developing countries, in accordance with their respective programs of support			
8.2	Achieve higher levels of economic productivity through diversification, technological upgrading and innovation, including through a focus on high-value added and labor-intensive sectors			
9.4	By 2030, upgrade infrastructure and retrofit industries to make them sustainable, with increased resource-use efficiency and greater adoption of clean and environmentally sound technologies and industrial processes, with all countries taking action in accordance with their respective capabilities			
9.5	Enhance scientific research, upgrade the technological capabilities of industrial sectors in all countries, in particular developing countries, including, by 2030, encouraging innovation and substantially increasing the number of research and development workers per 1 million people and public and private research and development spending			
9.a	Facilitate sustainable and resilient infrastructure development in developing countries through enhanced financial, technological and technical support to African countries, least developed countries, landlocked developing countries and small island developing States			
9.b	Support domestic technology development, research and innovation in developing countries, including by ensuring a conducive policy environment for, inter alia, industrial diversification and value addition to commodities			
9.c	Significantly increase access to information and communications technology and strive to provide universal and affordable access to the Internet in least developed countries by 2020			
11.5	By 2030, significantly reduce the number of deaths and the number of people affected and substantially decrease the direct economic losses relative to global gross domestic product caused by disasters, including water-related disasters, with a focus on protecting the poor and people in vulnerable situations			
11.7	By 2030, provide universal access to safe, inclusive and accessible, green and public spaces, in particular for women and children, older persons and persons with disabilities			
16.9	By 2030, provide legal identity for all, including birth registration			
17.6	Enhance North-South, South-South and triangular regional and international cooperation on and access to science, technology and innovation and enhance knowledge-sharing on mutually agreed terms, including through improved coordination among existing mechanisms, in particular at the United Nations level, and through a global technology facilitation mechanism			

Caption: In future work, SDGs and Targets that require technological intervention for their achievement could be assessed against a number of factors, including privacy impact, data rights impact and cybersecurity impact using a nominal scale.

Cybersecurity aims to prevent an attack before it even happens. This process is the ideal solution and where technology is the most helpful. This prevention may come in the form of antivirus software, firewalls, among many other toolkits like honeypots that lure hackers into revealing their identifying information. If an attack does occur, then detecting it as soon as possible is just as important to understand as what is causing the exposure. Auditing systems in intrusion detection are most effective here. Finally, an organization or government agency who has suffered a cybersecurity attack needs to recover from the attack as soon as possible- that is assess and repair the damage caused, and resume normal operations as soon as possible. It is important to remember that cybersecurity is not a static concern. At times, attacks may be organization agnostic and may be targeted at suppliers of commonly used software. Organizations need to assess their logical and physical relationships with other systems and partners to determine the level of intra-organizational activities, extra-organizational activities, and those on the internet. And as systems are linked to increase interoperability and efficiency, trust in partnerships is paramount when granting employees of other companies access to a system.

1) Laws and International Action

Given that the internet is a truly global phenomenon that has a distributed architecture, no one country rules over it. Instead, given the ill-defined boundaries of cyberspace, a network of institutions is responsible for addressing threats and international relations. Increasingly we are moving toward a governance model in cyberspace, and one where disclosure of data breaches is favored rather than closeted and uncoordinated responses to cybercrime. NGOs, for the more significant part, coordinate community-level responses. Moroever, one primary international institutional response has been the emergence of CERTS (Computer Emergency Response Teams). These teams organize responses to security emergencies, promote the use of valid security technology, and ensure network continuity. Although the majority of CERTs were founded as non-profit organizations, many have transitioned towards public-private partnerships. However, these types of organizations lack power at the national and international levels. The International Criminal Police Organization (INTERPOL) has also become involved in combating cybercrime, creating a 24/7 'Network of Contacts' in order to help national governments "identify the source of terrorist communications, investigate threats and prevent future attacks." The 24/7 Network of Contacts, empowered by Article 35 of the Convention on Cyber Crime, is a rare example of direct international intervention and collaboration [53].

D. The Culture of Security

This paper has only scratched the surface with respect to security, but the culture of security will help ensure that our data is safe and that technology lives up to its potential to be a useful tool for the betterment of humanity:

- Good practices need to be taught early, and guides need to be developed for citizens, governments, and every other sector.
- Stakeholders need to cooperate by sharing knowledge, especially about specific security incidents.
- Capacity building is paramount when it comes to security at every level, beginning with leadership, strategic, and operational staff.
- When it comes to cybersecurity at the national level, citizens and stakeholders must hold their governments accountable, especially as more and more government systems go online. The ITU's Global Cybersecurity Index (GCI) is a fantastic resource here, measuring the commitment of countries to cybersecurity [54].

