Title: Is Privacy The Future of Online Marketing?

Authors: Sveta Milyaeva and Daniel Neyland

Introduction

The online data industry continues to grow at a rapid pace. This growth is fueled by the monetization of online data. The monetization of data takes place through an ever more bewildering array of activities, devices, algorithms and human practices. The details of monetization remain unclear at best to many online users, whose data is transformed into profiles through which they can be targeted with adverts that supposedly match their interests. In the same way that many of the activities of the online advertising industry such as real-time auctioning of advertising space remain distanced from users, so do the profits made from data. Users' data is mined, scraped, collated, analysed and turned into a profitable commodity with no return received by the users. Various commentators suggest this position creates asymmetries of access, information, power and profit, and compromises users' privacy.

What should be done? Drawing on recent research, this report provides an analysis of the ever expanding online data industry and the various ways in which problems are offered to be resolved. The report begins with a description of the often opaque devices and practices of the industry. Then we consider regulatory responses to the industry, how these frame what precisely the problem is and the challenges regulators face. We then turn attention to the emerging (mostly start-up) firms who seek to make an intervention and change the terms of exchange in the online data industry. Finally we conclude with a suggestion that in examining the online data industry, careful consideration is required of what constitutes privacy, how privacy issues could be resolved and what these resolutions imply.

Personal data collection

How to 'make money without doing evil'? Put forward in 1998, this is the mission statement Google's CEO Larry Page had to revisit lately. In his interview with the *Financial Times* he admitted, 'The societal goal is our primary goal. We've always tried to say that with Google. I think we've not succeeded as much as we'd like' (Waters 2014). Google's business model – to provide information free of charge to individual online users but charge advertisers for access to personal information – is what makes this and other companies' (such as Facebook) advertising revenues soar.[1]

The access to personal information provided by Google and similar companies lays the grounds for behavioural advertising. Such advertising is driven by personal information that is collected (mined) in different ways. Internet searches, online shopping and payments, personal communications are the personal data that fuels the online data industry – the advertisers and data brokers. Data is collated and shared through, amongst other things[2]:

- *Cookies*: these are placed on an individual's browser by a third-party that rides on a website the individual visits; and if this third-party belongs to a network the personal data spreads widely and the individual's footprints are identified across the web[3].
- *Browser fingerprinting*: this involves collecting information about, or the 'fingerprint' of one's browser – its font, language, version and operating system. Through fingerprinting it is possible to identify its user.
- *Deep packet inspection*: where internet service providers offer online activity information to third parties.
- *History sniffing*: allowing a website to run a code that gets information on hyperlinks that a user clicked on.
- *Onboarding*: a tool that enables consumers' offline activities to be matched with online ones.
- *Data mining*: integrates different data sets (including offline data sets) to produce more information.

- *Mobile devices*: smartphone applications (mobile games, etc.) collect and share data with advertisers

The gathered personal data is then monetized. That is, it is sold to marketers to make their advertising more effective, thus increasing their revenues. Behavioural advertising (or interest-based advertising) delivers advertisements to screens and mobile devices. It is targeted at an online user and is enabled by, for example, 'registration targeting'.

In 2013 Facebook allied with data brokers Epsilon, Acxiom, Datalogix and BlueKai 'to allow brands to match data gathered through shopper loyalty program to individual Facebook profiles'; in 2014 Facebook unveiled a platform that lets advertisers target Facebook users not just on the website, but everywhere on the web and on all devices as well as offline (Constine 2013; Delo 2013; Goel 2014). The above mentioned partnership of Facebook with the data brokers is an example of 'registration targeting' where data brokers help a registration website (a user has to sign in to get a service the website provides) to boost its revenues by customising advertisement it displays to its members. Because a data broker has its own unique database of customer profiles, it searches them both – their own customer database and the database of registered users - to find matches and see which advertisement is most effective; this database matching also helps to broker a profitable partnership between a registration website and an advertiser.

These kinds of activities have raised numerous concerns, including questions of privacy, control, data ownership, who monetises data, and who benefits from monetisation. We will explore these concerns first through regulators and secondly through online data entrepreneurs, start-ups and other data intensive firms.

