How global corporations address Internet privacy within the United Kingdom

Alex Boseley, Michael Bull, Jenish Chandracim

March 13, 2014

1 Introduction

One of the biggest concerns within the digital age is the subject of Internet privacy. As consumers are increasingly adopting online social platforms such as Twitter and Facebook as well as utilizing digital tools such as Google or LinkedIn, many consumers believe that these companies are "collecting and selling an extensive consumer data profile without consumer consent" (McClurg 2003).

The Oxford English Dictionary defines privacy as a "state or condition of being free of disruptions and being observed by other people" (Stevenson 2010). It can be argued that this definition of privacy is somewhat out of place within the 21st century when we refer to online privacy, as people discussing online privacy may expect somewhat more from the concept, such as the right to their data not being distributed without their consent (as opposed to simply not being "observed"). The misnomer of online privacy often leads to consumers being confused with understanding what their rights are when protecting their data and results in many disputes over what consumers think they are entitled to compared to what companies actually provide them in terms of data protection. This claim of confusion was strengthened by Nissenbaum in 2009 who stated that there is "great ambiguity in the way personal information is used", going on to explain that "it can mean sensitive or intimate information, any information about a person, or only personally identifying information". In 2002 Chung and Paynter pointed out that the topic of consumer data protection is a key aspect that online companies should address, stating that "consumers are really interested in the safeguard of their privacy" (Chung and Paynter 2002). This topic of confusion and general responsibility for the consumer as well as the service provider will be discussed greater in the analysis section of the paper.

A more recent and relevant definition of privacy was given by Stein and Sinha in 2002 who defined privacy as "the rights of individuals to enjoy autonomy, to be left alone and to determine whether and how information about one's self is revealed to others" (Stein and Sinha 2002). Reflecting on this quote we can see a fundamental difference in this definition of privacy when compared to a more traditional definition; that difference being "the right to determine whether and how information about one's self is revealed to

others". The authors of this definition believed that the consumer has the right to dictate whether their information is given out and decide the methodology of distributing their information (e.g. maintaining anonymity, removing certain data). Many may argue that this more recent definition of privacy is the one that should be adopted by companies, however encouraging them to adopt such practices can be met with great reluctance as it would be at the expense of the company itself and require a lot of effort to implement the correct set of tools required for online anonymity. One method used to influence organisations is legislation. When the companies must comply with legislation they have no choice but to implement and uphold the standards that the law expects, however this may lead to further complications as many online related laws are somewhat out of date and open to interpretation, a subject that will be addressed later within the analysis section.

The major online corporations discussed within this paper, as well as their Internet privacy policies, consist of leading social media websites and search engines. The social media websites discussed are ones that have millions of registered users and are most likely to have a wide variance of privacy policies, such as Facebook and Twitter. Recent statistics show that Facebook has "one billion, one hundred and ten million monthly active users" (Facebook 2013) and that "17.09% users of Twitter are from the UK" (Twitter 2013). This is a large amount of users and potentially a large amount of data that is being publicly published for everybody to see. This data can easily be collected by the operators of such websites to then be sold to other companies as huge marketing patterns. Social networks such as Facebook and Twitter can be seen as huge data pools by any company looking for information regarding their product or to even utilize the user's information in order to create something that the majority of consumers are interested in. There are no limits to the data published on these sites can be used and even sold for. Social media plays a huge role in how online privacy is perceived and if the leading social media websites have poor privacy settings then what can we expect upcoming web businesses to base their standards upon? This is a question that is explored further within this paper as well as many other privacy related concerns.

