Journal of Management Policies and Practices
June 2016, Vol. 4, No. 1, pp. 71-77
ISSN: 2333-6048 (Print), 2333-6056 (Online)

Published by American Research Institute for Policy Development
DOI: 10.15640/jmpp.v4n1a5
URL: https://doi.org/10.15640/jmpp.v4n1a5

Shelley Martin[1]

Thesis statement

(a) Corporations exploit social media while disregarding the public's right to both Privacy and Choice.

Privacy

Privacy is a fundamental unalienable right placed in human rights charters alongside life, freedom of expression, religion and more (Cornell, 2015). If you curtail a right to privacy enough all other freedoms wither. It is difficult to be self-determining when someone continually evaluates your choices constantly monitoring you and impacting on your ability to express ideas, needs and wants freely (Guardian, Jan 28 2015).

Humanity has a deep seated need to share ideas and experiences, giving us the ability to connect with other people, to be heard, and to feel worthwhile and important. We have an innate curiosity about the world around us and a need to organise and manipulate it (Russell, 2014). Humans use communication to share observations, ask questions, and engage in meaningful conversations about issues.

Due to the lack of borders and regulations, privacy on the internet has become a major concern for all online activities (Wu, Huang, Yen & Popova, 2012). Defining privacy is difficult due to the fact that even for users of a product or service it is hard to quantify. Back in the 1960's Westin (1967) defined privacy as being the desire of people to choose who they will expose themselves to and to what extent, including attitudes and behaviours. As Liu et al. (2011) found in their research on privacy settings on Facebook, even photos can have multiple privacy needs depending on where they are taken and who is in them. In 2011 the LA Times commented in their blog on the attempt by LA law enforcement and consumer groups to require stronger privacy laws. Their attempts were blocked by Facebook, Google, Twitter and other firms as, if they were enacted they could cost the companies millions of dollars in lost revenue as they would be required to remove personal information from sites when asked and allow parents to edit their children's comments online and allow them to take down addresses and other identifiers (LA Times, 2011).

Launched in February 2004, Facebook is one of the most used and visited sites on the web. A popular free social networking site Facebook allows users to create profiles, upload photos, connect with other users (including friends and family), and message other users (Techtarget, Aug 2014). However Facebook has been dogged with controversy over its use of personal and private information garnered not just from your personal profile but also any and all third party apps that the user chooses to run. While everyone knows that Facebook places tracking cookies (harmless text files that a website places on your computer, that allows the programme to follow you where you go) on user's computers if they visit any page on Facebook.com, they may not realise that this also includes fan pages and other pages that do not require a Facebook account to visit (Guardian, March 2015; Lee, 2014).

[1] Student, Management, Auckland University, Newzealand. +64 9 2968680, sa.martin@xtra.co.nz

According to Hann et al (2002) privacy is one of the most critical impediments to e-commerce. Hoffman, Novak and Peralta (1999) looked at building consumer trust online. Despite the growth of online shopping they found that the revenues and related profits were minimal compared to expectations due to the fact that it was proving difficult to move some customers to the point where they actually clicked to purchase. It was expected that by 2002 the average revenue of online sales would reach approximately 37.5 Billion (Hoffman, Novak, & Peralta, 1999; Matzat & Snijders, 2012).

A report that was commissioned by the Belgium privacy commission and conducted by the Centre of Interdisciplinary Law and ICT at the University of Leuven in Belgium found that Facebook is currently acting in violation of European Union (EU) law in spite of having updated their privacy policy. The report claims that Facebook's privacy policy update in January only acted to expand on older policies and practices, and that it still violates European consumer protection law (Guardian, February 2015; thenextweb, March 2015; cnet, March 2015). The EU privacy law states that prior consent must be given in order to issue a cookie or perform tracking of any kind unless it is necessary either in order to connect to the specific service, or to deliver a service that has been specifically requested by the user (Guardian, February 2015). This same law requires all websites to notify their users on their first visit to the site that it uses cookies and to request the users consent.