Harmonization, collaboration, and – above all – education is required to make any progress against cybercrime. Empowering organizations to commit to cybersecurity will contribute to SDG 16– to promote justice and strong institutions– thereby ensuring security for all other ICT-related projects for sustainable development.

V. Assessing the Role of Technology in the SDGs

Privacy, data rights, and cybersecurity present each a distinctive challenge as technological innovations reach the far corners of the earth. Each area in its own right is vital for the successful implementation of any new technology, but the interlinkages are even more important and will invariably impact the potential for the SDGs and the associated targets to be achieved. Development is pluralistic, and very much in-situ and context dependent. The complexity of the systems, also require policymakers and civil society to ensure that SDGs are in harmony. This is a classic socio-technical-legal problem.

An initial step in seeking to understand the role that technology will play in the achievement of the SDGs, is to identify a list of relevant sustainable development targets that naturally incorporate or imply technological interventions. Table I, identifies an approach toward possible technology impact assessment based on the three criteria reviewed in this paper (privacy, data rights, cybersecurity). The table includes a select list of sustainable development targets in order to present a possible way forward into assessing the role that privacy, data rights, and security plays with respect to each SDGs. Each target is thus enabled or hindered by the presence of policies that address privacy, data rights, and security. The list is deliberately not exhaustive but sheds light on the role of technology within the SDGs framework, and will serve as future work.

The position of this paper is that the privacy, data rights, and security discussion serves as a tool to harmonize the SDGs. For example, innovation in facial recognition and AI can arguably allow a society to achieve SDG 16.1 (the significant reduction of all forms of violence and related death rates everywhere), or SDG 11.7 (the universal access to safe, inclusive and accessible spaces). However, the same technology is also designed to be able to exclude vulnerable people from open spaces. Moreover, the vulnerability in the security system can also inform the user's level of trust in an institution. As noted in SDG 16, trust can directly impact economic growth, as also stated in SDG #8 and SDG #16.9, which requires secure data collection and storage. It would, however, be wrong to claim that the role of the three elements is the same in each market/community. Much relies on the respective local laws in place and the role each SDG plays within that specific community. However, the point remains that despite the different levels of influence, privacy, data rights, and security are essential to understand, and integrate into a process of codesign.

VI. Conclusion

The SDGs are designed to elevate how we treat our environment and strive to provide communities with a dignified and safe life. This paper demonstrated the importance of privacy, data rights, and security to minimize externalities at the personal and international levels, but with an emphasis on citizenry as the focal point. The examples that are presented are evidence that humanity's exposure to technological innovation has to be understood and discussed within the framework of the sustainable goals and targets while embedding privacy, data rights and cybersecurity into the design process. This shall inform the choices of policymakers and civil society, as well as assist ICT players to orient their contribution toward the public interest. To that end, the three elements are able to be harmonized together toward the achievement of SDGs to ensure fundamental human rights are maintained.

Acknowledgment

We would like to acknowledge the contribution of the SDG Academy which is the online education platform of the Sustainable Development Solutions Network (SDSN), a global initiative for the United Nations. The elements of Privacy, Data Rights, and Cybersecurity were delivered in the module titled: "Concerns for our Digital Future" in the *Tech for Good: The Role of ICT in Achieving the SDGs* edX course https://sdgacademy.org/course/tech-for-good/.

References

[1] United Nations. (2019). *Sustainable Development Goals: Knowledge Platform -Technology*. Available: https://sustainabledevelopment.un.org/topics/technology

[2] S. Bronitt and K. Michael, "Human Rights, Regulation, and National Security," *IEEE Technology and Society Magazine,* vol. 31, no. 1, pp. 15-16, 2012.

[3] D. Byler. (2019). *China's hi-tech war on its Muslim minority*. Available: https://www.theguardian.com/news/2019/apr/11/china-hi-tech-war-on-muslim-minority-xinjiang-uighurs-surveillance-face-recognition

[4] P. Mozur. (2019). *One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority*. Available: https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html

[5] N. Singer. (2019). *Top Universities Join to Push 'Public Interest Technology'*. Available: https://www.nytimes.com/2019/03/11/technology/universities-public-interest-technology.html

[6] L. Robertson, R. Abbas, G. Alici, A. Munoz, and K. Michael, "Engineering based design methodology for embedding ethics in autonomous robots," *Proceedings of the IEEE,* vol. 107, no. 3, pp. 582-599, 2018.