Other areas where they may be potential security issues are those we use to handle our most personal requests in return for information on certain subjects. These tools can be addressed as leading search engines such as Google. Recent statistics show "the amount of monthly Google searches to be 12.4 billion" (Google 2013). Google stores these searches in a database with relation to the user who conducted them, meaning that they have knowledge of who and what users are making certain searches and the identity of the user that made them. These websites tend to be the ones we place a lot of trust in as they are handling our most personal requests and store our personal information. For example when somebody is ill Google may be their first place to research symptoms of the illness they are experiencing, this information is extremely personal yet is being processed and stored into a database. Looking at how the United Kingdom specifically addresses Internet privacy and attempts to regulate how companies address the subject, the most prevalent method used is the Data Protection Act of 1998 as its primary concern is that "personal data shall be processed fairly and lawfully" (Legislation.gov.uk 1998). This piece of legislation is a figurehead of online privacy within the United Kingdom and is covered more in depth further into the paper as well as other methods that the government uses to attempt to regulate online privacy.

Legislation is not the only method used in the United Kingdom to combat online privacy threats; independent regulators such as the Advertising Standards Authority (ASA) take an active role in ensuring that web based companies explicitly state when and how they are collecting user's personal information. Many companies use a technique referred to as "Online Behavioural Advertisements" (OBA), this being the method of displaying adverts more relevant to a viewer based on their online behaviour such as search history.

The ASA help to regulate online behavioural advertisements by creating a set of rules that companies must adhere to as well as forcing them to provide tools to opt out of such advertisements. These rules and the opt out feature are summarised on the ASAs official website: "we oversee require businesses to make clear when they are collecting and using information for OBA and require them to provide a tool so that you can choose not to receive it" (Advertising Standards Authority 2013). The effect that the ASA and legislation has on these companies is analysed further on in the paper.

Based on the research it was discovered that the organisations themselves are not solely to blame, but in many cases the users themselves. According to research from Ofcom's Adults media use and attitude report' UK adults concerns regarding online privacy have dropped significantly since 2005, falling from 70% of users to only 50% of users being concerned in 2011. The report also suggests that one reason why concerns are not being taken into account may be because the substantial growth in the amount of time spent on the Internet. The same research shows that 80% of adults now go online on a device regardless of location, a 20% increase when compared to the statistics from 2005.

This paper will investigate how these new global businesses address their consumer's privacy within the United Kingdom and will attempt to understand the methods they use to do so. After understanding how businesses address privacy, we will research into how effective their methods are as well as how the end user ultimately feels about their data, and the ways in which these companies are using it. Finally we will conclude with a comprehensive analysis of the research we have conducted and discuss various suggestions we have regarding the subject. As this paper focuses specifically on privacy within the UK, it will be an in depth look at how citizens of the UK fee these businesses address privacy, we will research into how effective their methods are as well as how the end user ultimately feels about their data, and the ways in which these companies are using it. Finally we will conclude with a comprehensive analysis of the research we have conducted and discuss various suggestions we have regarding the subject. As this paper focuses specifically on privacy within the UK, it will be an in depth look at how citizens of the UK feel about businesses from other countries being trusted with their information when compared to businesses that are operated within the UK itself and therefore comply to UK laws.

The research in this paper consists of various documents discussing the subject of Internet privacy which focus on personal information being captured and passed to third party organisations without the users being made aware of this. As well as academic resources, self-conducted research is included in the form of a Google survey that represents the way various consumers feel about online privacy. This particular piece of research

aids the paper in providing a reliable analysis of how online privacy is currently perceived by consumers. This ensures that the analysis and suggestions provided are relevant at the time of the research being conducted and the paper being written.

2 Methods Used

There are numerous major online organisations that drastically affect Internet privacy with no genuine prior intentions of doing so. This is now often deemed one of the consequences of the technologies such as online social interaction available today, as stated in an article by Mendel et al.: "Understandings of privacy have long been shaped by the technologies available, with early concerns about privacy surfacing with newspapers in the nineteenth century" (Mendel et al. 2012). These are now no longer concerns, in reality privacy issues on social media websites are now becoming something of the norm and there are many explanations as to why this is occurring. One of the reasons these privacy issues are on-going is a newly launched website that is growing at a rapid rate is unaware and unable to effectively deal with privacy concerns that may have risen inadvertently from their choices in design. Once a social media website's user base grows significantly in a situation where the website may be relatively new they must deal with such issues as wanting to find out more about their users thus storing a lot more personal and identifiable information about their users; this is known as data mining. "Recent developments in information technology have enabled collection and processing of vast amounts of personal data, such as criminal records, shopping habits, credit and medical history, and driving records." (Brankovic and Estivill-Castro 1999). This was written in 1999 and fifteen years later this statement is completely amplified due to the amount and type of data that can be collected.