Twitter is a microblogging service that allows people to communicate in 140 character messages that correspond to thoughts or ideas. It is a rich source of social data that is considered a great starting point by businesses for social web mining because of the fact that its nature is to be inherently open for public consumption. Twitter data is especially interesting to the businesses due to the fact that tweets happen at the speed of thought and the information is available for consumption by others as it occurs in near real time, represents the broadest cross section of society at an international level, and is inherently multifaceted (Jones, 2011; Russell, 2014).

While there are multiple barriers to the use of online consumerism, including the lack of secure payment, the biggest reason for the lack of online consumerism has to be linked to the lack of faith between consumers on the web and most businesses (Christensen, 2014; Lee, 2014). Research (Hoffman, Novak, & Peralta, 1999; Matzat & Snijders, 2012) shows that the lack of trust arises out of the cyber consumers feeling that they lack control over the access that web merchants have to their personal and private information. These concerns span both environmental control and the control over the secondary use of information. Environmental control is defined as the ability to control the actions of an online vendor, while control over secondary use of information is the ability to control the use of your information by other parties for uses secondary to those of the transaction where the information is collected.

500 million people are registered users of Twitter with at least 100 million users actively tweeting on a regular monthly basis. On average twitter users generate about 140 million tweets a day on a variety of topics (Jones, 2011), however according to Dataminr it is more in the region of 500 million a day (Business, 2014). The true power of Twitter is its open and real time communication of information among individuals and groups. However under the surface it is a treasure trove of information about the behaviours of the individual users and users as a group, as well as trends at both the local and global levels (Jones, 2011).

In 2012 the EU data protection authorities wrote a report on the emerging threat to individual privacy. Its focus was on Google's asserted right to expand its data mining to combine users' personal data across all accounts and services including Gmail, internet searching, Google Maps, locations apps and photo sharing. Individuals would have no way of opting out (Guardian, Oct 15 2012).

In the last month (July 2015) Facebook users have been in a state of panic over Zuckerberg's use of the Rainbow picture of the "Celebrate Pride" app which has been used by Facebook to accurately track more than 26 million users (Utah Post, July 2015) that have made use of the Facebook app. This is not the only overt use of this technology by Facebook. Facebook's opengraph technology allows third party apps and websites to tell Facebook what people are doing and to automatically publish their activities on their timelines. People using Facebook's timeline and social apps with Open Graph have been unknowingly transmitting details such as names, friend's names, as well as wider information to dozens of tracking and advertising companies.

The Dutch data protection authority has asked Facebook to delay the rollout of its new privacy policy and Facebook is being probed by the article 29 working party which consists of data regulators from individual EU countries, including the UK's Information Commissioner's Office (Guardian, 23 February 2015). Facebooks recently updated (January 2015) data usage policy states that 'we collect information when you visit or use third party websites and apps that use our services.

This includes information about the websites and apps, as well as information on the developer or publisher of the app or website provides to you or us'. Facebook also updated its cookie policy at the same time stating that the company will still use cookies even if the person does not have a Facebook account or are logged out to 'enable us to deliver, select, evaluate, measure and understand the ads we serve on and off Facebook'. While you could be forgiven for thinking that this was a recent thing, in 2012 charges were filed against Facebook for continuing to track users even while they were logged out (Lee, 2014). "Facebook's Statement of Right and Responsibilites (SRR) contains a number of provisions which have been proven to violate the Unfair Contract terms Directive. These violations were present in 2013 and continue to be present in 2015" (Guardian, February 2015).

According to Forbes magazine (2013) Twitter's revenue for the first half of 2013 was up but over 87% came from advertising, most of which was considered experimental. By late 2014 Twitter had reportedly begun collecting information on its users' smartphones in order to arm its advertisers with information that they can successfully use to target customers. The company has been found to not only be studying customer information within its own app, but also learning from other apps that the users download (Forbes, 2015).

Twitter isn't the first social media site to use customer smartphone data for its own advertising efforts. Facebook users who download apps using their Facebook login have their information gathered by Facebook and then delivered to developers of apps (Forbes, 2015).

