Passive Violation of Consumers' Privacy Rights on the Internet in the Age of Emerging Data Capital

Dr Anan Sh. Younes
Assistant Professor,
Al Falah University, UAE-Dubai

ABSTRACT

This paper looks at the several methods by which consumers readily step into the information dragnets set up by businesses, which are then utilised to classify and arrange people into classes of creditworthiness, taste, or even political views. We have looked at both the sides of this data capital owning industry, to understand why and how consumers are compelled to release their personal information knowingly or unknowingly. On the other hand, corporates are convinced about the competitive advantage offered by data capital, due to their enhanced capabilities to supply tailored products and services. Following a brief discussion about the various technologies that are used by companies to dig deeper into consumers' personal lives and the corresponding remedies of their breach, we have also looked at the global data protection laws that are ostensibly present to protect our privacy, but nevertheless, do not guarantee our online anonymity. While personalised browser advertisements may be merely the beginning and appear to be otherwise harmless, however connecting different aspects and choices of one's life to predict future behaviour results in loss of right to free choice and sets the platform for companies to do so on behalf of consumers, and they decide the rate of insurance or product cost by determining them basis the data possessed by them. We conclude on the note that even if a user decides to renounce the comforts offered by the digitally connected life and opt to be a digital hermit, it would be nothing but a pointless exercise since we are even being tracked offline at every moment. So the only possible solution seems to be highly aware of one's digital footprint since it will put us in control and in a better position to protect privacy.

Keywords: Big Data, Breach of Privacy, Cookies, Data Capital, Data Mining, Data Warehousing, Digital Footprints, Internet of Things, Passive Data Collection, Online Profiling

Introduction

It is a rather strangely conniving truth of surveillance society that we are now living in, that unidentified entities are collecting our data for unknown purposes. Privacy is one of the most convoluted legal issues concerning e-commerce businesses. With the persistent global advancement of e-commerce, an extensive range of personal information is being compiled by companies. Consequently, the internet has now facilitated the consistent trading of private information of its users. Corporates and the governments are constantly in an endeavour to deep dive into the active or passive digital footprints, as they keep diligently tracking our activities, location and contacts. While the methods and reasons behind such tracking are myriad, they range from annoying non-compliances like WhatsApp sharing the name and phone number of its users with Facebook so that e-commerce sites can freely advertise, or even the creation of detailed profiles being sold and used to circumvent consumer protections meant to limit predatory and discriminatory practices.

A data imperative often drives businesses to harvest data. This imperative calls for extraction of data from every available source. Thriving e-commerce companies and leaders like Amazon, Uber and Google have embraced the idea of considering data as an asset. Unlike the frequently used bombast, data does not exist independently in the world, nor is it capable of being generated on its own. Data is sourced and saved from people, often overstepping from the original intention and rather than merely collecting it, passive invasive systems are created for probing, monitoring and tracking people. The viewpoint of considering data as capital is now prevalent among many businesses. Data capital has been observed to be of the same level as financial capital in terms of generating new digital products and services. This development has implications for every company's competitive strategy and thereby indicates a change in the value of data

possessed by market leaders. This trend has been observed, thus implying that data is being hoarded, commodified to a huge extent.

Although some websites hardly have any interest in actively profiling their users or discovering personal information about them, however, they nevertheless end up collecting considerable quantities of personally identifiable data that may trigger liability risks. While the voluntary collection of such personal information is common and consumers are aware of the personal information voluntarily supplied by them, however, they are often taken by surprise to discover that their personal data and online behaviour are being tracked without their knowledge. For example, at times the host server records custom information pertaining to every visit of the user. Also, certain banner ads permit third-party advertisers to follow and record users' browsing trends.

In his *Harvard Business Review* article titled "Big Data: The Management Revolution", Brynjolfsson discusses how previously, managers were known to have relied on their "gut instinct" for decision-making simply because they lacked the data to do otherwise, while today it is more scientific, and many managers are not accustomed to making decisions this way. Researchers at Massachusetts Institute of Technology have conducted a survey including nearly 200 companies to conclude that data-driven decision making has augmented the development of productivity and output. So, it is apparent that businesses are benefitting from these data, but the question is to what extent can they cause inconvenience and annoyance to consumers while they are at it?

In the following sections, the aspect of liability of an e-commerce website's information collection practices will be discussed. This will be done by primarily understanding the kind of information being collected. Part I of this article discusses the conventional methods employed by e-commerce websites in collecting data of its users, followed by the emerging ones in Part II. Part III explores the ways in which one can manage their privacy in an Internet of Things setting, where the data generated by all smart things tend to be much more personal and commercially sensitive. As this technology grows, it is important for consumers to understand how to oversee the consent allowed to the smart things and to what extent they use them on their own. Next, we have discussed a global overview of data protection laws In Part IV, while briefly focusing on a few jurisdictions to understand the extent to which consumers are apparently protected there. Part V has reviewed some landmark judgments pertaining to the question of whether cookie technology which employs text files on a consumer's computer in order to access browsing history, commits trespass or other common law torts. While initially introduced as harmless convenient technology, it is now known to have been used for unscrupulously tracking consumer behaviour. Part VI has looked into both sides of the privacy- personalisation debate between consumers and businesses. Finally, we conclude on the note that violation of privacy has become a routine practice, in spite of several ostensible legislations out there. The way forward to protecting one's privacy seems to be by being aware of the ways in which we have shared data. This will only make the consumer more responsible about where they share their information, till the time when the data economy matures and consumers resume their lost power of self-determination, which lies with the corporations at present.

I. Traditional Procedures of Data Collection

E-commerce websites generally have a routine practice of directly prompting users to enter personal information by filling out forms. Additionally, some sites also document their users' browsing patterns and subsequently match the same with other statistical information to generate a profile of user preferences. These profiles are then put to use for the purpose of target advertising or to provide customized services to consumers. Also, the financial information recorded in these profiles might be used to discriminate among consumers while offering the same product. For instance, a higher amount might be charged to users who have shown willingness to buy a product more than others. This practice, also known as weblining enables e-commerce websites to frequently reduce the choices available to consumers. By adopting this practice, businesses are denying consumers the right to self-determination and are restricting their choices.

Even though a cursory glance at an e-commerce website might tempt one to rule it

out of the list of sites that engage in the practice of extensive data collection of consumers, however, attorneys are very well aware of the extent to which these sites actually do so. Depending on its extent and nature, such practice may invite liabilities, including breach of e-commerce contracts or fraud, where privacy policy has been violated, among others.

Users divulge their personal information in a number of ways, but most importantly, by means of the automatic disclosure of information that is collected by the website's server software. A significant data is collected by third-party advertisers that have access to the website. Most servers are known for keeping an account of browsing habits of visitors, in the nature of pages visited, including intricate details like the span of such visits, advertisements noticed during those visits, purchases made, search strings entered etc. Moreover, the basic details of users like the name and type of browser, IP address, computer name are directly recorded by the servers. In addition to this information, some sites allow third-party advertisers to place cookies on users' hard drives.