Data Mining is the analysis step of KDD (Knowledge Discovery and Data Mining), where data are collected then processed in large quantities to find specific patterns, essentially collecting and processing a large amount of data to construct readable and structured data patterns to be used. "Data mining involves the collection of massive amounts of data from numerous sources. Next, algorithms look for trends or correlations" (Goss 2013). Due to the nature of these data mining algorithms, for example data that shows potential customer is interested in a holiday to Greece, companies are able to utilise the consumer's data in order to more effectively advertise to them, i.e. showing advertisements for resorts in Greece. Consecutively this data can then be used to start marketing schemes or to help the administrators of social media websites to further develop their website given the data patterns gathered, or give other companies an opportunity to create advertisements that suit the needs of their users in a more exact way.

Not only is the social media website itself going to impose a threat on their own users but websites that are more popular are going to comprise of a minority of people who want to abuse the website such as hackers, and in general a lot more interest to the social media website. All of these consequences mentioned are going to be drawn into a popular website regardless and each and every one will be somehow connected to Internet privacy. This is simply because all of the consequences mentioned have the same

cure which is inevitably allowing the users of these social media website the preference of tightening the ropes on their own privacy settings, whether it is a user is being hacked due to poor privacy settings leading to enough information to be leaked into a hacker's hands via social engineering or similar methods, or whether the social media website starts building profiles on each and every user then selling them or using the profiles for marketing schemes or advertisements.

In the *International journal of information management* Weiss points out that "Social network application provider's benefit from the increasing amount of personally identifiable information willingly displayed on their sites" (Weiss 2009). This will continuously be the case no matter the situation; a majority of users will post their personally identifiable information whether they have privacy settings or not, although privacy settings allow users the decision of who sees this information and how it is processed by the website itself. Every popular social media website is going to progressively start to have enough personally identifiable information obtainable on its users to start marketing schemes that in turn could help them or other websites when it comes to developing new features for their own website or developing advertisements to be featured on their website. In theory social media websites could use the data gathered to know what advertisements to show each and every user of their social media website. This is because other major companies that have products to sell would specifically target the social media website with the bigger user base and the social media website with the most personal identifiable information available on their users. Although the social media website and the companies in question will think this is a great idea as this would increase both of their revenues by a vast amount, they may not think about the users of the social media website and neglect to ask whether the users of the website actually want all of their own personal information to be used to brand products or advertisements.

Not only are the growing social media websites affecting privacy on the Internet but advertising based websites and marketing teams are also making a change to how privacy on the Internet is addressed. This is because advertising websites and major marketing teams are applying far more pressure on social media websites for them to supply enough information to use in marketing schemes, which in turn means social media websites have to make sure all of their consumers/users have enough privacy settings to decide whether they want this to happen with their data. They also have to make sure that they have enough information to send to these data gathering websites and have enough information to create their own information profiles to make their own advertisements or build applications or new websites based on what their current users think/act. It is quite easy for a social media website to gather a lot of information; a social media website has a lot of power when it comes to knowing what their users like simply because their users are consistently posting this information on their website, whether it is what movies they enjoy, where they like to eat or what features they like in a website. All of this information can be used to build specific applications or websites suited to what users have mentioned or published.

