INTERNET POLICY REVIEW
Journal on internet regulation

Volume 5 | Issue 4

# The privacy role of information intermediaries through self-regulation

**Tatevik Sargsyan**
*School of Communication, American University, Washington, DC, United States of America*

Published on 16 Dec 2016 | DOI: 10.14763/2016.4.438

**Abstract:** Through qualitative analysis of the policies of two major global information intermediaries — Google and Microsoft — and related case studies, this paper demonstrates a) that intermediaries' participation in self-regulatory programmes and implementation of privacy principles does not necessarily translate into meaningful privacy safeguards for users in the face of growing private surveillance capacity; and b) that within the EU and US self-regulatory frameworks, information intermediaries have discretionary power to set their policies and practices prioritising strategic interests over privacy commitments. Discussions in this paper complement existing studies on the implementation of privacy principles stipulated in Fair Information Practices (FIPs) by enhancing understanding about the role of information intermediaries in defining privacy conditions of users within self-regulation.

**Keywords:** Privacy, Intermediaries, Platforms, Self-regulation, Fair Information Practices, Terms of Service (TOS)

Article information

**Received:** 30 Apr 2016 **Reviewed:** 08 Aug 2016 **Published:** 16 Dec 2016
**Licence:** Creative Commons Attribution 3.0 Germany
**Competing interests:** The author has declared that no competing interests exist that have influenced the text.

**URL:**
http://policyreview.info/articles/analysis/privacy-role-information-intermediaries-through-self-regulation

**Citation:** Sargsyan, T. (2016). The privacy role of information intermediaries through self-regulation. *Internet Policy Review*, *5*(4). DOI: 10.14763/2016.4.438

# INTRODUCTION

Privacy has become one of the most contested public issues in internet policy, and information intermediaries such as Google, Facebook, and Microsoft are at the forefront of defining privacy conditions of users via their data collection, processing and dissemination practices. Invariably, private intermediaries gain greater surveillance capacity as technology develops, usage of mobile devices grows, and online services transition into more personalised and integrated realm (e.g., King & Jessen, 2010; Popescu & Baruh, 2013; Sullivan, 2015). Simultaneously, data protection

authorities in the European Union (EU) and the United States (US) continue to embrace self-regulation mechanisms to address growing privacy concerns of users (CIGI, 2014; Madden, 2014). Among self-regulatory frameworks, the U.S. Federal Trade Commission (FTC) 2000 and 2012 Privacy Guidelines and the EU-US Safe Harbor Agreement have been significant in conceptualising how personal information should be protected online. These frameworks largely derive from the Fair Information Practices (FIPs) of the Organization for Economic Co-operation and Development (OECD) and set expectations for private intermediaries handling personal information (DiLascio, 2004; Export.gov, 2015; FTC, 2000, 2012; OECD, 2013, 2014). In spite of existent critique on the insufficiency of self-regulation to protect privacy (Gellman & Dixon, 2011; Lee, 2003; Rubinstein, 2011; Scott, 2015), regulators and data protection authorities in the EU and US have put their faith in a new Privacy Shield programme, which has replaced the EU-US Safe Harbor Agreement (ITA, 2016).

In light of these developments, in this paper, I seek to demonstrate that despite participating in self-regulatory frameworks, taking on privacy commitments, and evolving corporate policies towards FIPs, information intermediaries' do not offer meaningful privacy protection to users. Private intermediary companies have historically set and enacted their policies prioritising market considerations with opportunistic regard for privacy commitment under self-regulatory frameworks (e.g., DPA, 2010; FTC, 2011), and there is no reason to believe that this dynamic would change under the Privacy Shield programme. To make the argument, I first review a number of changes that two global information intermediaries, Google and Microsoft, have made to their policies in an attempt to operationalise notice and choice principles stipulated in FIPs; second, I analyse privacy implications of these policy changes; and third, I present two brief case studies to demonstrate clear deviations from privacy commitments for economic opportunity.

## INFORMATION INTERMEDIARIES' ROLE IN SETTING USERS' PRIVACY CONDITIONS

As millions of users in Europe and the US access online services such as Google maps, YouTube, Skype, Bing, and others, intermediaries' Terms of Service (TOS) and privacy policies grant these companies the right to collect vast amounts of data about users and their online activities. Intermediaries collect and process personal information such as name, e-mail, address, phone number, financial and location details, as well as non-personal data generated from users' interaction with services such as communication content, browsing history, search queries, etc. (e.g., Google, 2015b; Microsoft, 2015e). Private surveillance, while an essential source of advertising and revenue for intermediaries, reinforces government surveillance and exacerbates privacy conditions of users. Being a repository of user data, information intermediaries become a natural target by governments who turn to these private companies to gain access to user information for legitimate and illegitimate reasons (Deibert, 2013; DeNardis, 2012; Sargsyan, 2016). Intermediaries then carry a gatekeeping role by making decisions about collaborating on surveillance and disclosing user data to government agencies (e.g. Google, 2014b). In this context, information intermediaries' data collection, retention, and disclosure policies have significant public importance as they greatly reduce possibilities for anonymity and increase risks associated with inhibition of expression, physical, financial and reputational harms (Solove, 2006). Collection of personal information, for example, makes user identity known to information intermediaries and potentially their affiliates and governments, putting citizens at a higher physical risk, especially in countries where the rule of law is weak and inadequate. Cases

of imprisonment and harassment of journalists and activists based on their communicative activities via intermediary services are not uncommon (Hosein, 2010; MacKinnon, 2012; Weber, 2013).