When e-commerce websites provide access to advertisers to plant cookies in the users' system, through advertising networks, such cookies are used to evolve the users' detailed profiles by analysing their browsing habits over several visits. For example, a user 'X' surfs through an e-commerce website, intending to buy a specific kind of leather jacket. An advertising network prompts an ad, which is clicked on by 'X'. Henceforth, whenever 'X' visits any other affiliate website, a notification will be sent by his computer, detailing out the kind of website visited by 'X' and accordingly suggesting more advertisements basis the browsing history recorded. Such practices because have the potential to give rise to liability risks and therefore, must be disclosed in the site's privacy policy.

The example discussed above shows the need to comprehend the websites' practices of data collection. Software logs and third-party cookie placements are often overlooked spheres of information collection. Some websites unknowingly collect information automatically through their server software, and many allow third-party cookie placement. According to a recent FTC privacy survey, although 57 per cent of the most bustling websites allow third-party cookie placement, however only 22 per cent disclosed that fact in their privacy policies. It is important for website owners, online vendors to be well informed about the magnitude and scope of data collection employed so that they are not caught off-guard. They should be in a position to honestly brief consumers about the kind of data being tracked by them.

Apart from the above-mentioned traditional means of documentation of consumer information, there are constant streams of passively recorded data that are stored and analysed in the absence of the user's knowledge. For instance, passive tracking of Fitbit and similar health trackers are of much use to insurance companies. As the scope and depth of data collection keep on expanding, personal information comes in handy to classify people into groups depending on their likelihood or qualification to buy a product or service, like taking up insurance or repaying a loan. People are rated according to their scores and placed in rank lists according to their eligibility, determined from the data collected during tracking. These data scores awarded and classes that consumers are segregated to provide the lens to view corresponding consumers to the ideal goods or services they match against. Here, these matches and exchanges are made on the basis of individual measurements to capture moral categories such as trust, reputation, goodwill and respect on the input side, and extractability on the output side.

II. Evolving Technologies

Besides the very well-known traditional technologies like cookies, there are a number of developing technologies on the rise, which are utilised to monitor consumer behaviour.

A. Consumer Profile Exchange (CPEX)

CPEX is an XML-based standard that permits companies with different software and techniques for collecting consumer information to share their data more easily in a common format. A positive point about CPEX is that it offers a vendor-neutral code for facilitating the privacy-empowered exchange of customer information across disparate enterprise applications and systems.

B. Platform for Privacy Preferences (P3P)

P3P provides a covenant designed to boost the protection of consumer privacy protection. Websites facilitated with P3P includes data that can be comprehended by machines, displaying the type of data collected by the site and its manner of use. P3P was developed by the World Wide Web Consortium ("W3C") and was intended to augment the confidence of consumers and to allow ease of access during online transactions.

As was outlined above, privacy statements play an important role in addressing privacy through P3P. P3P is capable of corresponding to the various privacy choices of users. For example, with P3P identity concerned users have the potential to effectively exclude sites that demand information in the categories. Also, P3P is a relatively open platform standard. It could easily be extended to prohibit or at least warn of communication processes.

Since online users do have a substantial impetus to generally accept interactive and preference demanding websites, there is an ample amount of risk for online users to let go of their privacy. A question-answer session with a sales bot would be to categorise the kinds of questions enquired by the agent. For instance, a distinction could be made between questions in decreasing order of importance, starting with questions that are idiosyncratic to the product itself, from those that pertain to usage related and personal questions supporting the selection process, and finally, personal questions that have nothing to do with product selection. Categorising the products in this manner would enable users to have worthwhile choice to execute privacy during their interactions with sales bots because this practice allows them the knowledge of what is otherwise hidden behind the term 'interactive'.

III. Perception of Privacy in the Internet of Things

Internet of Things ("IoT") promises a range of interconnected, systematised, liaised environment that functions on the permission granted by the consumer to freely interconnect devices. For instance, a consumer's air conditioner might 'talk' to the weather station to discern the temperature condition and then switch on the machine when the phone's GPS alerts that the consumer is on the way home from the office. While these ''talkative' devices ensure the comfort of the consumer and saves him the hassle of waiting for a while for the room to be in the perfect temperature once he is home, the question to be considered here is whether the cost of the facility provided by IoT worth sacrificing the privacy during this process?

Privacy is a very wide-ranging and divergent idea which has been defined in various ways and perspectives. Various definitions have been discussed, ranging between media, territorial, communication, and bodily privacy. As noted above, information privacy has become a prevalent issue of the day. Information privacy had been defined in 1968 as '*the right to select what personal information about me is known to what people*'. While applying this definition to IoT, it is quite obvious that this definition from the 20th century has become too general in its meaning. Taking cue from the said definition, privacy in an IoT atmosphere can be assured to the subject to the extent of awareness of privacy risks imposed by smart things and services surrounding the data subject, individual control over the collection and processing of personal information by the surrounding smart things and control of subsequent use and dissemination of personal information by those entities to any entity outside the subject's personal control sphere.

With the emergence and increasing availability of smart devices, data collection has been invading the lives of people at a greater extent, in order to create entirely advanced groups of connected and ascertainable private data. During this explosion of data collection technology, human involvement has also qualitatively changed. While an active involvement is necessary for the use of social networks, users are, however, predominantly passive data collection is also done by the foreseen flood of smart things. Owing to its new approach of marketing, improved operations and customer management, expansive range of products and services, e-commerce has been able to rapidly increase its popularity and dependence within just a few years of its existence. A primary facilitator of this change is due to the increased use of tools facilitating data mining. Sophisticated data mining has now made it

possible to provide information to the management in manners that were previously never possible. For example, financial decisions taken while buying a product at online auction sites like e-Bay give away the information of how much money they are willing to spend on products. Similarly, the analysis of clickstream data hints at methods employed by consumers before deciding on what to buy.

The evolving technologies of IoT and its interaction with devices give way to a peculiar set of privacy threats and challenges. The ubiquitous presence of smartphones coupled with the perpetually active social media updates have led to an ever increased infiltration in the private and public lives of people, allowing technology to carry out data collection and identification, tracking, and profiling.

Research on location privacy has suggested several means that can be classified on the following basis (i) client-server, (ii) trusted third party, and (iii) distributed or peer-to-peer. These approaches, however, have mostly been built for outdoor situations, where the user actively employs a location-based service ("LBS") connected to a smartphone. Thus, these approaches do not fit without significant modifications to the changes brought by IoT. The primary challenges here are the need to create an awareness of tracking in the face of passive data collection, control of shared location data in indoor environments, and privacy-preserving protocols for interaction with IoT systems.

Profiling methods are mostly used for personalization in e-commerce, by means of recommender systems, newsletters, and advertisements and also for internal optimization based on customer demographics and interests. Examples of violation of privacy while profiling are price discrimination and instances of charging higher for the same hotel room, based on the ability to pay more. The data about the ability to pay more for a product is traced from the name of the handset being use, which gives away the information of whether it is expensive or not. Additionally, unsolicited advertisements, social engineering, or erroneous automatic decisions like Facebook's automatic detection of sexual offenders also, give away the information required during price discrimination. Also, collecting and selling profiles about people as practised by several data market places today is commonly perceived as a privacy violation.