After a social media grows and begins to branch out to advertisement companies and adopt social media in-house marketing schemes, the website may see a dramatically less amount of users a year prior to the website taking off and becoming quite popular. This ultimately could mean the privacy settings/options the social media website offered a

year ago may have "fallen off", meaning they do not fulfil the needs of their users due to the nature of how the social media website is using their users' personally identifiable information. The social media website must let them know what personal information is being used and how it is being used. "On its end, Facebook matches the email addresses in Datalogix's systems and compares that to an email address on Facebook. This effectively makes it so they can track if you see an ad on Facebook and then purchase it in a store" (Klosowski 2012). Facebook released a statement mentioning how they are working with certain club card companies using emails that users have signed up to Facebook with and the emails used to register club card contracts. They used this information to link certain users with their respective purchases to see if they were buying the products that were advertised. Although Facebook offered a way of opting out of it, their users were quite oblivious to this practice. Recently a lot of critics have made sure the social media websites are aware that they should always give an option to opt out of personal information collection, simply because not all users want their personal information to be stored regardless of whether it is being used to create products or advertisements or whether the information is not being used at all; any information that is stored online in a database can be used at any time.

This information collected by social media websites may seem like they are the only villain in the crime, but it does not seem to be this way with other companies such as advertisement companies affecting how social media sites go around collecting enough information for themselves and for other companies. The information collected from users of social media website allows the website to create products, websites and advertisements based on the users' personal interests.

There are many different methods that social media websites make use of to build data banks/information profiles on their users; these methods can usually be seen as quite devious behaviour by some users and most critics. These methods normally are used in a way which the user would not recognize that the social media websites they are signed up for are collecting information about them. One relevant example of this practice is Facebook; even if a user of the platform was not using it at the time but had logged into it at one point and then visited a website that has a Facebook extension (ones that allow you to share a webpage or like a page, without being on Facebook), Facebook can log which websites you have visited. This method allows social media websites such as Facebook and Twitter to collect information without the user actually being logged into the social media website. This method is commonly known as "tracking", when you log into a social media website such as Facebook or Twitter it will automatically download a cookie with your Facebook or Twitter user identification number stored in it. This cookie will then be used when you visit a website that uses a Facebook or Twitter extension which simply allows you to like the website or tweet it. The extension will know exactly where to look in your cookies to find out your Facebook or Twitter user identification number and then will store information about the site you have visited without you even being logged into the website. Tracking has been a big part of the World Wide Web for a while now it and easily allows social media websites such as Facebook, Twitter, Google+ and many more to build profiles on what websites their users are visiting.

This method is quite effective as social media websites are generally incorporated within a lot of different websites simply because a majority of websites will have a Face-

book fan page for their own website, it is the general consensus for many websites that using Facebook fan pages can increase their own user base. Therefore many websites will include a Facebook extension liking/comment feature on their homepage or other areas within their domain. The extension allows you to like their Facebook page without actually being on Facebook to do it. This gives users the option of clicking one button rather than logging into Facebook, finding the websites fan page and then having to like it. Although due to this method being quite effective it means social media websites such as Facebook and Twitter can build real time graphs with time stamps of what website their users tend to visit the most. They could use this information to incorporate aspects of the popular sites that their users visit, into their own website. The "tracking" method is quite popular, so much so that browsers such as Firefox and Google Chrome offer settings that send back to the website a "do not track" request with your browsing traffic, which is only a request of which the website may just ignore. There are many browser add-ons that developers have created to stop "tracking" as it is not an issue only related to social media; a lot of major online search engines and shopping websites use this method. This is a brutal method of building information profiles as even a user that is very knowledgeable when it comes to IT may not understand how they are being tracked or even if they are being tracked.

There are many misconceptions when it comes to methods of data mining and how major online corporations such as Google in this case collect data on their users. One of the misconceptions that will be discussed is where the user, whilst installing a piece of software, will overthink the situation and decline the offer of sending data back to the company you are downloading an application from. When you download Google Chrome browser in this case (although many other applications make use of this) there are many installation steps you have to go through before the application is installed on your computer. One of these steps of the installation process of Google Chrome consists of offering you a choice of sending back information send back data to Google, with a line or two explaining how this will send back usage statistics and crash reports. In non-technical terms when program applications have errors or if they crash the code that runs inside of them will catch these errors and log them.