[7] S. Warren and L. Brandeis, "The Right to Privacy," *Harvard Law Review,* vol. 4, pp. 193-220, 1890.

[8] R. Abbas, K. Michael, M. Michael, and R. Nicholls, "Sketching and validating the location-based services (LBS) regulatory framework in Australia," *Computer Law & Security Review,* vol. 29, no. 5, pp. 576-589, 2013.

[9] United Nations. (1948). *Universal Declaration of Human Rights*. Available: https://www.un.org/en/universal-declaration-human-rights/

[10] E. Black, *IBM and the Holocaust: The Strategic Alliance between Nazi Germany and America's Most Powerful Corporation*. New York: Three Rivers Press, 2002.

[11] UN High Commissioner for Refugees (UNHCR), "The 1954 Convention relating to the Status of Stateless Persons: Implementation within the European Union Member States and Recommendations for Harmonisation," 1954.

[12] R. Abbas, K. Michael, M. Michael, and R. Nicholls, "Using a Social-Ethical Framework to Evaluate Location-Based Services in an Internet of Things World," *International Review of Information Ethics,* 2014.

[13] P. Lewis. (2018). *'I was shocked it was so easy': meet the professor who says facial recognition can tell if you're gay*. Available: https://www.theguardian.com/technology/2018/jul/07/artificial-intelligence-can-tell-your-sexuality-politics-surveillance-paul-lewis

[14] M. Michael, K. Michael, and C. Perakslis, "Überveillance, the web of things, and people: What is the culmination of all this surveillance?," *IEEE Consumer Electronics Magazine,* vol. 4, no. 2, pp. 107-113, 2015.

[15] ACCC. (2018). *Consumer data right (CDR)*. Available: https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0

[16] McKinsey&Company. (2017). *Data sharing and open banking*. Available: https://www.mckinsey.com/industries/financial-services/our-insights/data-sharing-and-open-banking

[17] A. Barbaschow. (2019). *Australia's Consumer Data Right to finally make its way through Parliament*. Available: https://www.zdnet.com/article/australias-consumer-data-right-to-finally-make-its-way-through-parliament/

[18] R. Abbas, "The social implications of location-based services: an observational study of users," *Journal of Location Based Services,* vol. 5, no. 3-4, pp. 156-181, 2011.

[19] R. Pringle, K. Michael, and M. Michael, "Unintended Consequences of Living with AI," *IEEE Technology and Society Magazine,* vol. 35, no. 4, pp. 17-21, 2016.

[20] J. Pitt, "Transforming Big Data into Collective Awareness," *Computer,* vol. 46, no. 6, pp. 40-45, 2013.

[21] R. Abbas, K. Michael, and M. Michael, "Location-based privacy, protection, safety, and security," in *Privacy in a Digital, Networked World*, S. Zeadally and M. Badra, Eds. Cham: Springer, 2015, pp. 391-414.

[22] P. Karp. (2019). *Australians' Medicare details illegally sold on darknet – two years after breach exposed*. Available: https://www.theguardian.com/australia-news/2019/may/16/australians-medicare-details-illegally-sold-on-darknet-two-years-after-breach-exposed

[23] M. Haggan. (2018). *Opt-Out Period Begins with 'Disaster' (Australian Journal of Pharmacy Blog)*. Available: https://ajp.com.au/news/opt-out-period-begins-with-disaster/

[24] C. Knaus, "More than 2.5 million people have opted out of My Health Record," *The Guardian,* 2019.

[25] OAIC. (2019). *Part 4: Notifiable Data Breach (NDB) Scheme*. Available: https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response/part-4-notifiable-data-breach-ndb-scheme/

[26] J. Davis, "Massive SingHealth Data Breach Caused by Lack of Basic Security," *Health IT Security,* 2019.

[27] D. Alexander. (2015). *5.6 million fingerprints stolen in U.S. personnel data hack: government*. Available: https://www.reuters.com/article/us-usa-cybersecurity-fingerprints/5-6-million-fingerprints-stolen-in-u-s-personnel-data-hack-government-idUSKCN0RN1V820150923

[28] A. Cavoukian, "Global privacy and security, by design: Turning the "privacy vs. security" paradigm on its head," *Health and Technology,* vol. 17, no. 4, pp. 329-333, 2017.