Further, even when intermediary services do not require disclosure of personal information, technical affordances and analytics of huge sets of data can reveal private information about users. Computer scientists have confirmed that data sets containing no personal information can be deanonymised and lead to identification of specific individuals (Angwin & Valentino-DeVries, 2010; Montjoye, Radaelli, Singh, & Pentland, 2015; Ohm, 2010). For example, each device connected to the internet is assigned an Internet Protocol (IP) address based on geographic location, and each phone or computer has a unique device identifier consisting of a sequence of letters and numbers (e.g., Google, 2015b; Microsoft, 2015e). IP addresses and unique hardware numbers can be combined with other data such as search logs and browsing details to reveal the identity of hardware owners and sensitive information about them (DPA, 2010; Tene, 2008).

## LEGAL CONTEXT REINFORCING INTERMEDIARIES' LEADING PRIVACY ROLE

Information intermediaries' essential role in defining user privacy conditions took place organically and has been reinforced by their technical affordances and the legal context in which they operate. Many globally popular private intermediaries, including Google and Microsoft, originated in the US political system where the state favours unregulated markets as an efficient way to improve economy, distribute resources and boost innovation (Cohen, 2012; Mayer-Schönberger & Cukier, 2013; Pickard, 2013). The US government has refrained from passing a data protection law that covers private sector activities. Restrictions on private intermediaries' information activities exist only in the areas regulated by US privacy law, which are mostly limited to financial, health and children information. In response to the growing benefits of data in digital commerce and international trade, even the EU states, which have a more restrictive legal stance on information processing, have allowed intermediaries to collect, transfer and use consumer information across jurisdictions (Bennett & Raab, 2006; Zimmer, 2010).

Nonetheless, recognising that the private sector's data activities greatly impact public interest, government agencies have embraced alternative forms of regulation and expect information intermediaries to fulfill public policy goals through self-regulatory mechanisms. Self-regulation is an umbrella term that refers to a non-binding process of regulation conducted through voluntary agreements, delegated decision-making, standards setting, certification, etc. (Feeley, 1999; Senden, 2005). In the US, the FTC has been the major player in promoting self-regulation by putting forward loosely enforceable privacy standards and recommendations to guide information intermediaries' information processing and by exercising its authority to sanction unfair and deceptive practices of companies, in accordance with Section 5 of the FTC Act (Culnan & Bies, 2003; FTC, 2000). In Europe, under the 1995 EU Privacy Directive, personal information could only be transferred from the EU to countries with adequate data protection laws, as defined by the European Commission. Since the EU did not consider the US to have adequate privacy protection, policymakers in these jurisdictions authorised transfer of personal information via a self-regulatory scheme—the Safe Harbor agreement, which allowed voluntary participation by companies (Farrell, 2003). For example, to transfer and process EU citizens' data, many information intermediaries, including Google and Microsoft, received certification

and pledged to adhere to Safe Harbor privacy principles (Export.gov, 2015). In August of 2016, the EU-US Privacy Shield programme has replaced the Safe Harbor agreement, which was deemed invalid by the Court of Justice of the European Union in October of 2015 (ITA, 2016; Scott, 2015). Whereas, the FTC privacy recommendations, the Safe Harbor and the Privacy Shield have differences, they do promote many of the privacy protection fundamentals of the FIPs.

FIPs are a set of internationally recognised practices that reflect global norms for use of personal information. Initially put forth by the US Department of Health, Education and Welfare, the FIP principles are reflected in the Privacy Principles of the OECD and data protection laws in Europe (Rotenberg, 2001, OECD, 2013). OECD member states consider FIPs the minimum standards for privacy protection without restricting cross-border data flow. They are aimed at a) minimising data collection; b) ensuring that collected data is relevant to the purpose of its use; c) being open about practices of personal data; d) providing notice to users about the purpose of data collection; e) limiting use of data to the specified purposes unless user consent is obtained; f) providing data security; g) granting users the right to learn about collected data that relates to them and to challenge and correct the data; and h) being accountable (OECD, 2013).

In this context, Google and Microsoft, as intermediaries subject to the FTC authority and certified participants of the Safe Harbor and now, the Privacy Shield agreement, are expected to implement these privacy principles to legitimise their information practices online. However, despite visibility and millions of users in the US and EU (e.g., Craddock, 2013; Lardinois, 2015; Steele, 2013), even Google and Microsoft have been inconsistent in their efforts to align their policies with principles stipulated in FIPs, the Safe Harbor, and FTC recommendations. For example, instead of minimising data collection, these companies continue to grow their surveillance capacity. In 2015, for instance, Microsoft launched the Windows 10 operating system, which is not a static software stored and run out of users' devices like previous Windows versions. It is a cloud-based personalised system that is linked with all of Microsoft web-based services such as Bing, Skype, and Outlook.com, granting the company access to an unprecedented range of data across services and raising its advertising capacity (Hoffman, 2015; Microsoft, 2015g). Similarly, despite the acknowledgement that network encryption is an essential component of data security, Google's and Microsoft's encryption efforts used to be sporadic and intensified only after the revelations about the National Security Agency (NSA) mass surveillance scandal in 2013 and these companies' secret provision of user data to the NSA (Greenwald, 2013, 2014). Facing potential loss of business opportunities globally due to lack of trust, and foreign countries' efforts to increase reliance on domestic internet infrastructure (Chander & Le, 2015; Miller, 2014; Sargsyan, 2016), Google and Microsoft started encrypting data across all of their online services to regain trust and remain competitive (Google, 2014c; Microsoft, 2015b, 2015d). Thus, information intermediaries choose to codify privacy principles into their policies and tools opportunistically, based on market considerations. Moreover, even when information intermediaries change their policies to comply with privacy principles, it does not always denote meaningful privacy protection for users. In the next section, I argue this point by focusing on Google's and Microsoft's implementation and observance with notice and choice privacy principles.