This information is extremely useful for the organisation that created the program application as they can use the information relayed back from the users for debugging and working out all of the errors within the program, this allows a better experience for the users. Although there is a general consensus of people who believe that if they accept this option the corporation will steal all of your personal data which is simply not the case. It does seem like websites have a tendency to hide terms and conditions and keep relatively quiet while doing so, this can often be when they are stealing your personal information. When a website or application program tells you the exact data/information it will be sending back to the company is probably one of the only times you can somewhat trust the application or website's intentions.

3 Effects

In order for end users to understand the importance of online privacy they must be aware of the impact that such issues have on them sometimes without them knowing. As consumers consistently leave themselves open to privacy invasions such as others viewing their social media content, they heighten the risk of various issues outside of the platform itself such as identity theft. These inadvertent security risks are a result of the effectiveness that the platform's privacy options have to offer, which may end up being the uninformed decisions of a simple programmer working for the company.

Social media platforms are a prime example of the user having a lot to lose by participating fully in its available content. By registering something as sensitive as your locational information or as trivial as your favourite bar the experience offered by the platform itself grows by offering new content such as finding a place to eat close by or checking what time the movie you want to watch is on, however such improvements come at the cost at potential security breaches; if someone is able to access the user's account or simply has observable access to such information, be it through the user's own privacy settings or a breach of the platform's security, it can be an incredibly large security threat that the user may not have considered when initially signing up and entering their information in the hope of an improved content experience.

Information that major online corporations, specifically social media websites can collect in a very short amount of time, is very advantageous for the developers and analysers of that website. The analysis of these websites can use this information to build patterns of data which could be used to further develop their website, as they are constantly on the receiving end of user feedback without even asking for any; this is due to how everything posted on a social media website is in real time and normally consists of what the user is actually thinking, this puts social media websites in a very good position. Not only can this information be used to further build and develop their own website but can be used in a way that helps advertisement companies develop their advertisements, as a result of data mining algorithms the analysis of these social media websites can process vast amounts of data that then can be turned into structured patterns used to produce the most effective advertisements.

4 Analysis

In order to effectively review the way that corporations address privacy we must first understand how consumers themselves feel about the subject and begin to understand their opinions on the matter. With this in mind, this section will now discuss and assess research performed through the use of an online survey that was distributed through social networks that should help enlighten us on how the users of such social networks address privacy and how they feel the platforms they use address their privacy rights. The importance of such research is outlined by Carlos Jensen, Potts, and Christian Jensen who state that "several recent surveys conclude that people are concerned about privacy and consider it to be an important factor in their online decision making" (Carlos Jensen, Potts, and Christian Jensen 2005).

The consumers who answered the survey were predominantly young male adults, with 73.7% of the people polled being men and 68.2% of them being aged between 20 and 24. This indicates that the consumers polled are clearly old enough to be responsible for themselves on the Internet and are not simply children being taken advantage of when using social media sites.

When asked if these consumers had ever changed their privacy settings on their social media accounts, 68.2% responded that they had however a surprising 13.6% claimed that they were unaware of the settings existence. This lack of awareness could be linked to the responsibility of the site owners to educate their users but the responsibility can also be linked to the users as they should be aware of their privacy rights when using such sites and actively seek out their settings and potential options. Furthermore, 9.1% of users claimed that they simply use the default settings on their social media accounts. This may simply be a choice on behalf of the end user or they may be overwhelmed with the privacy settings available to them which may lead to potential problems dealing with an overly sophisticated and hard to use options menu. This ease of use problem can be a slippery slope when demanding privacy settings as the user may have the capability to control their account but lack the knowledge or understanding of how each option functions.

The importance of the lack of awareness regarding privacy settings mentioned in the previous question is amplified by the results questioning how often these consumers publish personal information on their social media accounts. 36.3% of users polled claimed that they publish personal information on a daily basis, with 22.7% of users adding that they publish information for every event that they attend. Other users claimed that they published information only once a week or once a month on average, with 9.1% and 13.6% being the cumulative responses respectively. This leaves only 18.2% of users claiming that they have never published personal information to their social media accounts. Some may argue that this low figure of people publishing information may be due to their confidence in their privacy settings and may directly correlate to being those who were actually aware of their privacy settings from the previous question.