[29] A. Bhattacharya. (2018). *Companies can't ask for Aadhaar anymore—or can they?* Available: https://qz.com/india/1402827/supreme-court-verdict-can-companies-ask-for-aadhaar-anymore/

[30] D. J. Edelman. (2015). *Edelman Trust Barometer*. Available: https://www.edelman.com/research/2015-edelman-trust-barometer

[31] Defence Information Systems Agency (DISA). (2018). *Data Rights*. Available: https://disa.mil/About/Legal-and-Regulatory/DataRights-IP/DataRights

[32] European Commission. (2012). *Data protection: Rules for the protection of personal data inside and outside the EU*. Available: https://ec.europa.eu/info/law/law-topic/data-protection_en

[33] C. Reichert. (2019). *Amazon files patent to record before you say 'Alexa'*. Available: https://www.cnet.com/news/amazon-files-patent-to-record-before-you-say-alexa/

[34] R. Abbas, K. Michael, and M. Michael, "The regulatory considerations and ethical dilemmas of location-based services (LBS) A literature review," *Information Technology & People,* vol. 27, no. 1, pp. 2-20, 2014.

[35] K. Michael, "Towards the Blanket Coverage DNA Profiling and Sampling of Citizens in England, Wales, and Northern Ireland," in *Uberveillance and the Social Implications of Microchip Implants: Emerging Technologies*, M. Michael and K. Michael, Eds. Hershey: PA: IGI, 2014, pp. 187-207.

[36] L. Geggel. (2018). *23andMe Is Sharing Genetic Data with Drug Giant*. Available: https://www.scientificamerican.com/article/23andme-is-sharing-genetic-data-with-drug-giant/

[37] 23andMe. (2018). *Privacy Policy*. Available: https://www.23andme.com/about/privacy/

[38] SANS Institute. (2019). *Policies*. Available: https://www.sans.org/security-resources/policies

[39] OAIC. (2019). *Draft CDR Privacy Safeguard Guidelines*. Available: https://www.oaic.gov.au/engage-with-us/consultations/draft-cdr-privacy-safeguard-guidelines/

[40] I. Lapowsky, "How Cambridge Analytica Sparked the Great Privacy Awakening," *WIRED,* 2019.

[41] A. Mak. (2019). *How Much Facebook Has to Pay in Fines and Settlements This Year*. Available: https://slate.com/technology/2019/10/facebooks-2019-fines-and-settlements.html

[42] European Commission. (2018). *EU Data Protection Rules*. Available: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

[43] N. Confessore. (2018). *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far*. Available: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

[44] A. Hern. (2018). *Facebook moves 1.5bn users out of reach of new European privacy law*. Available: https://www.theguardian.com/technology/2018/apr/19/facebook-moves-15bn-users-out-of-reach-of-new-european-privacy-law

[45] The Chartered Institute of Marketing. (2018). *Data Right: Best Data Practice*. Available: https://www.cim.co.uk/more/data-right/

[46] L. Fair. (2019). *FTC's $5 billion Facebook settlement: Record-breaking and history-making: Federal Trade Commission*. Available: https://www.ftc.gov/news-events/blogs/business-blog/2019/07/ftcs-5-billion-facebook-settlement-record-breaking-history

[47] M. Bailey, D. Dittrich, E. Kenneally, and D. Maughan, "The Menlo Report," *IEEE Security & Privacy,* vol. 10, no. 2, pp. 71-75, 2012.

[48] L. J. Robertson, R. Abbas, G. Alici, A. Munoz, and K. Michael, "Engineering-Based Design Methodology for Embedding Ethics in Autonomous Robots," *Proceedings of the IEEE,* vol. 107, no. 3, pp. 582-599, 2019.

[49] Open Banking Europe. (2019). *Building a Digital Europe Together:* . Available: https://www.openbankingeurope.eu/

[50] BBC Staff. (2016). *Australian census attacked by hackers*. Available: https://www.bbc.com/news/world-australia-37008173

[51] OECD. (2012). *Cybersecurity Policy Making at a Turning Point*. Available: https://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

[52] A. Cavoukian. (2011). *Privacy By Design: The 7 Foundational Principles*. Available: https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf

[53] Council of Europe. (2001). *Convention on Cybercrime*. Available: https://rm.coe.int/1680081561

[54] ITU. (2019). *Global Cybersecurity Index*. Available: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx