CS978 Legal, Ethical And Professional Issues For The Information Society Coursework Assignment

Group 23

Academic Year 2021/2022

Table of Contents

The Task (Will Be Removed Before Submission)

Brief

- 'White Paper' for compsci professionals
- Privacy: *legal* and *ethical* issues
  - Employer duties (to employees, field, society)
  - Employee duties
- Subset target? (data science, software engineers, etc.)
- 30%: Ethical issues
- 30%: Legal issues
- 30%: Background research
- 10%: Structure

Subset: Health Sector

- Fitness (voluntary / non-voluntary):
  - Strava, Garmin & Apple Watches
  - Social Media Image / Activity Sharing
- Health Care (mandatory / necessary):
  - Medical Records
  - Machinery & Data Recording
  - Social Media Surveilence (who's in need of what? e.g. Facebook sell)
- Health Insurace (mandatory / forced disclosure?):
  - Using pre-existing conditions against you
  - Using others' conditions against (e.g. husband not vaccinated, insurance up)

1 Introduction

1.1 Ethics & Legality of Morals

An ethical understanding is critical when considering how corporate bodies behave towards their employees and consumers, in the modern era. Ethics, whether conciously or unconciously, are a huge driving force in decision making amongst how corporations interact with thier networks throughout governings, industries, societal norms, culture etc. Thus, ethical reflection of corporations and people often defines who or what that body is and how they're perceived by society. For industries to be in harmony with their consumers' needs and desires, there must be a common goal saught between them, defined by ethical principal (Chonko, 2012).

1.2 Information Society Era

In modern times, information is exchanged and utilized technologically on an immense scale. Meaning it's more valuable than ever. Corporate bodies in the *information society* rely so heavily on the acquisition of information/data to simply continue to offer new and innovative solutions to their consumers (Chonko, 2012). This generally leads to consumer data being collected voluntarily (forced/unforced), or non-voluntarily (conciously/unconciously), which each carry thier own weight when considering the ethics of how each of those four viens may impact consumers and indistries on a whole. It could be argued that it is at this point were the legal-ethical trade-off of *duties to society and duties to industry* must be made (Martin, 2016).

Digital ethics are considered one of the most important indicators of tracking how we adopt our ethical standpoint to account for constantly developing technology. In a society which is fully 'connected', life becomes more and more dangerous when considering the uncountable amount of new data being produced and stored by developing technologies. However, it is how corporations and governing bodies decide to interact with this data and the management of such which often determines just how safe people are 'online' (Martin, 2016). Thus, poor decision making by these bodies, or consumers, can lead to something which was designed to enhance a consumers life becoming hostile. Spinello (2017) highlights the point that business is shifting from developing an understanding of consumers, to invading their information and privacy for a more synthesised understanding. Hence, the argument of *consumer relationships (ethical relationships and trust) vs. competition (in the context of big-data use and 'who gets there first')* for

corporate advantage becomes apparent.

1.3 The Health Sector

Many ages ago, the health sector was on the far more pragmatic end of the scale when it came to data collection, use and governing. However in this information society, everything has a value, meaning every microscopic detail about an individual could be of interest to someone, somewhere. So forth, this white paper explores the subsectors of the modern health sector, such as the fitness industry, health care providers, and insurers, etc. It highlights areas in which moral decision making and privacy may no longer be respected and/or governed in an appropriate or traditionally saught manner, when considering current uses of information technology and data. Bodies in this area must find the correct balance of responsibility fulfilment to their consumers and to reducing negative impact on industry and society as a whole.

2 Ethical Theory

Each individual has their own outlook upon ethics, known as their ethical principals. The way they choose to aggregate these, within themselves, society, their industry, and their decision making surrounding their responsibilities is known as their ethical application (Sandel, 2009). Principals include *beneficence*, *least harm*, *autonomy*, and *justice*. The application of these principals often removes the opportunity for grey spaces in legal boundaries of how society interacts.

2.1 Values & Principals

2.1.1 Beneficence

Beneficience is known as the objective factor which distinguishes right and good from wrong and bad (Kinsinger, 2009). That is, *what is the right thing to do?* regarless of how you feel and who else it could benefit. It's often associated with a feeling of moral obligation when one individual considers another. For example in a professional environment, the professional should always have the central interest of objectively doing the right and best thing to benefit a client and satisfy their needs. This particularly applies to the context of this white paper which focuses on the health industry, in which the outcome of the client's condision and position in society is ideally the driving force. As we know however, other not so morally-focused influences can take over. It's said that if a professional fully applies beneficence, especially in the health sector, any failure succeeding consultation with clients are purely the result of nature (Kinsinger, 2009). This is very much a 'greater good' factor.

2.1.2 Least Harm

There are often scenarios in which there is no apparent 'right' or 'wrong' option, which is where the professional (or any other individual) must make the decision through the lens of the rule of *least harmful impact* (Chonko, 2012). Much like in Game Theory where a move may negatively impact all the leader, follower and industry but there is no other move. Thus, under the idea of least harm, the decision must be made in which the negative margins are lowest, as many individuals believe it is more important to do as little harm to as many people as possible than it is to do good to fewer people. This creates the argument of *aggregate utility vs. individual payoff* (Jahn, 2011). That is, could it be more beneficial in the long-run to maintain a greater amount of people at an even level of utility? Or, would there be opportunity for exponential growth if

you decide to favour the benefit of a smaller amount while others are more significantly impacted?

2.1.3 Respect for Autonomy

There is a common mindset in particular circumstances that it's 'everyone for themselves'. To a degree having respect for autonomy accounts for the most practical elements of this belief. Being self-governing can be extremely beneficial at certain times, provided the correct knowledge and understanding is in place. Jahn (2011) argues that, much like legalization of things such as firearms, when bodies have the correct intentions, understanding of impact on themselves and others, and are not influenced by any external body or motivator such as money or power etc., autonomy is an extremely effective way of governing society into being truthful, respectful of privacy of others, respectful of confidentiality, and understanding of consent. This of course, relies on every idividual being equally as competent. The idea that people know themselves the best is usually true and given the right circumstances, if everyone fairly acted on their own behalf for their own payoff, aggregately everyone would theoretically benefit. However, the governing of people into this philosophy is far more difficult than ideal. For example, in an ideally autonomy-respecting world, you would expect every individual to have a perfect understanding of their experiences, motivations, capabilities and emotions (Chonko, 2012). Thus, people should learn how to act upon these factors, creating a more harmonious and understanding world. In this idea world in the context of the health sector, every individual would have a perfect understanding of their 'statistics' and the unethical sharing of user data / medical records etc. would be redundant as any product generated from the data would be attempting to make a user make decsions they already feel confident enough to make.

2.1.4 Justice

Justice. The most objective of them all. This factors is very similar to Cost-Benefit Analysis (CBA) in the sense that it accounts for long-term impacts on individuals and society and whether the net present value of future possible payoffs is great enough to justify any possible immediate costs and future costs to society. Jahn (2011) suggests that the purpose of taking a justice approach is to equally distribute costs, benefits, risk, and resources across society as a whole. Thus, decisions made with justice involved should ensure that the outcome is fair to all parties in-the-know and fair to external parties also (society) just of course, not with the same payoff. In an argument of Jahn

(2011), decisions considering justice should: equally payoff to parties involved and, equally cost parties involved. However, these are bound to the relative parameters of each party's effort, each party's contribution and, each party's merit. That is, people should get out what they put in, in the long-run. A direct contrast to this idea is particularly apparent in situations where corporate bodies may favour individuals with more promise in their characteristics and habbits (i.e. payoff *now* to the corporate) and thus, target them with benefits as opposed to more loyal long-term consumers.

2.2 Application of Ethics

The discussed values and principals of ethics are promising when viewed objectively however, there are multiple frameworks under which they must be applied in order to be functional and effective. These include *conseqentionalism and utilitarianism*, *deontology*, *rights*, and *virtue* (Chonko, 2012).