# INTERMEDIARIES' PRIVACY POLICIES TOWARDS NOTICE AND CHOICE

Solutions to consumer privacy concerns due to ubiquitous data collection and processing are predominantly associated with giving users more control over their information through notice and choice (FTC, 2012; The White House, 2012; ITA, 2016). Notice refers to the expectation that intermediaries should inform their customers about what information they collect, how they collect and use the information, and weather they disclose that information to third parties. Choice, used interchangeably with consent, is about giving users the ability to control how their data is used. The typical implementation of choice happens through provision of customisable privacy settings, as well as opt-in and opt-out tools, which allow companies to get implicit or explicit consent from users about primary and secondary uses of their information (FTC, 2000; Schwaig, Kane, & Storey, 2006). These two principles have become the most essential benchmark against which the FTC and EU data protection authorities evaluate intermediaries' policies and bring enforcement actions against them. The FTC and data protection authorities in Germany, France, and the UK among others have penalised information intermediaries for failing to provide notice to data subjects and obtain their consent in advance of collecting their personal information (Dutch DPA, 2010; FTC, 2011; O'brien, 2013; Streitfeld, 2012).

Google's and Microsoft's privacy policies have evolved to provide notice to users about their growing means of data collection. These intermediaries continuously update their policies to provide information about how they collect, combine and use data for analytics, advertising, and improvement of operation as their services evolve and include new features (e.g., Google, 2015b; Microsoft, 2015e). Both companies' policies are forthcoming and reveal that they virtually collect all information related to uses of online services including personal information voluntarily disclosed by registered users such as name, contact information, payment details, location information, etc. For example, with the introduction of its voice-enabled digital assistant Cortana, Microsoft informed users that Cortana collects information about their contacts, location, typing patterns, speech, browsing history, and more (Microsoft, 2015c).

In addition to providing notice to users by disclosing detailed information about their data practices, Google and Microsoft also implement the principle of choice by asking users to agree to privacy policies and TOS before processing personal information (e.g. Google, 2014a, 2015b). Moreover, the idea of choice has also been applied more broadly, beyond personal information, to give users options to customise their tracking, data sharing and advertising preferences. For example, in 2010, Google started offering an extension that users could download and add to their web browsers such as Chrome and Internet Explorer not to be tracked by Google's DoubleClick cookie, which monitors users' web behaviour for commercial purposes. Google has also created a "My Account" dashboard, where users can see how their data is managed and control their privacy settings in one place, such as turning off location sharing in most of Google's services. The "Ads Settings" on the dashboard allows users to turn off interest-based advertising from Google's products such as Maps and Gmail, as well as websites beyond Google.com (Google, 2015a). In 2011, Google also announced that owners of Wi-Fi routers can add "nomap" to the router's name, which will notify Google that users are opting out of having the names and locations of their routers from being collected and stored in the company's databases (Google, 2011a). In 2012, Google also joined a select number of companies to enable a Do Not Track system on its browser, however, not by default. When users turn on Do Not Track on Chrome, the system sends out requests with users browsing traffic to notify websites about

users' wish not to be tracked. Whether the websites will cease tracking depends on their willingness to respect users' requests. Companies have no legal obligation to do so (Google, 2015a).

Microsoft followed a similar path in implementing privacy choice controls in its services. In 2009, the company also added private browsing feature in Internet Explorer 8, and its versions that followed after. Microsoft has also had cookie control options enabled in its browser since the early 2000s (Microsoft, 2000, 2008). In 2011, Microsoft's browser Internet Explorer featured a tool called Tracking Protection, which enabled users to opt out of being tracked by cookies and other technologies by the websites they visited. When a user turns on the Tracking Protection, they can either download or create a personalised list of third-party websites that will be prevented from collecting user data (Microsoft, 2010, 2011). In addition, Microsoft has been a long-time supporter of the Do Not Track standard (Microsoft, 2015f). Like Google, Microsoft also created a dashboard where users can turn off personalised advertising from Microsoft's Windows and its applications, and from all other services that customers use with their Microsoft account (Microsoft, 2015a).

Table 1: Privacy choice by Google and Microsoft

| Choice via opt-in and opt-out tools and consent | | Google | Microsoft |
|---|---|---|---|
| Location information | Wi-Fi data opt-out | √ | NA |
| | Centralised opt-out | √ | √ |
| Personal information | TOS and privacy policy consent | √ | √ |
| Tracking | Do Not Track opt-in | √ | √ |
| | No tracking browser extensions opt-in | √ | √ |
| | Incognito browsing opt-in | √ | √ |
| | Browser cookie opt-out | √ | √ |
| Interest-based advertising | Centralised opt-out | √ | √ |

This brief overview demonstrates that Google and Microsoft have codified notice and choice into their policies and added privacy control tools to enable users to customise their privacy preferences. Undoubtedly, these changes can be valuable in some contexts but they have had no substantial impact on users' ability to stay anonymous, control uses of information about themselves, and minimise many potential risks such as inhibition of expression, information inequality, profiling, discrimination, etc. First of all, not all users read policies to give their informed consent to intermediaries (e.g. Smith, 2014). Second, privacy policies do not capture privacy implications of intermediaries' ever growingly complex data practices such as the extent of data flows among devices, platforms, advertising networks, and third parties. Third, while users may give consent to the practices of intermediaries at the time of registration, intermediaries reserve the right to make changes to their policies without asking users' consent again, greatly undermining the purpose of consent. Moreover, the dichotomy between personal and non-personal information is misleading. Even anonymised data sets can be deanonymised to reveal information about specific individuals (Mayer-Schönberger & Cukier, 2013; Ohm, 2010).

Justifiably, users have a choice to decline to provide information to companies but need to be prepared to be denied the service. Google, for example, will not allow users to create a Gmail account without providing their phone number (Google, n.d.-b). Users of Google's and Microsoft's services can also opt out of receiving interest-based advertising but it does not mean companies stop collecting information about users. For example, Google warns users that opting out of personalised advertising does not stop the company from serving ads to users. Simply, instead of serving ads based on interests and browsing behaviour, the company delivers ads based on more general attributes such as browser type, location information, search terms, and more (Google, n.d.-a). Google and Microsoft also give their users the option to turn off location tracking on their mobile applications and from their centralised privacy dashboard. However, sometimes intermediaries make it challenging for users to easily opt out. Google phone users, for example, found out that Google Play—which is the app store in Android phones—was tracking their location in the background. If any app on a user's phone needed to access location, it had to do it through Google Play, the central provider of the location services. It means that if users disabled location tracking in Google Play, none of their apps could access their location. Similarly, if users chose to enable location tracking in a single app, they had to grant location tracking to Google as well (Ducklin, 2016). Moreover, even if users completely turn off location in all of Google's and Microsoft's services, these intermediaries can still locate users, albeit approximately, based on their IP address. Ultimately, if a user has a Google or Microsoft account, the intermediary collects his/her contact information, location (IP) and device identifiers, usage data and content of communication with no option to opt-out.

Thus, the evolution of information intermediaries' policies towards notice and choice do not necessarily provide users with means to define the condition of their privacy and the uses of their information. With users' reliance on endless applications on personal computers and mobile phones, and companies' constant data exchange with partners who engage in their own online and offline information collection, intermediaries are still able to collect data on users' behaviours and interests and use it in various contexts. Hence, safeguarding users' privacy does not depend on control but on these companies' practices and decision that take place beyond the content level of services. Information intermediaries have historically made decisions that advance their strategic interests, sometimes violating notice and choice principles.

## INTERMEDIARIES' DISREGARD FOR NOTICE AND CHOICE

In 2012, Google announced that it would consolidate privacy policies from over 60 services to legitimise merging user data collected and generated from and by users on its numerous services. While the policy change would allow Google account holders to seamlessly navigate from Google Maps to YouTube to Search to Google Plus to Gmail and Google Drive with single account credentials, it also enabled personalisation of one service based on user data collected from across all of these services. Google presented the policy change as a simplification and addition of conveniences for users, but it raised privacy flags (Google, 2012a, 2012b). Regulators in the EU and US and privacy groups strongly opposed the policy change questioning its legality and observance with the notice and consent privacy principles. In the US, Congress members sent a letter to Google raising concerns about Google's compliance with the FTC's settlement agreement following an earlier privacy violation (Bartz & Richwine, 2012). Similarly, attorneys general from 35 states sent a letter to Google criticising its intent to change its privacy policy without allowing users to opt-in or out of the modification and expressed worries about privacy

risks associated with Google's expanding ability to create richer user profiles under the new privacy policy (Paulson, 2012).

The Transatlantic Consumer Dialogue (TACD), which is a forum of US and EU consumer groups, also followed suit with a letter to Google's CEO, asking the company to suspend the privacy policy consolidation plan. The letter stated that combining and repurposing data provided by users in different contexts and for different purposes without consent was an unwise choice (Mello, 2012; TACD, 2012). US privacy groups even filed a lawsuit against the FTC to compel the agency to enforce its earlier consent order by prohibiting Google's policy change (EPIC, 2012). Moreover, consumer groups argued that in a complaint filed with the FTC that Google misled its users by failing to accurately describe that the real motives behind its consolidation of policies was to gain increased access to more user data for advertising opportunities (Chester, 2012; Mills, 2012). In fact, according to the *Wall Street Journal* Google's sales representatives informed advertising agencies about their new advertising potential with the consolidation of the privacy policy (Efrati, 2012). For example, Google collects personal information, content of e-mails and contacts of its e-mail users to show them advertising. With the changed policy the company could use content of e-mails with the user's YouTube browsing and his/her location history to make analytic inductions about the user's behaviour to identify more nuanced interests and enable its clients to design marketing messages and products accordingly (Sullivan, 2012).

Privacy agencies in Europe also widely criticised Google's plans. France's data protection agency (CNiL) officials announced that their preliminary assessment of the policy indicated a violation of European privacy rules and urged Google to reconsider its policy decision (Pfanner, 2012). The EU data protection authorities wanted to halt the changes until a formal investigation would determine whether the new policy was in compliance with the European data protection principles. However, Google ignored the extensive pressure from government officials and non-profits and enforced its new privacy policy (Efrati, 2012; Google, 2012a). Two years later Microsoft followed suit and also consolidated its privacy policies into one document and reserved the right to collect and analyse user data from one service to improve service quality, security, and offer tailored content in another service (Gutiérrez, 2015). Like Google, Microsoft did not obtain user consent in advance of the update and simply stated that by using its services, consumers automatically agreed that their data may be used, modified, distributed and displayed upon necessity to improve Microsoft products and services (Bishop, 2012; Microsoft, 2012b; Toor, 2012).

This case demonstrates that when intermediaries' market interests are concerned, they are willing to defy authorities' requests and recommendations and disregard their privacy commitments under self-regulatory agreements. Ceasing data integration would have cost Google and Microsoft long-term loss in marketing and advertising opportunities, and hence they ignored the fierce pressure and implemented a fundamental policy change risking legal action and financial penalties in Europe (Arthur, 2013; CNiL, 2013; Schechner, 2013; Souppouris, 2013).