Created by Gabriel Weinberg, the DuckDuckGo search engine promises a level of privacy and choice unseen of in other apps and engines. Named after the childhood game Duck Duck Goose, it is now receiving over 10 million searches a day (roughly 115 a second). The search engine has built its reputation on being 'the search engine that doesn't track you' (Fox News, 2015). This is important as, whenever you search for something your computer automatically sends information on you to that particular website. This information can include things such as your IP address and real name.

Weinberg believes that the personalisation that people want is localisation as opposed to engines such as Bing and Google which try to show you things they think you want to click on (Fox News, 2015). Localisation data is embedded in the search requests and does not get kept after the search is completed. DuckDuckGo has grown by over 600% since the true extent of the tracking done by the NSA and other companies came to light 2 years ago. A recent Pew report quoted by Weinberg shows that over 40% of Americans think that their search provider shouldn't be able to retain information about them (Fox News, 2015).

However, a study by University of Cambridge and Stanford scholars published in early January 2015 concluded that they could create an algorithm that would know the average Facebook user better than anyone except their spouse, and that with enough information even better than their spouse (Guardian, Jan 28 2015). Based purely on the likes on Facebook, an act that is considered the least-revealing, the algorithm can get an accurate picture of the user from 200 likes. The information gained allowed the researchers to guess a user's personality better than a friend, housemate or family member by using the widely used OCEAN scale (openness, conscientiousness, extraversion, agreeableness, and neuroticism). With 300 likes or more even the spouses knowledge of the user was left behind (Guardian, Jan 28 2015).

In 2012 the EU data protection authorities wrote a report on the emerging threat to individual privacy. Its focus was on Google's asserted right to expand its data mining to combine users' personal data across all accounts and services including Gmail, internet searching, Google Maps, locations apps and photo sharing. Individuals would have no way of opting out (Guardian, Oct 15 2012).

According to the Guardian (28th Jan 2015) the information age is heading towards the stage where no one will be able to come in and out of the European Union (EU) for example without trading at least 42 pieces of private information as the price of entry. In some countries the mere act of making a phone call now has a trade-off where you give away details on who you were calling, when and for how long. To read a Newspaper online you now trade the rights to information around what you are reading through the use of cookies.

Both a fundamental right and a low-cost commodity, we will be making trades in personal information for the foreseeable future which means that it's important we start thinking about the price.

Abuse of trust

It has been found (Hoffman, Novak, & Peralta, 1999) that consumer expectations of privacy are dependent on the medium. The traditional attitudes towards privacy invasion in traditional media ranges from tolerance to disgust, in electronic media though, 87% of web users think they should have complete control over demographic information, and 71% feel that there should be laws to protect their privacy online (Pitkow & Kehoe, 1997). Approximately 20% in the survey stated magazines have a right to sell consumer information for marketing purposes but only 12% say that web sites and third parties have the same rights (Hoffman, Novak, & Peralta, 1999).

Of the 63% who refuse to divulge their personal information to websites, they report that it is because of the fact that they don't trust the people collecting the data. 65% state that the benefits of providing the information are far outweighed by the risk of revealing it, and 69% refuse on the grounds that they have been given no information by the web provider on how they intend to use the data collected. On the other side of this argument over 72% of users stated that they would happily give websites demographic information if the sites would provide a statement telling them how their information would be used and by whom (Hoffman, Novak, & Peralta, 1999; Wu, Huang, Yen & Popova, 2012).

With huge amounts of personal information being collected on customers and utilised by companies through registration and order forms as well as through tracking software and cookies, online customers often measure the risk of information misuse or revelation (Liu, Marchewka & Ku, 2004b; Milne & Culnan, 2004; Wu, Huang, Yen & Popova, 2012). The spread of the internet has eliminated the ability of people to remain anonymous on the web, users leave electronic footprints in the form of cookies and other tracking devices that detail online behaviours and preferences that can be easily shared and used by strangers (Zviran, 2008; Wu, Huang, Yen & Popova, 2012).