2.2.1 Consequentionalism & Utilitarianism

Consequentialism relates to the human aspect of decision making through which an individual considers each outcome of a decision and the present value of any future decisions which may arise due to the current one. Thus, on many occasions people may forced to be overly 'predictive' in their decision making (Lloyd, 2019), leading to possible human bias. Therefore, someone who's considered a 'consequentialist' generally makes decisions which produce the objectively greatest consequences. That is, what's 'right'.

It's argued that consequentialists don't generally consider the path towards their best outcome, meaning they're often prepared to lie, bend the truth, or create their own set of circumstances if it means their idea of the best consequences were to be achieved through doing so. By adopting this mindset, a 'utilitarian' approach is developed. This is simply defined as where decisions are made with bias towards the greatest amount of benefit of the greatest number of people (Lloyd, 2019). Hence, if benefiting a great number of people causes a significant cost to a little amount, or an average cost to a great amount of people, the utilitarian approach will still be favoured.

Objectively, you may think that benefiting the greatest number of people would have the best effect on society as a whole but unfortunately, each utilitarian individual makes decsions based on different sets and views of well-being (Lloyd, 2019). This means what

they see as the best outcome for everyone may not actually be so, in the eyes of the receivers. As a result of this and components alike, many utilitarian decisions made could lead to immoral consequences for those who will always be negatively impacted and, those who may be believed to be getting the benefits but actually are not.

The classic example of digital activity monitoring is present here. Such as a scenario where-in a ogvernment wishes to track criminals through various algorithms which monitor browser searches, chatroom conversations, cookies, etc. The argument of a utilitarian is that having a governmental body survey this type of content, society is better off as a whole as there is a chance of reducing criminality. However, in that path to achieving this, data of harmless users has been gathered which then creates a whole new vein of ethical trouble where this information could be at risk of breach, misuse, or sale etc. Thus, maybe locking up a few criminals will help keep a portion of society 'safer' in the medium-run however, the digital issues that many harmless consumers may run into may result in long-term harm by the act of future hostility or cyber-criminals. Cost-Benefit Analysis must be applied to weigh-up the present values of all outcomes.

2.2.2 Deontology

Deontology takes into account a clearly specified or understood set of rules, standards, conventions, and such alike when decision-making (Chonko, 2012). It literally means there is an obligation to adhere to necessities. In the field of ethics, this is often seen where individuals hold themselves accountable to their 'obligation' to follow the societal belief of what it 'ethically correct'. An individual with attributes associated with this theory may tend to find decision making easy as they're driven by their own inner beliefs. However, this attitude can fail to hold on a more macroscoping level, for example: corporate, as its principals may not be easily transferred. That is, not everyone has the same perspecive on 'good' and 'bad'.

Of course, this approach is expremely variable based on the mental capacity and well-being of individuals associated. There is often very little logic and rationale considered in the decision making of extremely emotional or incapacitated indiviuals, for example. This means that although they may believe the decision they're making is 'correct' or 'fair', their perspecive may be so skewed that the benefit of the outcome to any indiviual/body is little or negative. Hence, decision making can be very linear in this

context. For example in the digital era, a developer may see it as their 'ethical obligation' to enforce security around an application. However, for whatever specific reason, over-development of this may cause lack of functionality in other places, higher costs, etc. Thus, much of the decision making process can be in favour of personal interest and beleifs and may ignore much of the path to fulfilment for the greater numbers or overall task at hand.

2.2.3 Virtue & Rights

The theory of virtue suggests that, unlike previous branches, some individuals can be judged primarily based on their character, as opposed to their acts or physical decisions (Chonko, 2012). This scope relaxes the outlook upon how observable emotion reflects upon people. Thus, it is arguably the most difficult of the series to quantify as a large sample of people may have very skewed subjective perspectives upon an individual's beliefs, morals, thoughts, reputation and motives. It's in cases like this that, for example, even people closer to and more understanding of certain individuals will likely have a greater judgement of their future acts. This also isn't a linear equation; people change, meaning even if this method was quantifiable, there would be huge difficulty in accounting for volatility. This aspect of ethics is difficult to convey in the digital era however, as the industry is heavily dominated by pragmaticism and even highly emotional people still must convey physical (judgeable) acts in it.

This theory ties-in heavily with the concept of 'rights', where outlook upon entitlement may differ with personality. Many people may have a clear idea of trade-off and exchange of rights. For example, if one person performs an act of favour in benefit of another person, they may have their own quantification of its worth, in their mind. Thus, they expect some sort of entitlement in return, perhaps unmatched by the second party. It's cases like this in which professional approaches differ regarding what people believe a consumer is due.

3 Morals of Accessability

As we recall, this white paper specifically explores the *health sector* and associated industries, including: the *fitness industry* (mobile technologies, devices, social media, etc.); *health care* (medical records, machinery and data recording, social media surveilence, etc.); and *health insurance* (leverage, pre-existing conditions, conditions of others, etc.). This section explores ways in which moral or legal issues could be encountered in the operations of each of these areas.

3.1 Restrictions

3.1.1 User Freedoms & Expression

The fitness industry is generally a place where user expression is welcomed and encouraged to drive motivation and competition. Thus, software such as GPS apps, social apps, GPS watch technology, etc., is regarded some of the most 'freeing' technology of the modern age. Much like the modern action taken towards land access and tourism, fitness software encourages free expression under the belief that 'everyone is part of nature', seeing that people willing to support such a lifestyle have enough integrity to ensure they practice their opinions and expressions in a respectful manner. There is little room for, what is considered 'rightfully restricted content', such as hate crime/speech, terrorism, etc. in this mode of interaction (Barendt, 2006). Hence, the very minimal tolerance by the community of such behaviour; almost adopting a communal deontological approach, where there is a mutual alignment of 'right and wrong'. Thus, an obligation to preserve the nature of the community and industry, and a common support of local rights and virtue. Barendt (2006) argues that freedom of expression is essential for accountability, and that is exactly apparent in this case. People have a common democratic goal which can aid in pinpointing outliers; in effect, sustaining a healthy society.

3.1.2 User Access & Content Filtering

Access to social media begins with accepting the terms and conditions (T&Cs) and privacy policy of the platform, without which one can't gain access to the service. One important factor to look at here is the relationship between social media companies and their users, and how these companies communicate their terms and conditions, which contain important information about user data processing. It is often the case

that T&Cs and privacy policies are excessively long and use complex and technical language, which makes them difficult to understand for the average user and deters them from reading them thoroughly. This often results in users just accepting the terms and conditions without fully understanding how their information is being collected and used.

The main question here is: do users fully understand the terms and conditions they're agreeing to and, do companies consider this when designing them? Users seeking convenience will glance at the terms and reluctantly accept them, as it would be too burdensome and time consuming to read through pages of legal jargon. Here, the convenience that social media provides contrasts with the complexity of the T&Cs, which are obligatory to accept in order to use the service. However, not using social media would not be an inconvenient for a lot of people who rely on these services to socialise and remain in contact with family and friends.

To demonstrate this scenario, an experiment by Obar and Oeldorf-Hirsch (2018) found that 75% of respondents skipped the privacy policy when joining a fake social media site called Namedrop and immediately selected the"quick join" option as participants found them to be a "nuisance". The experiment also found that 98% of the participants didn't notice several important sections of the terms and conditions regarding data privacy, some which even stated that users must present their first-born child as payment for using the service. This makes it evident that the lack of clear, user-friendly language could be the issue. It may lead to information overload that discourages users from reading the T&Cs and being adequately informed about the conditions surrounding their online privacy in relation to the services they choose to use. Although accepting the terms may legally constitute consent, its in most cases debatable how informed that consent is. Arguably, social media firms must design terms and conditions and privacy policies that exhibit full transparency in order to equip users with sufficiently clear information to enable them to make informed decisions and know the full extent of how their data is used.

3.1.3 Online vs. Real Freedoms & Access

More social media-based.

3.2 Malware & External Intrusive Action

3.2.1 Types of Intrusion

As many modern fitness services, such as Strava and Garmin Connect, are highly rear-end based, user data is at great risk of breach. Much data associated, such as personal details, is volunteered simply to make the technology functional however, there seems to be just about no limit to data recording of user attributes. From GPS, to heart rate, to sleeping mechanics, to what time of day you ride a certain route; if the user is even slightly unaware of any of this (i.e. terms and conditions documents are an afterthought to the user), much of this data recording may be considered non-voluntary. Attackers value this type of data greatly as it's the literal breakdown of a human being. Thus, alongside the enormous databases, which are recording data about users a thousand times a second, comes huge corporate responsibility for implementing proper security systems. Any form of malicious attack or misuse of data in this case is particularly unethical as such raw data could be used to harm such a wide variety of aspects upon a person's life.

3.2.2 Impact on User

...

3.2.3 Corporate Response

In the use of modern fitness technology, it's arguably more important than ever that the providers make it extremely clear what users sign-on for. User awareness is vital for rational decision making and it could be argued that full disclosure and trust in the correct (but hard to identify) users would create create a respect for autonomy (Aycock, Sullins, 2010). This could possibly lead to users being more knowledgable of and better equipped to deal with attacks on their data and, providers better-understanding what users value the most out of the use of their data.

3.3 Corporate Responsibility to Consumers, Field & Society

Generally, we would argue that there are three primary types of information exchange: *voluntary* (user chooses to disclose more information, often to enhance features or expe-

rience of the service); *mandatory* (perhaps necessary for service to function, or required for user identification); and *non-voluntary* (perhaps forced or stolen). We see that the fitness industry often claims user information is either voluntarily collected or collected out of functional necessity.

...

4 Privacy & Regulation

4.1 Corporate Data Misuse & Privacy

4.1.1 Social Media & Information Volunteering

As technology and the use of social media have become more ubiquitous, the data we provide about ourselves has become more and more valuable to companies for a number of reasons such as marketing, advertising and research. Besides personal information, there is also so much behavioural information contained in our activities on social media platforms such as what we like, what we share, what we post about ourselves, our opinions on current affairs etc. Most social media users aren't fully aware of how platforms use that information or what other third parties they share it with. This data can be coupled with artificial intelligence (AI) algorithms to spot certain patterns that reveal more information about the user and create a fuller profile of them. A recent development within AI is that it can convert personal user data into "Emergent Medical Data" which Mason Marks, a health law professor at Gonzaga University describes as "health information inferred by artificial intelligence from otherwise trivial digital traces" (Marks, 2021).

Such algorithms have already been deployed by companies such as Facebook, who in 2017 created a "suicide detection algorithm" in an effort to prevent suicide. Using this algorithm, they gathered user mental health data from Facebook activities and posts, which they then used to make assessments about their mental health state and their propensity to commit suicide, referring serious cases to trained professionals (Holpuch, 2018). This was particularly concerning from an ethical perspective as Facebook did not make users aware of this algorithm and didn't give them the option to opt out, thus infringing on their right to privacy and to exercise autonomy about how their data is used. This was a situation where the law failed to protect user privacy as in the case of the US, the algorithm fell outside the scope of HIPPA which only covers patient data held in patient records by medical institutions and insurance companies.

Further more in contrast, this Facebook algorithm wasn't launched in the EU amid concerns it would violate the General Data Protection Regulation (GDPR). GDPR was introduced in May 2018 with the purpose of giving Internet users wider legal protections when it comes to privacy and more control over how their personal data is used. This was a significant step in preserving the human right to privacy in the current

digital age where personal data is more valuable than ever to companies. Although one could see the potential benefits of the Facebook algorithm to save lives and offer help and support to those that need it, there's valid concern over how this highly sensitive data could be misused or exploited by companies or third parties that gain access to it. It also showed the lack of transparency some companies like Facebook can have with their users regarding data gathering and processing. In addition, Laws concerning data privacy seem to lag behind technological innovations in some places and are not evolving at the same pace, leading to situations where current laws are not sufficient to protect user privacy.