Disregard for privacy commitments during consolidation of privacy policies, however, was not an isolated case. During the implementation of its Street View project Google compiled publicly accessible routers' Medium Access Control (MAC) addresses, which is a unique hardware number, and SSIDs, such as network names, to improve its location services. Simultaneously, supposedly by mistake, the company also collected information sent over public Wi-Fi networks, including e-mails, passwords, and financial information without users' knowledge or consent.

Google's unauthorised collection of personal information went undetected for two years until the German Data Protection Authority (DPA) made it public in 2010 (Kiss, 2010). The incident was highly publicised in the media and criticised by regulators globally, leading to many formal investigations into the company's data collection incident in Europe and in the US. At least nine countries determined that Google violated their privacy law by capturing and storing personal data without authorisation including the Netherlands, France, Germany, and Spain (EPIC, 2010; Paul, 2010).

In the Netherlands alone, Google captured information on more than 3.6 million routers, equivalent of 63% of the households and companies with broadband connection. The radio antenna attached to Google cars recorded publicly broadcast Wi-Fi radio signals enabling the company to collect unique MAC addresses for each of these routers; the strength of the signal; and the name of the network (Dutch DPA, 2010; Google, 2010). In addition, Google obtained large scale of personal data from unencrypted networks, including names, phone numbers, hardware identifiers, and more than 16,000 e-mail addresses. As a result, the Dutch DPA concluded that Google violated the Personal Data Protection Act on many accounts by not having a justified reason for such data collection and by failing to provide notice to data subjects and obtain their consent in advance. Moreover, the Dutch DPA established that the router MAC addresses in combination with the location information constitute personal data as they can lead to the revelations of the identities of routers' owners (Dutch DPA, 2010; Kravets, 2012; O'brien, 2013).

In the aftermath of investigations and negative publicity, Google made a few amendments to its privacy practices. The company also announced that it would build effective privacy controls into its products and internal practices; train its employees on the responsible collection and use of data; and document privacy design initiatives. Further, Google introduced a method to allow users to opt out of having their wireless access point included in Google's data collection for location services (Google, 2011a, 2011b). Nonetheless, such opt-out tools and promises do not guarantee against unethical and unauthorised use of information by intermediaries. In fact, in 2012 Google was caught tracking users without their knowledge and consent by circumventing the privacy settings of Microsoft Explorer and Safari, which blocks third-party tracking cookies by default. Framed as a mistake again, the incident undermined the effectiveness of the training programmes and other internal changes that Google promised to implement after the Wi-Fi data collection controversy (Mayer, 2012; Microsoft, 2012a; Valentino-Devries, 2012). Thus, these cases demonstrate information intermediaries' discretionary power to make decisions that prioritise their strategic interests over privacy commitments.

# CONCLUDING REMARKS

The rationale of this paper was a) to demonstrate that participation in self-regulatory programmes and the implementation of privacy principles by information intermediaries does not necessarily translate into meaningful privacy safeguards for users in the face of growing technical affordances that enable greater surveillance capacity online; and b) to highlight the discretionary power of information intermediaries to set their policies and practices with opportunistic regard for their privacy commitments in order to prioritise their strategic interests. In exploring the implementation of notice and choice framework as a case study into information intermediaries' behaviour, this paper has highlighted that despite growth in privacy awareness and a number of policy changes, information intermediaries have not reduced the amount of data they collect and process about users. These private companies have mastered the

strategy of implementing seemingly privacy-centric policies and tools without compromising their economic interests. Policy changes towards notice and choice and privacy controls are all positive developments but they have not affected intermediaries' surveillance and subsequent implications for anonymous expression and privacy risks. Instead, they may have enabled intermediaries to justify their ever-growing data processing activities based on the idea that users agree to their privacy terms. The discussions of the policies and cases in this paper have implications for policymakers and civil society actors by highlighting that participation in self-regulatory frameworks and update of policies does not mean control over information and protection from misuse of information and various risks. Moreover, there is precedent to believe that without strong enforcement mechanisms, information intermediaries may continue to set and enact policies in a manner consistent with their business interests, even if that means violating privacy commitments. In this light, it is worth acknowledging that the Privacy Shield that has replaced the Safe Harbor agreement might be slightly superior to the latter in having better oversight mechanisms. However, it is still fundamentally based on privacy principles that rely on notice and choice principles (among others), putting the burden on users to read, understand, and agree to information practices despite the questionable utility of such an approach. Instead, the privacy principles that government agencies endorse and enforce should shift responsibility on the companies. After all, in the current information environment there is an inherent power differential between users and information intermediaries, who are the ones designing the platforms and setting the rules of engagement.

## REFERENCES

Angwin, Julia, & Valentino-DeVries, Jennifer. (2010). The Information That Is Needed to Identify You: 33 Bits. *Wall Street Journal.* http://blogs.wsj.com/digits/2010/08/04/the-information-that-is-needed-to-identify-you-33-bits/

Arthur, Charles. (2013, July 5). European watchdogs order Google to rewrite privacy policy or face legal action, *The Guardian*. Retrieved from https://www.theguardian.com/technology/2013/jul/05/google-privacy-policy-legal-action

Bartz, Diane, & Richwine, Lisa. (2012, January 27). Lawmakers press Google on privacy policy changes, *Reuters*. Retrieved from http://www.reuters.com/article/us-google-privacy-idUSTRE80P1YC20120127

Bennett, Colin , & Raab, Charles (2006). *The governance of privacy: Policy instruments in global perspective*. Cambridge, MA: MIT Press.

Bishop, Todd. (2012). Microsoft gives itself more leeway in new online services user agreement. *GeekWire.* http://www.geekwire.com/2012/terms-service-give-microsoft-leeway-integrate/

Chander, Anupam, & Le, Uyen P. (2015). Data Nationalism. *Emory Law Journal, 64*(3).