Building trust is a key element in reducing privacy concerns of consumers and improving the relationship between consumers and businesses (Milne and Boza, 2000). Completing a transaction without disclosing something in the way of personal data is very difficult, even when the disclosure is being made to a trusted third party. Without that buffer of having trusted people who retain your data while ensuring that other parties cannot access it, the consumer has to weigh their perceptions of trust in that party and the benefits of disclosing the information to them against the risks of that information being shared with a not so benign other.

A report that was commissioned by the Belgium privacy commission and conducted by the Centre of Interdisciplinary Law and ICT at the University of Leuven in Belgium found that Facebook is currently acting in violation of European Union (EU) law in spite of having updated their privacy policy. The report claims that Facebook's privacy policy update in January only acted to expand on older policies and practices, and that it still violates European consumer protection law (Guardian, February 2015; thenextweb, March 2015; cnet, March 2015).

The EU privacy law states that prior consent must be given in order to issue a cookie or perform tracking of any kind unless it is necessary either in order to connect to the specific service, or to deliver a service that has been specifically requested by the user (Guardian, February 2015). This same law requires all websites to notify their users on their first visit to the site that it uses cookies and to request the users consent.

According to the report completed by the Belgium privacy commission, Facebooks policies around profiling for third party advertising do not “meet the requirements for legally valid consent”, while the social network “fails to offer adequate control mechanisms” with regard to the use of the user-generated content for commercial purposes (Russell, 2014).

Four popular third party applications run by Facebook are Foursquare, Glancee, Sonar, and Highlight. Foursquare is an app that combines social networking, geolocation and advertising. It is an app that encourages its users to share their recommendations with others based on their location, as well as providing an opportunity for businesses to offer incentives to current and potential customers (Thomsett-Scott). Users are able to download the app for free to their mobile, however it works better when a user’s mobile is geolocatable. Geolocation is the technique of identifying the geographical location of a person or device by means of digital information processed via the internet (Oxford). The app ‘Hell is other people’ uses Foursquare to track friends and then calculate the optimal distance from them geographically in order to avoid them (Thomsett-Scott).

Glancee is a Facebook app that explores the Facebook profiles of the people nearby through their phone or laptop connections and notifies the Glancee user when someone nearby has common friends or mutual interests. Sonar is a mobile app that analyses Twitter, Facebook and Linkedin to see if any friends are nearby. Highlight uses Facebook data to give names, photos, mutual friends, hobbies, interests and anything they have chosen to share.

The new privacy policies are contra to what Facebook originally told users, which was that the third party apps installed by the users would only have access to the user information that they needed in order to operate. As can be seen, the apps access all of a user’s information (Lee, 2014). Facebook also promised users that they would not share any personal data with their advertisers, however it does.

In 2011 Facebook rolled out their ‘read, watch, listen, want’ which broadcast every interaction that the users have with them. Consumers are always very comfortable with Amazon using data to recommend books they might like. When users are in control of it, it's a win-win — if they feel empowered.

The real payoff for businesses on social media comes from the ability to track then understand and predict consumer desires and purchase intentions. Drawing a line between helpful customisation and Big Brother manipulation is far from clear or easy, and a few users are consciously aware of how closely their every move is watched and remembered (Forbes, 2013). Twitter states that “the mission we serve as Twitter, Inc. is to give everyone the power to create and share ideas and information instantly without barriers”.

There are some very good reasons in business terms that brands are moving their advertising to Twitter. First, according to Twitter 74% of people following a brand product on Twitter do so in order to get updates. This is an enormous opportunity for businesses to promote products and services to an engaged audience. Second, whether or not it backed by the particular company people are talking all the time about businesses or products on Twitter, with businesses monitoring brand mentions. Third, 72% of Twitter followers are more likely to make a future purchase after engaging with a brand on Twitter. 73% of Twitter users shop online each month compared with 69% of Facebook users.