4.1.2 Information Record Keeping

...

4.1.3 Information Communication & Sale

...

4.1.4 Information Use & 'Tailored' Products

...

4.1.5 Information Gathering to Help the User or Company?

...

4.1.6 Digital Footprint & Being 'Forgotten'

...

4.2 Basic Intervention

Often bodies fail to match what is legal with what is ethical. Therefore, over the course of the 80s, 90s and 00s, various legal acts were issued to attempt to combat the misuse of current loopholes in the growing digital environment.

4.2.1 The Data Protection Act 1998

The Data Protection Act aims to protect primarliy large databases of data held by institutions such as large corporations or, in this case, medical bodies in order to

better-insure proper use of user data. It sees that the 'data controller' (institution) is fully transparrent with users about who they are and what they do, what they intend on using data for, and who may view the held data. The act also ensures that data should only be acquired if the intended use is law-abiding; it sees that data should be relevat to its intended use and should not exceed requirements; it sees that any out-of-date or unrequired data should be removed from storage immediately, and data should not be retained if it is no longer required by the controller. Finally, it ensures that any wrong-doing by the data controller is met with relative compensation to the user. We can see why in black and white this is useful however, it has its deep contraints. The ethical constraint to the users here however, is based on how institutions decide to disclose these requirements, perhaps making it un-user-friendly for institutional benefit.

4.2.2 The Computer Misuse Act 1990

This act is another which is extremely relevant to this context. It again, is very 'legal' and does not account for many behavioural and ethical aspects around how institutions and individuals will interact with it however, the constraints are well justified. This act prohibits any unauthorized access to data stored on machines of another party; prohibits unauthorized access with negligent or harmful intent; and, prohibits unauthorized attempts to make critical changes to a computer network which could cause harm. Again, this is very black and white; it directly prohibits actions and does not even involve the client-side, only the operator-side. This means the margin for ethical mis-alignment between the client and operator (common individuals and institution) is fairly narrow.

4.2.3 Other Acts

Some other similar acts passed include the Copyright, Designs and Patents Act 1988, the the Freedom of Information Act 2000 and Creative Commons Licensing. these are not particularly relevant here however. As they either apply to more intangible aspects which arent directly related to the issue at-hand or, they account for far too general circumstances in which ethical grey areas tend not to be present.

4.3 Use & Morals of Government Intervention

4.3.1 Government Access to & Use of Information

Arguably the largest area of legislative requirements surrounding the use of data lies with goverment surveilence. This accounts specifically for data acquired in the context of the health industry, and far beyond. The biggest concern of society in this aspect of privacy is around what governments want data of their citizens for. Majorly, it's argued that government surveilence is primarliy used for macroeconomic payoffs. This for example, could be from gathering behavioural data about the people of a town and how they travel; monitoring road cameras, using personal satellite navigation data etc., to decide where to build new roads, new fuelling stations etc. Although many governemnts argue that this is harmless as it also benefits civilians, many say if there is no critical requirement for the government to servey, they should not. This may extend to the belief that governments should only intervene if they have observed possible threat or harm; of course, many believe governments should not intervene at all when it comes to personal data. The parameters of these practices however, can be vague and awkward, especially when it comes to genuine duties of governments such as protecting civilians from crime, terrorism and other harm.

4.3.2 Safety vs. Intrusion

As well as involvement in the direct use of data, governemnts also have an important role of deciding, on a larger scale, who is using data and the way in which they can use it. Many other conglemrates and large firms have the ability to significantly alter people's lives by using their data for protection and the user's benefit etc., for intrusive action and personal gain or wrecklessly; allowing leaks etc. The governemnt must also decide how much they wish to be involved in the surveilence of this data. Legislation such as the Investigatory Powers Bill adresses issues relevant to this by, for example, regulating and observing internet browser data sored by the operating firms, and regulating product releases to align with governemnt data surveilence (Griffin, 2016). In some sense, governements may see themselves as adopting a utilitarian approach where they see stopping crimes and terrorism as a top priority and it doesn't matter who suffers minor blows on the path there. For example, medical records, health statsistics, etc., are often excellent comprehensive indicators of people's abilities and functional paths. Therefore, making it convenient for legal bodies to intercept criminals at vulnerable times. This is just one example of many, of course.