Users' confidence in their privacy settings may also be linked to the following question, which asks how often the users check up on their privacy settings, where a surprisingly large result of 54.5% of consumers claimed that they never check their privacy settings.

This result could support the previous questions in the notion that a user has originally designated their privacy options and feel confident in publishing their personal information and feel that they do not need to repeatedly check their options as they chose them correctly the first time. However a worryingly low amount of users claimed that they check their privacy settings when a Terms of Service update occurs, with only 9.1% of people polled admitting to this. This may reflect on the users trust in the social network to not breach their privacy rights with a Terms of Service update or it may indicate a lack of awareness about such updates.

Confidence in the user's awareness regarding the severity of online privacy is definitely strengthened when seeing that an average mark of 4.09/5 was given when rating how serious the users take privacy on their social media accounts, with no user giving a rating below 4. This is also strengthened by the result of 4.5/5 when the users were polled on how serious they take privacy elsewhere on the web and not just on social media sites.

Moving away from the users general approach on their privacy settings, we see that their opinions on the importance of personal information is not matched by their feelings of safety when trusting social media sites with such information, as an average mark of 3.55/5 is given when ranking the safety of their personal information on their social media accounts, with 40.91% of users rating with just 3/5. This average mark shows that there is definitely room for improvement on behalf of social media companies to instil confidence in their user base with safely managing people's sensitive information.

Looking specifically at Facebook, a platform that users "spend more than 700 billion minutes per month on" (A. Porterfield et al, 2011), 63.6% of users claimed that only their friends could see their content published on the site. This figure correlates well with the response in the first question which stated that 68.2% of users had edited their social media privacy settings. However analysing the results further we see that the second most common response was users claiming that everybody could see their information as 18.2% of users chose this option. This figure may be worrying to some as such a large amount of users actively choose to publicise their entire social media account to anyone in the world, however it is hard to distinguish whether this is intentional behaviour from the users or a mistake in their settings or simply lack of awareness regarding the existence of such settings.

Moving away from Facebook to Twitter we see a very different response in that 59.1% of the users we polled do not use the platform. This statistic is very surprising given that "17.09% users of Twitter are from the UK" (Twitter 2013). Given the nature of Twitter's platform being more of a blogging and sharing site compared to Facebook's social connection approach it comes as no surprise that a much large amount of users allow anyone to see their Twitter content as 27.3% of users responded with this answer. An incredibly low amount of users (13.6%) seemed to restrict the visibility of their content on Twitter answering that they restrict their friends or restrict content to their followers.

Considering more than just social media platforms, users then answered which websites they feel most concerned about with their personal information. Despite this being a broader question in terms of different sites and platforms such as banking applications and search engines, Facebook still ranked the highest with 25.5% of users stating that they feel most concerned about their information on this platform, followed closely by

PayPal and other banking applications which accumulated 23.6% of user's votes. Surprisingly only 10.6% of users felt most concerned with Twitter, however this may correlate to the previous answer that 59.1% of users polled do not have a Twitter account. Analysing this result we see that the users polled treat Facebook as a higher concern with their personal information than their own banking and payment platforms, which arguably forcibly require more personal details from the user upon entry.

Finally we look at the type of content these users published on their social media accounts, which were primarily photographs (43.5%) and videos (26.1%). Whilst not strictly personal information, these two mediums of content still leave the user identifiable which may put them at risk off of the platforms themselves. Coupling these statistics with the result that 8.7% of users post their locational information online leaves a worrying picture that a user may be identified by their online accounts and even tracked down to their own home based upon the data that they published through a social media platform.

The last result shows yet more areas for concern as 19.6% of users claimed that they publish personal information to these sites. This figure is summed up well by Young and Quan-Haase who pointed out that "despite concerns raised about the disclosure of personal information on social network sites, research has demonstrated that users continue to disclose personal information" (Young and Quan-Haase 2009).