Chester, Jeff. (2012, February 22). CDD to FTC: Google Violated Buzz Consent Decree by Failing to Inform Consumers Real Reasons for its Expanded Data Practices. Retrieved from https://www.democraticmedia.org/content/cdd-ftc-google-violated-buzz-consent-decree-failing-inform-consumers-real-reasons-its

CIGI. (2014). CIGI-Ipsos Global Survey on Internet Security and Trust. Retrieved from https://www.cigionline.org/internet-survey

CNiL. (2013). CNIL orders Google to comply with the French Data Protection Act, within three months. Retrieved from https://www.cnil.fr/fr/node/15570

Cohen, Julie E. (2012). What privacy is for. *Harv. L. Rev., 126*, 1904.

Craddock, Dick. (2013). Outlook.com: 400 million active accounts, Hotmail upgrade complete and more features on the way. Retrieved from http://blogs.office.com/b/microsoft-outlook/archive/2013/05/02/outlook-com-400-million-active-accounts-hotmail-upgrade-complete-and-more-features-on-the-way.aspx

Culnan, Mary J, & Bies, Robert J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of social issues, 59*(2), 323-342.

Deibert, Ronald. (2013). *Black code : inside the battle for cyberspace*. Toronto: McClelland & Stewart.

DeNardis, Laura. (2012). Hidden levers of internet control: An infrastructure-based theory of Internet governance. *Information, Communication & Society, 15*(5), 720-738.

DiLascio, Tracey. (2004). How Safe Is the Safe Harbor-US and EU Data Privacy Law and the Enforcement of the FTC's Safe Harbor Program. *BU Int'l LJ, 22*, 399.

Ducklin, Paul. (2016, September 13). How Google Play tracks you even if your other apps don't, *Sophos*. Retrieved from https://nakedsecurity.sophos.com/2016/09/13/how-google-play-tracks-you-even-if-your-other-apps-dont/

Dutch DPA. (2010). Final findings: Dutch Data Protection Authority investigation into the collection of WiFi data by Google by using Street View Cars. Retrieved from https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/en_pb_20110811_google_final_findings.pdf

Efrati, Amir. (2012, February 1). Google Defends New Privacy Policy, *The Wall Street Journal*. Retrieved from http://www.wsj.com/articles/SB10001424052970204740904577195083676240406

EPIC. (2010). Investigations of Google Street View. Retrieved from https://epic.org/privacy/streetview/

EPIC. (2012). EPIC v. FTC (Enforcement of the Google Consent Order). Retrieved from https://epic.org/privacy/ftc/google/consent-order.html

Export.gov. (2015). Welcome to the U.S.-EU Safe Harbor. Retrieved from http://export.gov/safeharbor/eu/eg_main_018365.asp

Farrell, Henry. (2003). Constructing the international foundations of e-commerce—The EU-US Safe Harbor Arrangement. *International Organization, 57*(02), 277-306.

Feeley, Matthew J. (1999). EU Internet regulation policy: The rise of self-regulation. *BC Int'l & Comp. L. Rev., 22*, 159.

FTC. (2000). Privacy Online: Fair Information Practices In The Electronic Marketplace. *A Report To Congress*. Washington, DC.

FTC. (2011). FTC Charges Deceptive Privacy Practices in Googles Rollout of Its Buzz Social Network, Retrieved from https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz

FTC. (2012). Protecting Consumer Privacy In an Era of Rapid Change: Recommendations for Businesses and Policymakers. Washington, DC.

Gellman, Robert, & Dixon, Pam. (2011, October). Many failures: A brief history of privacy self-regulation in the united states. Retrieved from http://www.worldprivacyforum.org/wp-content/uploads/2011/10/WPFselfregulationhistory.pdf

Google. (2010, April 27). Data collected by Google cars. Retrieved from http://googlepolicyeurope.blogspot.com/2010/04/data-collected-by-google-cars.html

Google. (2011a, November 14). Greater choice for wireless access point owners. Retrieved from https://googleblog.blogspot.com/2011/11/greater-choice-for-wireless-access.html

Google. (2011b, September 13). A new option for location-based services. Retrieved from http://googlepolicyeurope.blogspot.com/2011/09/new-option-for-location-based-services.html

Google. (2012a, February 29). Google's new Privacy Policy. Retrieved from

https://googleblog.blogspot.com/2012/02/googles-new-privacy-policy.html

Google. (2012b, January 24). Updating our privacy policies and terms of service. Retrieved from https://googleblog.blogspot.com/2012/01/updating-our-privacy-policies-and-terms.html

Google. (2014a, April 14). Google Terms of Service. Retrieved from https://www.google.com/policies/terms/

Google. (2014b). Google Transparency Report. Retrieved from http://www.google.com/transparencyreport/userdatarequests/countries/

Google. (2014c). HTTPS as a ranking signal. Retrieved from https://googleonlinesecurity.blogspot.com/2014/08/https-as-ranking-signal_6.html

Google. (2015a). Opt Out. *Ads Help*. Retrieved from https://support.google.com/ads/answer/2662922?hl=en&ref_topic=2941003

Google. (2015b). Privacy Policy. *Google Privacy and Terms*. Retrieved from https://www.google.com/policies/privacy/

Google. (n.d.-a). Advertising. *Google Privacy and Terms*. Retrieved from https://www.google.com/policies/technologies/ads/

Google. (n.d.-b). Create your Google Account. Retrieved from https://accounts.google.com/signup

Greenwald, Glenn. (2013, June 7 ). NSA Prism program taps in to user data of Apple, Google and others, *The Guardian*. Retrieved from http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Greenwald, Glenn. (2014). *No place to hide: Edward Snowden, the NSA, and the US surveillance state*. New York, NY: Metropolitan Books.