Methods employed to preserve privacy used at present include client-side personalisation, data perturbation, obfuscation and anonymization, distribution, and working on encrypted data. The application of these methods in the context of IoT can be done but must be readjusted from the usual model, which assumes a central database and account for the distributed data sources that are expected in the IoT. This would demand significant efforts for recalibration of metrics and redesign of algorithms. Thus, it can be observed that balancing the interests of businesses for profiling and data analysis with that of users' need for privacy will indeed be a challenging task in itself.

IV. A Global Perspective of Consumer Privacy

A normal day in the life of an internet user results in the creation of passive and active digital footprints. The comfort and ease of use offered by e-commerce businesses, coupled with the huge amounts of data provided by telephone service providers, free Wi-Fi have resulted in an abundance of consumer data trails. People have become used to living in smart voice-controlled homes, being prompted about the traffic conditions, having readily available ridesharing services and paying from credit cards linked e-wallets. Undoubtedly, this has led to increased monitoring of consumer behaviour thereby requiring effective measures of protection of privacy of the consumer data.

The right to privacy is an element of various legal traditions to restrain governmental and private actions that threaten the privacy of individuals. Over 150 national constitutions mention the right to privacy. Data privacy had started to enjoy the spotlight since the 1990s when several developed economies recognised the importance of the citizens' data and its potential exploitation from organisations. This focus resulted in the framing of comprehensive data regulations and industry-wise laws in these nations to conserve the personal data of its citizens.

The United States has a Privacy Act in place which regulates government departments and agencies since 1974, while other states have

separate privacy laws. Hong Kong, Australia and New Zealand have been some of the first in the Asia-Pacific to embrace legislations covering privacy and data protection laws. The global gaps in coverage of these laws have been witnessed in Africa and the Middle East, although now legislations concerning personal information is steadily increasing in both these regions.

In Asia, countries like India, although at a nascent level when compared to the global timeline, reliefs under the Indian Penal Code, 1860 along with tort remedies have always been in existence. However, recent amendments to the primary legislation along with the introduction of other regulations have strengthened the position as compared to its erstwhile state.

Data privacy laws worldwide have been framed with a shared intention of safeguarding the privacy and personal data of individuals. While these legislations have varied requirements, however, some common elements like Fair Information Practices (FIPS) and Organization for Economic Cooperation and Development (OECD) guidelines are at the core. In this section, we will look at the data privacy laws of some nations to have an overview of the enactments in these nations.

i. **United States**

The US privacy law is a complicated mixture of national privacy laws and regulations that focus on specific matters, while state laws focus on issues pertaining to privacy and security of personal information, and federal and state prohibitions against unfair or deceptive business practices.

Additionally, the US Federal Trade Commission (FTC) enjoys jurisdiction over several commercial entities under its authority to prevent and protect consumers against unfair or deceptive trade practices, including materially unfair privacy and data security practices.

ii. **India**

At present, the Indian data privacy regime exists under the Information Technology Act, 2000 (“IT Act”). India has also adopted the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 which mandates corporates to abide by certain compliances while collecting, processing and storing personal information and sensitive personal information.

India is on its way to adopting a new regulatory framework for data protection and privacy. In a historic judgment, a nine-judge constitution bench, the Supreme Court of India unanimously recognised the right to privacy as a fundamental right.

Additionally, the Telecom Regulatory Authority of India ("TRAI") suggests certain crucial standards defining personal data, the sufficiency of the existing data protection framework, user empowerment and data privacy, and security of telecom networks. The authority requires that the ‘privacy by design' principle be made applicable to all the entities in the digital ecosystem.

iii. **Canada**

Apart from statutory torts, privacy requirements under separate legislations, federal, criminal code etc., Canada has several legislations governing the use of personal information in different sectors. Personal Information Protection and Electronic Documents Act (“PIPEDA”) regulates consumer as well as employee personal information practices of organisations that are deemed to be a ‘federal work, undertaking or business’ eg. banks, telecommunications companies, airlines, railways, and other interprovincial undertakings.

iv. **United Kingdom**

The United Kingdom has adopted the General Data Protection Regulation (EU) 2016/679 (“GDPR”), which along with the Data Protection Act 2018 ("DPA") regulates a number of criminal offences relating to personal data processing. The GDPR has also been empowered with an extra-territorial effect, i.e. an organization that processes personal data of data subjects who are in the Union where the processing activities are related "to the offering of goods or services", will be subject to GDPR even in case they are not established within the European Union.

v. **China**

The People's Republic of China has not adopted any specific exhaustive data protection law, but rather there are rules in place pertaining to personal data protection, which form a part of several complex

structures of laws and regulations. It is apparent that the relevance of such laws and regulations would customarily revolve around the factual background of each case.

Apart from these, there are provisions of civil law and interpretations of tort liabilities which give way to the right to privacy; however, these interpretations may not always be very categorical. Recently, in 2017, the Cyber Security Law of the People's Republic of China ("PRC Cybersecurity Law") has been enacted to govern the transnational transmission of data at critical information infrastructure and to establish a security system for key information infrastructure, among others. However, in spite of this national level law aimed at the protection of data privacy, there have been certain controversies leading to ambiguity as to the application of the law. In addition to the PRC Cybersecurity Law, there are a number of regulations and standards to further augment the PRC Cybersecurity Law form the foundation of general data protection rules existing in the country.

V. Of Cookies and Courts

Internet users in general and e-commerce users more specifically, are familiar with the practice of being bombarded with numerous banner ads the moment they visit a website. Internet advertising firms store cookie files on the users' drive to carefully craft selected ads based on their previous choices. Consumer profiles thus created from these databases are then placed on affiliate websites of the client.

The history of the usage of cookies dates back to the 1990s, when Netscape introduced a technology to modify the presentation of the website to visitors. Technically speaking, a cookie refers to a small text file that an Internet server transfers on the users' hard drive. The storage capacity of the cookies varies from one browser to another. For example, Google Chrome allows approximately 4096 bytes while Internet Explorer permits about 5117 bytes.

Cookies were originally introduced as a straightforward method to enable ease of use and facilitate users with the convenience of storing websites previously visited so that users are saved of the effort of having to identify them on each visit. For example, if a certain website required the disclosure of personal or financial information that is mandatory to enter the site, then the site would place a cookie carrying this information, thus facilitating much convenience to users who are spared from the repeated efforts during subsequent visits. The trail of information left behind by an internet user, usually referred to as "clickstream data" including general information, like the type of computer, websites visited, kind of browser being used etc.

However, with time, the initial objective of cookies has been replaced by organisations that have discovered a means to employ this technology to follow consumers' movements on the web. This is done by furtively placing cookies and later recovering them in a way that permits them to construct exhaustive profiles containing consumers' interest-related data that might may initially appear to be innocuous and at most be only a little bothersome at best, however it can be rather disconcerting to imagine how these databases of consumers' personal choices ultimately might be utilised to group them as representatives of distinct groups.

Having said that, the other side of the story is that not all cookies are harmful. They are in fact capable of contributing valuable functions on the web and providing ease of access to users.

The extensive transfer of cookie information facilitates Internet advertising firms with abundant information pertaining to consumer choices and related data. The collection of all these cookie files collected from different associated client websites allows internet advertisers to preserve a huge database of information, which is of course much more than what an individual client may be able to manage. Consequently, these profiles enable advertisers to place ads on affiliate websites that focus on the particular user's previous online activity, in spite of it being unrelated to the website visited by the user.

For instance, a user who had previously clicked on a cosmetics website might find an advertisement for lipsticks even when visiting a real estate website later on. It is more important to note that internet advertising firms could possibly advertise the profiles they extract that are beneficial to various companies that are not limited to conducting business over the Internet.

There has been much hype about the compliance of cookies with the E.U.'s new General Data Protection Regulation. However, it is not new and follows the E.U.'s "Cookie Directive," which has been in effect for several years. Prior to the implementation of GDPR, websites would have been in perfect compliance by simply publishing a statement on the lines of "*By using this website, you accept cookies*". While this informed users about the use of cookies, however, it hardly gave them an alternative. It did not allow them to make an informed choice. With the introduction of the GDPR, users have now been given the much needed option of informed choice. Since cookies can be used to specifically recognise the online behaviour of a person, therefore, quite evidently, they are being perceived as personal data. Identifiers employed for the purpose of chats, analytics, surveys, advertising among others have been covered under this purview.

The technology facilitated by cyberspace gives access to an imperceptible and accurate investigation of consumer behaviour. The data generated as an offshoot is of course valuable enough for entities to pursue it for commercial exploitation. This is where consumers resist, at a point where their privacy is compromised, thus leading to much dissension about this data generated. Reconciliation of this conflict calls for judicious deliberation.

In spite of occupying a significant and contentious role in the world of e-commerce, a very small number of courts have dealt with the subject. Since there are no specific legislations directly governing online profiling and related concerns, there have been several class action suits filed basis common law tort remedies like trespass and unauthorised access to hard drive due to the storage of cookies. Besides, arguments concerning unfair trade practices, violation of anti-stalking laws have also been made.

Over time, courts have had to address concerns revolving around the aspect of internet trespassing by the cookie technology. The reason behind such alleged violations is due to the internet advertising agencies' dependence on cookies. Uncomfortable with the unwarranted stalking while trying to match online ads with the specific interests and characteristics of individual Internet users, groups of aggrieved consumers have moved the court. There have been a number of class action suits, but only the landmark ones are being discussed in the sections bellows. The following represent some of the significant questions considered by Courts.

a) *Are advertising firms violating consumers' privacy by placing targeted banner ads on affiliated websites?*

One of the most landmarks decisions concerning privacy, property and the internet is *In Re: DoubleClick Inc. Privacy Litigation*, in which Plaintiffs brought in a class action suit against the largest internet advertiser DoubleClick. According to the Plaintiffs, the defendant company would place a cookie on users' hard drives that collected personal information of internet users, like their browsing patterns, names, addresses, and phone numbers among others. The petitioners contended the violation of three federal laws, namely the Electronic Communications Privacy Act (ECPA), the Federal Wiretap Act (FWA) and the Computer Fraud and Abuse Act (CFAA), along with other common-law doctrines of invasion of privacy, unjust enrichment and trespass.

The Court, however, dismissed all the above-mentioned grounds and noted that the collection of data by the use of cookies fell under an exception to the general statutory prohibition, intended to prohibit hackers from obtaining, altering or destroying certain stored electronic communications. Similarly, the defendant's collection of data was also similarly covered by a statutory exception to the prohibition in FWA. Additionally, the court also observed that due consent was accorded from the defendant's client websites to receive information contained in the cookie. Such consent gave protection to the defendant from being held criminally or civilly liable, unless it could be proved that "'*such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or any State*.'"

Unable to find any allegations regarding the criminal or tortious motive behind the collection of the users' data, the Court dismissed the petition concluding that the defendant's use of cookies to collect personal data of consumers was exempt from the provisions of the FWA. Further, the allegations under CFAA were also turned

down and it was noted that the said legislation would have been applicable only in a case where the alleged damages would have surpassed $5,000.

b) *Whether an Internet advertising "subcontractor" could be held liable for depositing cookie files on the hard drives of Internet users?*

In *Chance v Avenue A, Inc*., a number of Internet users filed a suit against an internet advertising firm for planting and accessing cookies for information of users from their hard drives. Avenue A also functioned as a sub-contractor for DoubleClick and placed specific banner advertisements on DoubleClick affiliated sites. Therefore, the plaintiffs argued on similar lines as the DoubleClick case, alleging a violation of ECPA, FWA and CFAA, coupled with common law torts of invasion of privacy, unfair business practices, trespass etc.

c) *Whether or not an Internet tracking firm and its clients could be held liable for using cookies to build detailed profiles of website visitors?*

In yet another case based on similar facts to the DoubleClick case, In *Re: Pharmatrak, Inc. Privacy Litigation*, several internet users brought a class action suit against an Internet monitoring company called Pharmatrak. The defendant along with other drug companies were in the practice of employing cookie technology to generate comprehensive profiles of users visiting these drug company sites. Following the arguments made by plaintiffs in DoubleClick, Intuit and Avenue A, the class in the case alleged that the defendant had not only violated the ECPA, FWA, CFAA and had attracted common law torts like trespass, unjust enrichment, among others. Once again, the Court noted that there was due authorization obtained by the defendant. Echoing the analysis in the DoubleClick judgment, the Court reiterated that the cookie files were not in "electronic storage" thus not satisfying the requirement set by ECPA.

According to the class, cookies were then surreptitiously utilised to combine different kinds of personal information in the nature of "*names, addresses, telephone numbers, dates of birth, sex, insurance status, medical conditions, education levels, and occupations* . . . Yet again, it was noted that the class did not succeed in demonstrating any tortious or criminal intention in the collection of the cookie behind the interception of the cookie files.

VI. Enabling *Audi Alteram Partem*: Consumer v Business Perspectives

The business perspective of the collection of data is explicable to a certain extent since personalisation can help boost the financial perspectives of e-commerce sites. It has been suggested that personalisation can permit five to eight times the return on investment and boost sales by minimum 10 per cent, so it is apparent why some business owners are even covertly attempting to capitalize on this effective technique. Expecting to produce highly organic traffic to their websites and to outpace competitors, businesses are known to seek personal data to help them to improve consumer experience over time.

A recent report of internet trends has suggested that generalised content will no longer be required since personalization and local marketing have visibly led to more successful results. However, some marketers are so dazzled by the depth of information that modern technology can unveil, they seem to have overdone the pudding when it comes to personalising data and need to remember it's the quality not the quantity of customized content that matters.

Businesses, mostly, are tempted to be passive with data collection efforts because of the convenience and speed it offers, however, by doing so, they make a mistake since it has an effect of estranging consumers. It is therefore not advisable to be dependent on algorithms to passively record data since consumers are exasperated by such attempts, rather collaboration is much more helpful. This has been distinctly portrayed by the Accenture Report which depicts that nearly two-thirds of consumers who reported a brand experience that was too personal or invasive did so '*because the brand had information about the consumer that they didn't share knowingly or directly, such as a recommendation based on a purchase they made with a different business.*'

Therefore, e-commerce businesses must implement similar social etiquette as though the interaction is taking place at a personal level, in the brick and mortar stores. If one imagines and replicates a personal conversation between a customer and a shop assistant, aimed at directing the former to

make an informed choice by directing them to their preferred products in the digital world, it would be an ideal one. The said conversation does not entitle the shop assistant to information about the customer's visit to a shop in the next neighbourhood or to follow around for the remaining day. It would be rather preposterous for the assistant to justify such stalking activity in order to ready the consumer for his subsequent visit, merely because he had consented to speak to the shopping assistant in the first place. This situation clearly demonstrates why consumers are usually creeped out by businesses crossing the line while taking unfair advantage of their personal data.

A study of various online surveys demonstrates the fact that consumers have explicitly been worried about their internet privacy; however, their online behaviour repudiates this fear. In spite of having concerns about privacy, internet users are known to not having carefully read privacy policies. For instance, a survey by a team of corporate and trade association executives demonstrates that only 3 per cent of consumers actually read privacy policies, and 64 per cent only cursorily do so or never read it at all.

Consumers may tell survey-takers that they fear for their privacy, but their behaviour does not say necessarily demonstrate such apprehension. In many instances, consumers have been more than willing to give away their personal information when businesses have offered high discount or freebies. To add to the list, consumers do not care to read privacy policies.

Conclusion

While the entire privacy debate surrounding e-commerce seems to be a modern issue, which has seemingly surfaced with the rise of the internet, however, it must be understood that this is not a new practice since the collection and management of information regarding consumers have always been a practice for businesses. Consumer behaviour discernments in the nature of loyalty card schemes at supermarkets have existed since a long time to help businesses strategise effectively and surpass competitors. With the emergence of the digital imperatives and dependence on the Internet, consumers are now actively and passively generating massive amounts of data upon every use.

The introduction of newer technologies like the IoT and artificial intelligence have facilitated companies with the opportunity to capture and analyse a plethora of data, some done with users' active consent while others have been doing so very sneakily. The dependence on digital technologies has thoroughly transformed the manner in which we exist today. Therefore, it is necessary to harmoniously live in this digital world, where we generate data at an extraordinary volume and pace. Naturally, it follows that facilitating privacy to the end consumer and protecting their data has occupied significant importance while allowing businesses to smoothly conduct their business at the same time. As observed earlier, businesses are heavily reliant on consumer data. The term ‘data capital' when used, is no longer in a metaphorical sense, it is very much literal. The purview of the term ‘capital' as understood in economics, includes produced goods. The knowledge of consumer preference and behaviour might be effective enough to yield higher value over the next few years.

The Road Ahead: Recommendations

Imagine waking up one fine day to realise that Google will henceforth be charging fees for every search that carry out or if Facebook asks you to pay for staying connected to your friends. This will help us realise that the content on the Internet which might appear to be free of cost, actually isn't. The cost associated with the services demands payment and of course, when we do not pay for it, someone else has to. That gives rise to the issue at hand, compromising consumers' privacy, thereby making them the product rather than the consumer.

In order to ensure co-existence, both consumers and businesses need to accommodate and take authority for their actions. The central issue of privacy is to find a balance between privacy rights for consumer protection and while still providing benefits to businesses. While the issue is a persistent one, adoption of the following measures on part of both the parties could help ameliorate the situation.

i. Taking active control of personal data

Regardless of our knowledge, we are constantly leaving shreds of data exhaust. This data exhaust comprises not merely our pet's photos but also personal health information like heart rate generated by tracking devices. This warrants a constant awareness on part of the consumer. Unlike a prevalent perception, privacy is not about having secrets but rather being entitled to choose the kind and extent of information to be shared.

The knowledge and control of the amount of data shared are empowering. Once aware of various ways in which personal data is shared, consumers tend to be more responsible about where they shared these data. Some mobile applications that do not require the access to location, track it anyway. Turning off the permission to share location these apps would help clients. Also, the lure of supposedly free services collects data in the background. It is imperative for consumers to realise the extent of data footprints so that they can demand custody and control of such data.

ii. Being more Aware of the Personal Data Shared

In a recent survey by CEB, consumers were given the following choices and asked about how they feel when they view an online Advertisement based on their personal data:

(i) Creeped out

(ii) Angry

(iii) Indifferent

(iv) Bad

(v) Positive About Brand

(vi) Valued

(vii) Confused

The response received showed that almost half of consumers were 'creeped out' by the way in which online ads had used their details. This suggests that they weren't aware marketers had access to this information. One reason for this is that many consumers do not truly appreciate what the term 'personal data' encompasses and what scraps of information marketers are pulling together to create customized content.

The question of why consumers are so blissfully unaware of the imminent threats associated with readily sharing personal information is an extensive topic for discussion in general, but in short, it can be analysed to discuss a few aspects. Firstly, the acute inclination to documenting our lives and letting people know about it on social media platforms results in disregarding the possibility of certain intrusive entities who simultaneously keep an eye on these activities. Secondly, in the absence of physical parameters to judge the loss of the right to privacy, one does not realise it until much later, much like being subjected to a heavy interest post an expensive shopping spree. Also, the comfort supplied by technology-driven e-commerce apps that make our lives easier every moment are difficult to sacrifice once used to, thus making consumers ready to make amends with any dissatisfaction cause due to unwarranted access of personal information. We might be under an impression that financial and other important personal information not disclosed by us on the internet, like bank details, address, passport details etc. are secure enough; we are oblivious of the impending threat. These data can easily be fished out by manipulation.

It is now known that while being connected to free public Wi-Fi networks exposes users to the risk of being sharing information with all other users on that network. Corporates use this opportunity to sieve through messenger conversations and emails to pick up the data that is useful to them. Consumers have been similarly shocked to discover businesses tracking their calls and subsequently being subjected to online ads for articles they have never searched online. One might be speaking to friends about their last holiday trip, only to discover a bunch of related advertisements being suggested. Microphone permissions granted to mobile applications might collect passive non-triggered data which are forwarded to researchers and advertisement network agencies. The use of these applications on the smartphone is not private. The apps are not one's assistant or friend as they may claim, but rather carefully crafted tracking devices. Since it is evident that businesses will continue to passively and actively track data to boost their growth and provide convenience to consumers, it is upon the latter to act more responsibly and act according to some of the discussed ways out to protect privacy.

iii. Do you Really Agree?

For most consumers in general, it is a gruelling task in itself even to discover and understand a company's privacy policy, much less to monitor the company's use of personal information and detect when violations have occurred.

Consumers must start the practice of conscientiously reading privacy policies to understand exactly what they are agreeing to and consequently assess long term consequences of sharing information, as opposed to doing so for instant gratification.

This, however, becomes nearly impossible in cases where companies provide extremely lengthy privacy policies. In such cases, most consumers are left with little choice but to claim that they read something that they actually can't possibly have read. So it would be a good practice on the part of businesses to at least have a brief overview of the contents preceding the mammoth document. The introduction of GDPR already has introduced some effective ways in which privacy policies have to be framed.

iv. Demanding Custody and Control over Data

When consumers are more aware of their data being shared, it gives them more control over it. Consequently, it will lead to a state where consumers will realise the magnitude of their digital footprint and demand custody of their personal data. If personal data is recognised as individual property rights, it will become increasingly difficult for companies to mine and hoard data without the consumer's knowledge. Once the control moves back to the consumers, it might be possible for the consumers to be given the choice to monetize their own personal data from the data trail.

v. Are Government Regulations the most efficient solution to address Consumer Privacy Concerns?

In spite of the explicit set of data protection laws, there is an aggressive erosion of our privacy because of the internet. The European Union, which has been known for having the highest global standards. Ever since the internet was in its nascent stage, the EU had introduced the1995 Data Protection Directive, which has now been replaced by the GDPR.

Several countries have revised their data protection laws to match their standards with that of the EU, except the United States remains which complies with safe harbour agreement during the conduct of business. However, it interesting to note that a January 2001 study from Consumers International has indicated that EU sites in general offer visitors quantifiably less privacy than in the United States, where privacy regulations for the Internet have been largely non-existent. The obvious question that arises here is whether or not government regulation really is the most efficient solution for consumer privacy concerns?

vi. Compelling Businesses to Self- Regulate

When consumers take better control of their personal data and at the same time the media is vigilant about the compromise of consumer privacy, inevitably businesses would be compelled to self-regulate their practices in the apprehension of being exposed of the violation of consumer privacy. Companies would seek to avoid negative attention for the breach of consumer privacy at any cost since it would otherwise lead to great financial loss. Therefore, the better the company protects the privacy of personal data, the lesser negative attention it attracts from the media, and is able to attract and retain more customers.

vii. Is being a Digital Hermit the Only way out to Protect Privacy?

We are now living in an age where passive data tracking technologies have reached an extent where even if one stays off the internet and pledges not to use social networks and does not use a smartphone, even then their data are being continuously monitored and analysed. At a recent TED conference, a neurophysiologist revealed to her audience how passive data tracking monitors analyse their carbon dioxide emissions to determine their emotions. She has argued that though this system might seem to invade privacy, however, it is good in the long run, since the technology can be put to good use by healthcare providers, high school counsellors and the like, to make the best of what they have to offer. This is a debatable idea and advocates of privacy might not agree with the implications of such passive data tracking and its potential misuse. Therefore, it is for sure that abstaining from the digital world and the

utilities offered by it, is definitely not an answer.

Bibliography

Primary Sources

A. Table of cases

1. *Chance v Avenue A, Inc*
2. *In Re: DoubleClick Inc. Privacy Litigation*
3. *In Re: Pharmatrak, Inc. Privacy Litigation*
4. *Justice KS Puttaswamy (Retd) & Anr vs Union of India & Ors*

B. Table of legislations

1. Cyber Security Law of the People's Republic of China
2. Data Protection Act, 2018
3. Federal Trade Commission Act
4. General Data Protection Regulation (EU) 2016/679
5. Information Technology Act, 2000
6. Personal Information Protection and Electronic Documents Act

Secondary Sources

A. Journal articles

1. A. Joint, E. Baker, and E. Eccles. 'Hey, you, get off of that cloud?' *Computer Law & Security Review*, (2009) 25(3):270--274.
2. Benjamin, R., and R. Wigand. 1995. "Electronic Markets and Virtual Value Chains on the Information Superhighway." *Sloan Management Review* (1995) 36 (2): 62–72
3. C. J. Hoofnagle and J. King. Research report: What Californians understand about privacy online. Available at SSRN: http://ssrn.com/abstract=1133075, September 3, 2008
4. Clark, Eugene and Cho, George. 2000/2001. 'Privacy in an e-business world: a question of balance'. *Journal of Law and Information Science*, (2001) 11: 7–37.
5. Esther Dyson, "Labeling Practices for Privacy Protection," National Telecommunications and Information Administration (NTIA), at http://www.ntia.doc.gov/reports/privacy/selfreg5.htm
6. Fayyad, U.M., Gregory, P.S., Padhraic, S.: From Data Mining to Knowledge Discovery: an Overview. In: Advances in Knowledge Discovery and Data Mining, pp. 1–36. AAAI Press, Menlo Park (1996)
7. FH Cate and V Mayer-Schönberger: "Notice and consent in a world of Big Data" (2013) *International Data Privacy Law*
8. Frohmann, B, "Subjectivity and information ethics." *Journal of the American Society for Information Science and Technology,* (2008) 59 (2):267–277
9. Hesselink, M. W "Towards a Sharp Distinction between B2B and B2C? On Consumer, Commercial and General Contract Law after the Consumer Rights Directive." *European Review of Private Law* (2010) 18: 57–102.
10. Kobsa A. 'Privacy-enhanced web personalization in the adaptive web' Springer-Verlag: Berlin, Heidelberg, (2007); 628–670.
11. Marion Fourcade and Kieran Healy (2017) 15 *Socio-Economic Review*
12. Obradovic, Z., Vucetic, S.: Challenges in Scientific Data Mining: Heterogeneous, Biased, and Large Samples. Technical Report, Center for Information Science and Technology Temple University, ch. 1, pp. 1–24 (2004)
13. Ponnurangam Kumaraguru, Lorrie Cranor, 'Privacy in India: attitudes and awareness', (2005) Proceedings of the 5th international conference on Privacy Enhancing Technologies,pp.243-258, Cavtat, Croatia [doi>10.1007/11767831_16]
14. Privacy on the Books and on the Ground, (2010) 63 *Stanford Law Review* 247
15. R. Gellman. 'Privacy in the clouds: Risks to privacy and confidentiality from cloud computing' (2009) World Privacy Forum.
16. Rajarshi Chakraborty, Srilakshmi Ramireddy, T. S. Raghu, H. Raghav Rao, The Information Assurance Practices of Cloud Computing Vendors, IT Professional, (2010) pp.29-37.
17. Rastogi V, Nath S. Differentially private aggregation of distributed time-series with transformation and encryption, Proceedings of the 2010 ACM SIGMOD International Conference on Management of Data, SIGMOD '10, New York, NY,

USA, 2010; 735–746, [doi:10.1145/1807167.1807247]

18. Rolf H. Weber, 'Internet of Things – New security and privacy challenges' *Computer Law & Security Review* (2010) 26(1): 23-30.
19. Tara J. Radin, "The Privacy Paradox: E-Commerce and Personal Information on the Internet." (2001) Vol. 20, *Business and Professional Ethics Journal*.
20. Tene, O., Polonetsky, J.: 'Privacy in the Age of big data: A Time for Big Decisions', (2012) *Stanford Law Review Online*
21. The Role of Privacy, Security and Site Attributes." *The Journal of Strategic Information Systems* 11 (3): 245–270.
22. Viktor Mayer-Schönberger, 'The Internet and Privacy Legislation: Cookies for a Treat?', (1998)1 *West Virginia Journal of Law and Technology*.
23. Warren, Samuel D. and Brandeis, Louis D. 'The right to privacy', *Harvard Law Review*, IV(5)192–220.
24. Westin AF, 'Privacy and freedom', *Washington and Lee Law Review*, (1968) 25(1): 166.

B. Books

1. Alan R. Simon, Steven L. Shaffer: Data Warehousing And Business Intelligence for e-Commerce (Morgan Kaufmann Publishers, 2001)
2. Andrew D.Murray and Arno Lodder: EU Regulation of E-Commerce: A Commentary (Edward Elgar Publishing, 2017)
3. William Roebuck: Privacy in E-Business: Promoting respect, trust and confidence in your organization (BSI, 2004)

C. Websites

1. 'B2C Marketing- Most consumers find marketing personalisation creepy' accessed on March 6, 2019.
2. Ariel Schwartz, 'Forget Facebook - Your Body Emits Data That Could Be Used To Read Your Emotions, Check Your Health, And Track Aggression' (*Business Insider*, 2018) accessed 6 March 2019
3. Matt Ariker, Alejandro Díaz, Jason Heller, and Jesko Perrey, 'Personlizing at scale', accessed 6 March 2019.
4. 'Publications - Consumers International' accessed 6 March 2019
5. Sam Nichols, 'Your phone is listening and it's not paranoia', accessed 6 March 2019.
6. Simon Hill, 'The History of Cookies and their effect on privacy', accessed 4 March 2019.

Bibliography

- 'Apple users pay more for hotel rooms' < http://www.spiegel.de/wirtschaft/service/datenauswertung-bei-orbitz-apple-user-zahlen-mehr-fuer-hotelzimmer-a-840938.html> accessed 4 March 2019.
- Von Shoshana Zuboff, 'Google as a Fortune Teller: The Secrets Of Surveillance Capitalism' (*Faz*, 2016) <https://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-secrets-of-surveillance-capitalism-14103616.html> accessed 2 March 2019.
- Ubiquity: Legal Issues Involved in E-Commerce' <https://ubiquity.acm.org/article.cfm?id=985607> accessed 2 March 2019.
- Tene, O., Polonetsky, J.: Privacy in the Age of big data: A Time for Big Decisions. Stanford Law Review Online (2012)
- Mayor.S.Desai, Thomas.C.Richards and Kiran.J.Desai, "E-commerce policies and customer privacy" Information Management and Computer Security [2003]
- Dan Tynan, 'WhatsApp Privacy Backlash: Facebook Angers Users by Harvesting Their Data' (*The Guardian*, 2016) <https://www.theguardian.com/technology/2016/aug/25/whatsapp-backlash-facebook-data-privacy-users> accessed 4 March 2019.
- 'How Companies Turn Your Facebook Activity into A Credit Score' <https://www.thenation.com/article/how-companies-turn-your-facebook-activity-credit-score/> accessed 4 March 2019.
- Marion Fourcade and Kieran Healy (2017) 15 *Socio-Economic Review*.
- 'Leading Through Digital Disruption' (Gartner 2019) <https://www.gartner.com/imagesrv/books/digital-

disruption/pdf/digital_disruption_ebook.pdf> accessed 2 March 2019.

- 'The rhetoric of "knowledge hoarding": a research-based critique'<https://www.spotx.tv/resources/blog/product-pulse/us-companies-care-pii-non-pii-personal-data/> accessed 2 March 2019.
- 'Why US Companies Should Care About PII, Non-PII, and Personal Data' <https://www.spotx.tv/resources/blog/product-pulse/us-companies-care-pii-non-pii-personal-data/> accessed 2 March 2019.
- 'Big Data: The Management Revolution' (*Harvard Business Review*, 2012) <https://hbr.org/2012/10/big-data-the-management-revolution> accessed 2 March 2019.
- 'Erik Brynjolfsson On Big Data Revolution' (*MIT Sloan Experts*, 2012) <http://mitsloanexperts.mit.edu/erik-brynjolfsson-on-big-data-a-revolution-in-decision-making-improves-productivity/> accessed 4 March 2019.
- Marcia Stepanek, Weblining, Business Week, < https://www.bloomberg.com/news/articles/2000-04-02/weblining> accessed 4 March 2019.
- 'Online Profiling: A Report to Congress' <https://www.ftc.gov/sites/default/files/documents/reports/online-profiling-federal-trade-commission-report-congress-part-2/onlineprofilingreportjune2000.pdf> accessed 6 March 2019.
- 'Customer Profile Exchange (CPEX) Working Group' <http://xml.coverpages.org/cpex.html> accessed 4 March 2019.
- Robert O'Harrow, Jr., 'Internet Firms Act to Ease Sharing of Personal Data', <http://www.washingtonpost.com/wp-dyn/articles/A23676-2000Dec4.html.> accessed 4 March 2019.
- Simone Fischer-Hübner, IT-security and privacy: design and use of privacy-enhancing security mechanisms, Springer-Verlag, Berlin, Heidelberg, (2001)
- Rolf H. Weber, 'Internet of Things – New security and privacy challenges' Computer Law & Security Review Volume 26, Issue 1, January 2010, Pages 23-30
- Renaud K, Gá Andlvez Cruz D. Privacy: aspects, definitions and a multi-faceted privacy preservation approach, Information Security for South Africa (ISSA), 2010, 2010; 1–8, doi:10.1109/ISSA.2010.5588297.
- Westin AF, 'Privacy and freedom', *Washington and Lee Law Review* 1968; 25(1): 166.
- 'Emerging E-Commerce Technology Trends - Netscribes' (2018) <https://www.netscribes.com/ecommerce-technology-trends/> accessed 2 March 2019.
- Radomirovic S. Towards a model for security and privacy in the Internet Of Things, *1st International Workshop on the Security of the Internet of Things*, Tokyo, Japan, 2010; 1–487.
- Kranz M, Roalter L, Michahelles F. Things that Twitter: social networks and the internet of things. In What can the Internet of Things do for the Citizen (CIoT) Workshop at The Eighth International Conference on Pervasive Computing (Pervasive 2010), 2010.
- 'Apple users pay more for hotel rooms' < http://www.spiegel.de/wirtschaft/service/datenauswertung-bei-orbitz-apple-user-zahlen-mehr-fuer-hotelzimmer-a-840938.html> accessed 4 March 2019.
- Toch E, Wang Y, Cranor LF. Personalization and privacy: a survey of privacy risks and remedies in personalization-based systems. User Modelling and User-Adapted Interaction 2012; 22(1): 203–220, doi:10.1007/s11257-011-9110-z.
- Orgill G, Romney G, Bailey M, Orgill P. The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems. In Proceedings of the 5th Conference on Information Technology Education, CITC5 '04. ACM: New York, NY, USA, 2004; 177–181, doi:10.1145/1029533.1029577.
- Spiekermann S, Cranor L. Engineering privacy. IEEE Transactions on Software Engineering 2009; 35(1): 67–82, doi:10.1109/TSE.2008.88.

- 'Social networks scan for sexual predators, with uneven results' (2012) Available at http://reut.rs/Nnejb7 (Accessed 2013-02-07).
- Kobsa A. Privacy-enhanced web personalization. *In The Adaptive Web*. Springer-Verlag: Berlin, Heidelberg, 2007; 628–670; Spiekermann S, Cranor L. Engineering privacy. *IEEE Transactions on Software Engineering* 2009; 35(1): 67–82, doi:10.1109/TSE.2008.88.
- Rastogi V, Nath S. Differentially private aggregation of distributed time-series with transformation and encryption, Proceedings of the 2010 ACM SIGMOD International Conference on Management of Data, SIGMOD '10, New York, NY, USA, 2010; 735–746, doi:10.1145/1807167.1807247
- A. Joint, E. Baker, and E. Eccles. 'Hey, you, get off of that cloud?' Computer Law & Security Review, 25(3):270--274, 2009.
- 'Right to Privacy' <https://www.constituteproject.org/search?lang=en&key=privacy> accessed 6 March 2019.
- Personal Data (Privacy) Ordinance (Cap. 486 of the Laws of Hong Kong) (Ordinance).
- The Privacy Act 1988
- Privacy Act 1993
- <https://cis-india.org/internet-governance/publications/privacyapproachpaper> last accessed March 06, 2019.
- 'Right to Privacy'< http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm> last accessed March 06, 2019.
- *Justice KS Puttaswamy (Retd) & Anr vs Union of India & Ors* [2017] Writ Petition (Civil) No 494 of 2012 (SC).
- 'Personal Information Protection And Electronic Documents Act' <https://laws-lois.justice.gc.ca/eng/acts/p-8.6/> accessed 6 March 2019.
- 'The History Of Cookies And Their Effect On Privacy' (Digital Trends) <https://www.digitaltrends.com/computing/history-of-cookies-and-effect-on-privacy/> accessed 4 March 2019.
- 'How Internet Cookies Work' <https://computer.howstuffworks.com/cookie.htm> accessed 5 March 2019.
- 'Learn The Maximum Size That A Cookie Can Be' (2019) <https://www.lifewire.com/cookie-size-limit-3466810> accessed 5 March 2019.
- Lawrence Jenab, '*Will the Cookie Crumble?: An Analysis of Internet Privacy Regulatory Schemes Proposed in the 106th Congress*', 49 U. KAN. L. REV. 641, 648 (2000)
- 'Getting The Message: How the Internet Is Changing Advertising' (*HBS Working Knowledge*, 2000) <https://hbswk.hbs.edu/item/getting-the-message-how-the-internet-is-changing-advertising> accessed 6 March 2019.
- Viktor Mayer-Schönberger, 'The Internet and Privacy Legislation: Cookies for a Treat?', 1 *West Virginia Journal of Law and Technology* (1997)
- Jonathan Stearn, 'The 10 Common Myths of Cookies, Computer Fraud' [1998] Computer Fraud & Security.
- Eric Davis, 'Despite The GDPR, Cookies Are Vital To Ecommerce | Practical Ecommerce' (*Practical Ecommerce*, 2018) <https://www.practicalecommerce.com/despite-gdpr-cookies-vital-ecommerce> accessed 6 March 2019.
- Schermer, B. W., B. Custers and S. van der Hof. 2014. The crisis of consent: How stronger legal protection may lead to weaker consent in data protection. *Ethics and Information Technology* 16 (2):171–182.
- Stein, Alex and Porat, Ariel, *Tort Liability under Uncertainty*, Oxford University Press, December (2001).
- 'A New Millennium Dilemma: Cookie Technology, Consumers, and the Future of the Internet' < http://via.library.depaul.edu/cgi/viewcontent.cgi?article=1253&context=jatip > accessed 6 March 2019.
- Tara J. Radin, "The Privacy Paradox: E-Commerce and Personal Information On The Internet." (2001) Vol. 20, *Business and Professional Ethics Journal*.
- 'Personalizing At Scale' (*McKinsey & Company*, 2015) <https://www.mckinsey.com/business-functions/marketing-and-

sales/our-insights/personalizing-at-scale> accessed 6 March 2019.

- 'Analysis of Mary Meeker's Internet Trends Report 2018.'<https://www.clickz.com/analysis-of-mary-meekers-internet-trends-report-2018-part-1/214833/> accessed 6 Mar. 2019.
- 'Accenture 2018 Personalization Pulse Check Report' <,https://www.accenture.com/t20161011T222718__w__/us-en/_acnmedia/PDF-34/Accenture-Pulse-Check-Dive-Key-Findings-Personalized-Experiences.pdf> accessed 6 Mar. 2019.
- Goldman, Eric, The Privacy Hoax, Forbes, 10/14/2002, Vol.170 Issue 8, P42
- 'B2C Marketing- Most consumers find marketing personalisation creepy' <https://www.cebglobal. com/blogs/b2c-marketing-most-consumers-find-marketing-personalization-creepy/> accessed on March 6, 2019.
- 'Your Smartphone is leaking your information'< https://www.youtube.com/watch?v=2GpNhYy2l08> accessed 6 March 2019.
- 'Your phone is listening and it's not paranoia', <https://www.vice.com/en_in/article/wjbzzy/your-phone-is-listening-and-its-not-paranoia> accessed 6 March 2019.
- Sandra Wachter, 'Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR
- 'The History Of The General Data Protection Regulation - European Data Protection Supervisor - European Data Protection Supervisor' (*European Data Protection Supervisor - European Data Protection Supervisor*) <https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en> accessed 6 March 2019.
- 'Publications - Consumers International' <http://www.consumersinternational.org/news/pressreleases/fprivreport.pdf> accessed 6 March 2019.
- 'Forget Facebook - Your Body Emits Data That Could Be Used To Read Your Emotions, Check Your Health, And Track Aggression' (*Business Insider*, 2018) <https://www.businessinsider.in/Forget-Facebook-your-body-emits-data-that-could-be-used-to-read-your-emotions-check-your-health-and-track-aggression/articleshow/63738872.cms> accessed 6 March 2019.
- M Hysing ،Pallesen, S. et, all. Sleep and use of electronic devices in adolescence: results from a large population-based study. BMJ open,5(1), e006748. (2015).
- Olivia solon. smartphones wont make your kids dumb- we think. Scientific American. (2016),https://www.scientificamerican.com/article/smartphones-won-t-make-your-kids-dumb-we-think,
- Fatima Al-Saadi, The Child and Electronic Games Through New Media, Between Entertainment and the Impact of Influence, First Edition, (Amman: Dar Al-Khaleej, 2018), p. 116
- Harwood, J., Dooley, J. J., Scott, A. J., & Joiner, R. (2014) ,constantly connected–The effects of smart-devices on mental health. Computers in Human Behavior,. 34, 267-272.
- Cain, N., & Gradisar, M. (2010). Electronic media use and sleep in school-aged children and adolescents: A review. Sleep medicine, 11(8), 735-742.
- Bar-On, M. E., Broughton, D. D., Buttross, S., Corrigan, S., Gedissman, A., De Rivas, M. R. G., & Hogan, M. (2001). Children, adolescents, and television. Pediatrics, 107(2), 423-426.

***