5 Future Propositions

Users are not the only ones to blame when it comes to Internet privacy as they are the ones posting their personal information and media to the site as well as conducting other activities without thinking twice about the consequences of those actions. However corporations both of smaller and bigger size are the ones that are responsible with maintaining information in a safe and secure manner for theirs users in order to guarantee true transparency with the way information is kept and shared with other third party organisations without the users consent. A suggestion to eliminate these kinds of activities from the company side would be to adopt to new privacy policies that can satisfy the users. It is also important for the organisations to understand that it is very crucial that user information should be maintained secured at all the times, enforcing Data Protection Act 1998. Organisations should better understand the level of security required by the users and this could be achieved by taking their opinions regularly using surveys, feedback boards, polls and focus groups.

According to the survey we conducted 13.6% of users have responded that they didn't know privacy settings actually existed, however they were concerned about the information they publish online. The only reason why the users didn't know the existence of those settings is because companies didn't give enough effort in publishing the amount of support that they provide for the users and how those settings could be used to benefit the users. Also many companies presume that statements framed in legal language within their privacy policies actually describe their true information collection and processing practices. Defined as success for online privacy, L.F Cranor claims that such platforms: "must be accompanied by tools and procedures to provide strong security" (Cranor 1999).

Solutions must be implemented to overcome such interpretations from companies and actions such as tutorials on how to set privacy settings may help the users to decide how secure they want certain information to be. However it is important for companies to promote their privacy settings using online tutorials, screen prompts and also make them easily accessible in the same way they promote other services such as prompts requesting users to share posts, pictures, videos and other content.

Organisations such as Facebook, Google and Twitter have got privacy settings in place, but they are not always clear of the functionality, which raises users concerns about the outcomes. Therefore companies, as well as promoting their provided settings, should also make it simpler for the users to understand how the settings work as it is not always the quantity of settings that matter but rather their effectiveness in providing the user with the tools required for online anonymity. Fewer settings may provide a clear image of their usefulness compared to a large number of options to toggle on and off, as a suggestion companies should start looking more into how clear their settings are and not only implementing and making them available.

Facebook's Chief Privacy Officer, Michael Richter, announced last year the removal of a privacy setting called "Who can look up your Timeline by name?" (Richter 2013). This is considered to be a step backwards in a world where privacy and user data security is a major concern. It also shows that the company is not very concerned about their users' privacy and safety. Organisations must work towards making their privacy settings even stronger so that user security is maintained to its highest standards and not follow the same step taken by Facebook. In 2012 Fuchs et al summed up the requirement for such developments by stating that "the traditional privacy concept is challenged, and new protective measures must be developed" (Fuchs et al. 2013).

Big corporations such as Google and Facebook should help the users to better understand how their privacy policy works and also when first signing up to use the website users should be made aware of the level of privacy the company is offering. However that is not all, as many corporations have term and conditions that are presented to the user when first signing up to use the company's services, but these are often written in small fonts and not very appealing to the users. As a solution to overcome the privacy issues organisations should make it clear, perhaps in large and bold fonts, detailing how information is processed and secured within the organisation.

According to the results of the survey conducted 40.91% to 95.46% users responded that they take privacy on the web as a serious matter. This shows that the users expect their information to be secured at all the times and be able to makes changes to their privacy settings according to their needs.

The United Kingdom itself, as a member of the European Convention on Human Rights, adheres to Article 8 of the Human Rights policy which guarantees that "everyone has the right to respect for his private and family life, his home and his correspondence" (Kilkelly 2003).

6 Conclusion

The analysis performed has shown us that the issue of online privacy within the United Kingdom is a concern for many consumers and one that corporations must consider when entering the UK market. The online survey analysed previously in the paper highlighted the concerns and effects that companies have on consumers in the UK when they are unprepared or unaware for the adoption of their online platforms. For this reason the future propositions provided include increasing awareness of privacy concerns to both the consumer as well as the corporations.