Gutiérrez, Horacio. (2015). Improving the Microsoft Services Agreement and Privacy Statement for consumers. Retrieved from http://blogs.microsoft.com/blog/2015/06/04/improving-the-microsoft-services-agreement-and-privacy-statement-for-consumers/

Hoffman, Chris. (2015, August 3). 30 Ways Your Windows 10 Computer Phones Home to Microsoft. Retrieved from http://www.howtogeek.com/224616/30-ways-windows-10-phones-home/

Hosein, Gus. (2010). No hiding place. *Index on censorship, 39*(1), 58-68.

House, The White. (2012). Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy. Washington, DC.

ITA. (2016). EU-U.S. Privacy Shield Program Overview. Retrieved from https://www.privacyshield.gov/Program-Overview

King, Nancy J., & Jessen, Pernille Wegener. (2010). Profiling the mobile customer – Is industry self-regulation adequate to protect consumer privacy when behavioural advertisers target mobile phones? – Part II. *Computer Law & Security Review, 26*(6), 595-612. doi:

http://dx.doi.org/10.1016/j.clsr.2010.09.007

Kiss, Jemima. (2010, May 14). Google admits collecting Wi-Fi data through Street View cars, *The Guardian*. Retrieved from www.theguardian.com/technology/2010/may/15/google-admits-storing-private-data

Kravets, David. (2012, May 2). An Intentional Mistake: The Anatomy of Google's Wi-Fi Sniffing Debacle, *Wired*. Retrieved from https://www.wired.com/2012/05/google-wifi-fcc-investigation/

Lardinois, Frederic. (2015, May 28). Gmail Now Has 900M Active Users, 75% On Mobile. Retrieved from http://techcrunch.com/2015/05/28/gmail-now-has-900m-active-users-75-on-mobile/

Lee, Ya-Ching. (2003). Will self-regulation work in protecting online privacy? *Online Information Review, 27*(4), 276-283.

MacKinnon, Rebecca. (2012). *Consent of the networked: The worldwide struggle for Internet freedom*. New York, NY: Basic Books.

Madden, Mary. (2014, November 12). Public Perceptions of Privacy and Security in the Post-Snowden Era. Retrieved from http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/

Mayer-Schönberger, Viktor, & Cukier, Kenneth. (2013). *Big data: A revolution that will transform how we live, work, and think*. London, UK: John Murray Publishers

Mayer, Jonathan. (2012, February 17). Safari Trackers. Retrieved from http://webpolicy.org/2012/02/17/safari-trackers/

Mello, John P. (2012, February 29). Multinational Consumer Group Asks Google to Delay Privacy Changes, *PCWorld*. Retrieved from http://www.pcworld.com/article/251058/multinational_consumer_group_asks_google_to_delay_privacy_changes.html

Microsoft. (2000, July 20). Microsoft Announces New Cookie Management Features For Internet Explorer 5.5. Retrieved from http://news.microsoft.com/2000/07/20/microsoft-announces-new-cookie-management-features-for-internet-explorer-5-5/#xojGUzzoApBpVe7a.97

Microsoft. (2008, August 25). IE8 and Privacy. Retrieved from https://blogs.msdn.microsoft.com/ie/2008/08/25/ie8-and-privacy/

Microsoft. (2010, December 7). IE9 and Privacy: Introducing Tracking Protection. Retrieved from https://blogs.msdn.microsoft.com/ie/2010/12/07/ie9-and-privacy-introducing-tracking-protection/

Microsoft. (2011). Tracking Protection. Retrieved from http://windows.microsoft.com/en-us/internet-explorer/products/ie-9/features/tracking-protection

Microsoft. (2012a, February 20). Google Bypassing User Privacy Settings. Retrieved from https://blogs.msdn.microsoft.com/ie/2012/02/20/google-bypassing-user-privacy-settings/

Microsoft. (2012b). Microsoft Services Agreement. Retrieved from https://www.microsoft.com/en-us/servicesagreement/default.aspx

Microsoft. (2015a). About our Ads. Retrieved from https://choice.microsoft.com/en-us/opt-out

Microsoft. (2015b, June 15). Bing Moving to Encrypt Search Traffic by Default. Retrieved from https://blogs.bing.com/webmaster/2015/06/15/bing-moving-to-encrypt-search-traffic-by-default/

Microsoft. (2015c). Cortana: Privacy Statement. Retrieved from https://privacy.microsoft.com/en-us/privacystatement/

Microsoft. (2015d). Cumulative Security Update for Internet Explorer. *Security TechCenter*. Retrieved from https://technet.microsoft.com/library/security/MS15-056

Microsoft. (2015e). Microsoft Privacy Statement. Retrieved from https://www.microsoft.com/en-us/privacystatement/

Microsoft. (2015f, April 3). An update on Microsoft's approach to Do Not Track. Retrieved from http://blogs.microsoft.com/on-the-issues/2015/04/03/an-update-on-microsofts-approach-to-do-not-track/

Microsoft. (2015g). Windows: Privacy Statement. Retrieved from https://privacy.microsoft.com/en-US/privacystatement

Miller, Claire Cain. (2014, March 21). Revelations of N.S.A. Spying Cost U.S. Tech Companies, *The New York Times*. Retrieved from http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html

Mills, Elinor. (2012). Consumer group files FTC complaint against Google, *CNET*. Retrieved from http://www.cnet.com/news/consumer-group-files-ftc-complaint-against-google/

Montjoye, Yves-Alexandre de, Radaelli, Laura, Singh, Vivek Kumar, & Pentland, Alex "Sandy". (2015). Unique in the shopping mall: On the reidentifiability of credit card metadata. *Science, 347*(6221), 536-539. Retrieved from http://www.sciencemag.org/content/347/6221/536.abstract

O'brien, Kevin J. (2013). Germany Fines Google Over Data Collection, *The New York Times*. Retrieved from http://www.nytimes.com/2013/04/23/technology/germany-fines-google-over-data-collection.html

OECD. (2013). The OECD Privacy Framework. Retrieved from https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

OECD. (2014). OECD Principles for Internet Policy Making. Retrieved from http://www.oecd.org/sti/ieconomy/oecd-principles-for-internet-policy-making.pdf

Ohm, Paul. (2010). Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA law review, 57*, 1701.