Many people however, argue that the discussed is extremely invasive and it is only in rare occurences that powers such as these are practiced in a completely authentic manner. Therefore, there is no true justification for governments to have these abilities. Thus, there reamins the argument of: do governments play it safe (utilitarian) and cause some people very minor harm to stop potentially enormous, although rare, threats? Or, do governments aim to keep the masses happy but suffer the (perhaps rare) consequences of larger scale threats? On a simple basis, the answer is obvious; protection against crime and terror is objectively far more important than not 'upsetting someone'. However, it's in cases which involve governmental collusion or wrong-doing which create unfair economic benefit to corporations that tend to create the most issues. For example, collusion or manufacturing of monopolies.

4.4 Corporate Responsibility to Consumers, Field & Society

Much of what society recieves from law and legislation relies heavily on the interpretation of such from common individuals. One person's ethical standpoint may differ heavily from another's, meaning that opinion on the purpose of rights and restriction also vary. The purpose of any piece of legistlation, in the health industry or beyond, is to protect and serve. There is a heavy weight on ordinary individuals to understand and properly practice what they're being informed of. Trust in governments, trust in corporations, trust in medical and health industry bodies especially, is extremely important and forms the basis of any ethical relationship an individual will have with thiers. It seems that in many cases in the modern day, society must not express themselves to express themselves, actively hide data just to be neutral, and knwo exactly what it is they;re doing at all times, just to live. So yes, the question sill remains, is that worth it for 'necessary' services and protection (medical, legal, criminal, anything) which not all of society may even benefit from?

5 Conclusions

...

Bibliography

[1] Aycock, J., Sullins, J. (2010). *Ethical Proactive Threat Research.* Workshop on Ethics in Computer Security Research, Pages 231–239

[2] Barendt, E. (2006). *Freedom of Speech.* Oxford University Press, 2nd Edition

[3] Chonko, L. (2012) *Ethical Theories.* The University of Texas at Arlington

[4] Griffin, A. (2016). *Investigatory Powers Bill: 'Snoopers Chapter 2' to pass into law, giving Government sweeping spying powers.*

[5] Holpuch, A. (2018). *Facebook admits it discussed sharing user data for medical research project.* Available at: https://www.theguardian.com/technology/2018/apr/05/facebook-medical-research-data-sharing. Accessed: 24/10/2021

[6] Jahn, W. (2011). *The 4 basic ethical principles that apply to forensic activities are respect for autonomy, beneficence, nonmaleficence, and justice.* J Chiropr Med, Volume 10, Issue 3, Pages 225–226

[7] Kinsinger, F. (2009). *Beneficence and the professional's moral imperative.* J Chiropr Humanit, Volume 16, Issue 1, Pages 44–46

[8] Lloyd, C. (2019). *Religious Studies: Religion And Ethics.* Hodder Education

[9] Martin, D. (2016). *The Internet of Things: A UKeiG White Paper.* UKeiG White Paper

[10] Obar, J., Oeldorf-Hirsch, A. (2018). *.The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services.* Information, Communication & Society, Volume 44, Pages 1–20

[11] Privacy International. (2019). *Your mental health for sale. How websites about depression share data with advertisers and leak depression test results..* Available at: https://privacyinternational.org/sites/default/files/2019-09/Your%20mental%20health%20for%20sale%20-%20Privacy%20International.pdf Accessed: 24/10/2021

[12] Sandel, M. (2009). *Justice: What's the Right Thing to Do?* Penguin

[13] Spinello, R. (2017). *Cyberethics: Morality and Law in Cyberspace.* Jones & Barlett Learning, 6th Edition