When a company neglects the severity of online privacy they leave both themselves and their users at risk as they are liable by law to adhere to the various data protection legislation that the United Kingdom has in place. Ignorance of this legislation is a concern to the consumers also as many are unaware of their privacy rights online and think that the set of privacy tools provided by an online platform is all that they are entitled to.

Improvements in the usability and awareness of online privacy tools will ultimately benefit both parties and ensure a safer environment for the consumers of such online tools. As the diversity of privacy risks continually grows in the form of identity theft and cyber bullying it is imperative that both parties understand their role when using such a platform and understand that they both share some level of control with regards to their safety.

References

McClurg, Andrew J (2003). "Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling, A". In: *Northwestern University Law Review* 98, p. 63.

Stevenson, Angus (2010). *Oxford dictionary of English*. Oxford University Press.

Nissenbaum, Helen (2009). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

Chung, Winnie and John Paynter (2002). "Privacy issues on the Internet". In: *System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference on*. IEEE, 9–pp.

Stein, Laura and Nikhil Sinha (2002). "New global media and communication policy: the role of the state in the twenty-first century". In: *Handbook of new media: Social shaping and consequences of ICTs*, pp. 410–31.

Facebook (2013). *Facebook Statistics*. URL: `http://www.statisticbrain.com/facebook-statistics/`.

Twitter (2013). *An Exhaustive Study of Twitter Users Across the World*. URL: `http://www.beevolve.com/twitter-statistics/#f3`.

Google (2013). *By the Numbers: 88 Amazing Google Stats and Facts*. URL: `http://expandedramblings.com/index.php/by-the-numbers-a-gigantic-list-of-google-stats-and-facts/`.

Legislation.gov.uk (1998). *Data Protection Act*. URL: `http://www.legislation.gov.uk/ukpga/1998/29/schedule/1`.

Advertising Standards Authority (2013). *Online behavioural advertising*. URL: `http://www.asa.org.uk/Consumers/What-we-cover/Online-behavioral-advertising.aspx`.

Mendel, Toby et al. (2012). *Global survey on internet privacy and freedom of expression*. UNESCO.

Brankovic, Ljiljana and Vladimir Estivill-Castro (1999). "Privacy issues in knowledge discovery and data mining". In: *Australian institute of computer ethics conference*, pp. 89–99.

Goss, Sherri (2013). *Data-mining and our personal privacy*. URL: `http://www.macon.com/2013/04/10/2429775/data-mining-and-our-personal-privacy.html`.

Weiss, Stefan (2009). "Privacy threat model for data portability in social network applications". In: *International journal of information management* 29.4, pp. 249–254.

Klosowski, Thorin (2012). *How to Opt Out of Facebook's Newest Attempts to Track Everything You Do, Even Offline*. URL: http://lifehacker.com/5946030/how-to-opt-out-of-facebooks-newest-attempts-to-track-everything-you-do-even-offline.

Jensen, Carlos, Colin Potts, and Christian Jensen (2005). "Privacy practices of Internet users: self-reports versus observed behavior". In: *International Journal of Human-Computer Studies* 63.1, pp. 203–227.

Young, Alyson L and Anabel Quan-Haase (2009). "Information revelation and internet privacy concerns on social network sites: a case study of facebook". In: *Proceedings of the fourth international conference on Communities and technologies*. ACM, pp. 265–274.

Cranor, Lorrie Faith (1999). "Internet privacy". In: *Communications of the ACM* 42.2, pp. 28–38.

Richter, Michael (2013). *Reminder: Finishing the Removal of an Old Search Setting*. URL: http://newsroom.fb.com/News/735/Reminder-Finishing-the-Removal-of-an-Old-Search-Setting.

Fuchs, Christian et al. (2013). *Internet and surveillance: The challenges of Web 2.0 and social media*. Vol. 16. Routledge.

Kilkelly, Ursula (2003). "The right to respect for private and family life". In: *A guide to the implementation of Article 8 of the European convention on Human Rights*.