There is a powerful reason why cloud services and other data-mining companies aggregate data across multiple accounts and services: the results are extremely valuable. Just as tiny bits of coloured tile can be combined and transformed into a coherent piece of art, tiny bits of seemingly unrelated personal data, when aggregated and mined at huge scale, can provide immense value to advertisers, marketers, corporate sales forces and others.

The revenue generated by combining and monetising such data – by mining the mosaic – is the reason "free" cloud services can afford to be free.

Mining of Data

Mining allows you to grab application information, analytical information on a website’s structure. Or in the case of big businesses, information a person’s likes, dislikes, preferred suppliers, the way that they might vote in an election. Companies are mining the social web to build a dossier, with information posted publicly on Facebook, Twitter and other social media being fair game.

Data mining is the process of searching large stores of data in order to discover previously unexplored connections between items of information (Oracle, 2014). Web data mining takes resources and an understanding of the Internet as you need to “crawl” the internet to gain the information you are after. It is believed that the biggest most successful Data miner is Google. Through the use of a crawler that the company calls a “Googlebot” it spiders or crawls through the Internet looking for factors that it then mines, stores and uses not just for ranking websites in search engines but for targeted advertising.

Rapleaf, a company acquired by Towerdata in 2013, collects comprehensive data on email addresses and the people behind them (Crunchbase, 2014). A counter on the Rapleaf website states that they have mined social data on more than 389 million customers. This is done by crawling the internet just like Google, however they only crawl sites like forums, blogs, social networks and review sites where the information is freely given and publicly available.

In 2014 the economist ran an article on a company called Dataminr who are mining twitter feeds for information in order to trace back stories that prove genuine and market-moving events, finding their earliest appearances on twitter and predicting which tweets and trends will go viral then selling this information on to interested parties (Business, 2014). In January 2014 Dataminr and Twitter struck a deal to provide CNN with alerts and in April 2014 Twitter was used by Boston authorities to prevent a repeat of the Boston Marathon bombings.

Huawei, a leading telecommunication company in China, is unapologetically open about the fact that it engages in Data Mining on a large scale. A Hong Kong Jobsite advertisement has Huawei looking for a Data Mining Specialist with at least 7 years’ experience and a Master’s Degree in Math or Statistics (HKJobsDB, 2015).

Data mining companies like Rapleaf Inc. and Dataminr make their living from collating information about individuals and then on selling it to companies that want to learn about the individuals and their online habits. Erica Sandberg, a personal finance reporter, states that a data mining company can turn your chatter into a behavioural pattern that they then can prove has worth to companies. Entities like airlines, politicians and not for profits can use the data to target new customers and create products specific to existing ones. Financial institutions such as banks and lenders also use the same data mining services to market effectively and make lending decisions. While it cannot affect your credit rating, Sandberg says that it can affect the credit you are offered and receive. Social media also impacts as your Facebook friends affect whether you yourself are seen as a good credit risk. If they have a good rating then you are considered a good credit risk, however if they have a bad credit rating then companies are going to see you as a possible bad credit risk.

Ethics at work

An Australian email provider company subject to Australian law, FastMail does not engage in any surveillance or monitoring of customers as well as taking steps to ensure that others are not able to surveil their customers without permission. While they do not guarantee that their measures are 100% effective as no one knows the current capabilities of hackers. As an Australian company they are legally required to disclose information on a customer to Australian Law Enforcement when supporting documentation is given (FastMail, 2015).

Fast Mail prides itself on the fact that it does not sell or give information about their users to any third party. Credit card details are not held by the company but rather go through a third party (Pin, Stripe, or Paypal), and that third party may store the details for the purposes of future payments. They also only scan incoming and outgoing messages for the purposes of spam detection, which they have provided users the ability to turn off if they so wish. Emails reported as spam are automatically analysed to help train the spam filter.

Also, if enabled, emails reported as spam are forwarded on to some external email reporting services. “These services aim to help monitor and reduce overall spam on the Internet. Currently the services we report to are Return Path and LashBack. These may change in the future. If you don't want this, you can disable the reporting in the FastMail advanced settings” (FastMail, 2015).