Paul, Ian. (2010, Jun 22). Google Under Multistate Privacy Microscope: How We Got Here,

*PCWorld* Retrieved from http://www.pcworld.com/article/199508/Google_Under_Multistate_Privacy_Microscope_How_We_Got_Here.html

Paulson, David. (2012, February 22). Attorney General Gansler Challenges Google on New Privacy Policy. Retrieved from https://www.oag.state.md.us/Press/2012/022212a.html

Pfanner, Eric. (2012, February 28). France Says Google Privacy Plan Likely Violates European Law, *The New York Times*. Retrieved from http://www.nytimes.com/2012/02/29/technology/france-says-google-privacy-plan-likely-violates-european-law.html?_r=0

Pickard, Victor. (2013). Social democracy or corporate libertarianism? Conflicting media policy narratives in the wake of market failure. *Communication Theory, 23*(4), 336-355.

Popescu, Mihaela, & Baruh, Lemi. (2013). Captive But Mobile: Privacy Concerns and Remedies for the Mobile Environment. *Information Society, 29*(5), 272-286. doi: 10.1080/01972243.2013.825358

Rubinstein, Ira. (2011). Privacy and regulatory innovation: Moving beyond voluntary codes. *I/S, A Journal of Law and Policy for the Information Society, 6*, 356.

Sargsyan, Tatevik. (2016). Data Localization and the Role of Infrastructure for Surveillance, Privacy, and Security. *International Journal of Communication; Vol 10 (2016)*.

Schechner, Sam. (2013, September 27). French Privacy Agency Moves to Sanction Google, *The Wall Street Journal*. Retrieved from http://www.wsj.com/articles/SB10001424052702303342104579101250040525172

Schwaig, Kathy Stewart, Kane, Gerald C, & Storey, Veda C. (2006). Compliance to the fair information practices: How are the Fortune 500 handling online privacy disclosures? *Information & management, 43*(7), 805-820.

Scott, Mark. (2015, October 6). Data Transfer Pact Between U.S. and Europe Is Ruled Invalid, *The New York Times*. Retrieved from http://www.nytimes.com/2015/10/07/technology/european-union-us-data-collection.html?_r=1

Senden, Linda. (2005). Soft Law, Self-Regulation And Co-Regulation In European Law: Where Do They Meet? *Electronic Journal of Comparative Law, 9*(1).

Smith, Aaron. (2014, December 4). Half of online Americans don't know what a privacy policy is. Retrieved from http://www.pewresearch.org/fact-tank/2014/12/04/half-of-americans-dont-know-what-a-privacy-policy-is/

Solove, Daniel J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, 154 (3), 477-560.

Souppouris, Aaron. (2013, April 2). Google braces for fines in Europe over privacy policy, *The Verge*. Retrieved from http://www.theverge.com/2013/4/2/4173652/eu-google-privacy-policy-cnil-investigation-conc

lusion

Steele, Elisa. (2013). Skype Celebrates a Decade of Meaningful Conversations! Retrieved from http://www.skype.com/en/about/

Streitfeld, David. (2012, June 19). Google Responds to New British Investigation of Street View. Retrieved from http://bits.blogs.nytimes.com/2012/06/19/google-responds-to-new-british-investigation-of-street-view/

Sullivan, Danny. (2012, January 24). Google's New Terms of Service & Privacy Policy: Anything You Do May Be Used To Target You?, *Marketing Land*. Retrieved from http://marketingland.com/google-terms-of-service-privacy-policy-4293

Sullivan, Danny. (2015, September 18). How Google Now, Siri & Cortana Predict What You Want, *Search Engine Land*. Retrieved from http://searchengineland.com/how-google-now-siri-cortana-predict-what-you-want-229799

TACD. (2012, February 29). Trance Atlantic Consumer Dialogue Google Letter. Retrived from https://epic.org/privacy/ftc/google/TACD-Google-Letter.pdf

Tene, Omer. (2008). What Google Knows: Privacy And Internet Search Engines. *Utah law review, 2008*(4), 1433-1492.

Toor, Amar. (2012, September 2). Updated services agreement allows Microsoft to integrate content across cloud properties. *The Verge*. Retrieved from http://www.theverge.com/2012/9/2/3285455/microsoft-updates-services-agreement-privacy-class-action-waiver

Valentino-Devries, Jennifer. (2012, February 16). How Google Tracked Safari Users, *The Wall Street Journal*. Retrieved from http://blogs.wsj.com/digits/2012/02/16/how-google-tracked-safari-users/

Weber, Rolf H. (2013). How Does Privacy Change in the Age of the Internet. In K. B. Christian Fuchs, Anders Albrechtslund & Marisol Sandoval (Ed.), *Internet and Surveillance: The Challenges of Web 2.0 and Social Media,* New York: Routledge.

Zimmer, Michael. (2010). Privacy Protection in the Next Digital Decade: "Trading Up" or a "Race to the Bottom"? In B. Szoka & A. Marcus (Eds.), *The Next Digital Decade: Essays On The Future Of The Internet*. Washington, D.C.: TechFreedom.