US Regulators (2009-2015)

Concerned with the lack of transparency in online targeted advertising, in 2009 the Federal Trade Commission, which is responsible for consumer protection in the US, published the 'Self-Regulatory Principles for Online Behavioral Advertising' to

encourage public discussion of the issue and to nudge industry in the direction of developing a considerate attitude towards data collection (FTC 2009). However, in February 2012 the Obama Administration released a report that stated that principles cannot be implemented through self-regulation alone. It also affirmed consumers' rights to control how personal data is collected online. The report stated that these rights 'should be reflected in a privacy law and [the Administration] will work with Congress to enact these rights' (White House 2012).

However, two years later, in February 2014, an association of public activist bodies[4] wrote a letter to the President, urging him to fulfill the Bill's promise 'to update the privacy laws of the United States', a promise which had been 'largely ignored by Congress' (Hamburger 2014). By 'largely ignored' the coalition referred to the fact that since 2012 there was just one bill introduced in February 2014 by Congress – the Data Broker Accountability and Transparency Act. It would 'require data brokers to establish procedures to ensure the accuracy of collected personal information' and gives FTC the power to enforce it (US Congress 2014). However, its estimated chance of enactment is 15 per cent as it has to get approved by the Senate Committee on Commerce, Science, and Transportation, the Senate, the House of Representatives, and finally signed by the President, and (although it was re-introduced in Senate in April 2015) by July 2015 it had not passed the Committee yet.[5]

This lack of progress was also confirmed by a report issued by the Executive Office of the President: 'Big Data: Seizing Opportunities, Preserving Values'. The report advised the Administration to 'advance the Consumer Privacy Bill of Rights' by creating and passing it through Congress (White House 2014: 60). Its twin report, which was produced by the President's Council of Advisors on Science and Technology (PCAST) provided further support to this notion of taking privacy seriously. The report suggested that current Notice and Consent policies for online users create "a non-level playing field" through a lack of clear information, placing the burden of privacy protection on the individual, offered in take it or leave it terms. These issues, the PCAST report concluded, amount to: "a kind of market failure" (PCAST 2014: xi-xii).

Also in May 2014 the FTC published a report that detailed the results of a study of nine data brokers that the Commission initiated in 2012. The aim was to produce a report on the ways in which the data broker industry operates, in order to make the industry's practices more transparent and raise consumer awareness. The report concluded that the industry utilizes a vast number of data sources (online as well as offline), its practices of data collection are unknown to consumers, and could be very sensitive as the analytics are based on inferences that might harm consumers in numerous ways[6]. The Commission also issued legislative recommendations to address the lack of transparency in the industry's data collection practices and urged the US Congress to think about putting forward legislation that enables a consumer to negotiate data collection (FTC 2014).

As a result, by 2015, it could be said that a certain pressure was put on the online data industry (data brokers and advertisers) to develop more rigorous principles of self-regulation. However, these efforts also went beyond self-regulation. The Federal Trade Commission joined with the White House and privacy advocates in pushing Congress to legislate on online commercial surveillance.

The response from the online data industry has been clear in its emphasis on the importance of free-flowing data for economic growth. In her reply to the comments made by the FTC Commissioner Julie Brill (2013) about data brokers, at that time the President and CEO of the Direct Marketing Association (an alliance of data-driven marketers), pointed out that 'third-party data use and sharing are essential for business success in today's information economy' (Wooley 2013).

These debates, raising concerns of privacy in opposition to economic growth, has also been mirrored in European legislative development. In the next section we will outline the new European Data Protection Regulation and the controversies surrounding its enactment.

EU Regulators

Concerns regarding online data collection in Europe are addressed by a number of legislative bodies at the national and European levels. The legislation that contains the current regulatory principles for online data collection (by both private business and public organisations) was adopted by the European Commission in October 1995. The 95/46 Directive (also known as the Data Protection Directive) is viewed as the text that laid out the foundations for personal data treatment in Europe (EU 1995). In July 2002, with rapid development and changes in electronic communications, the Data Protection Directive was supplemented with the Electronic Privacy Directive. It regulates the processing of personal electronic data and puts an emphasis on disclosing information on the use of cookies, enabling users to opt-out (EU 2002). Continuous advances in online communications resulted in the introduction of an amendment of the Electronic Privacy Directive; the EU 'Cookie' Directive 2009 put in place more stringent rules on cookies' use (EU 2009).

In January 2012, after two years of assessment of the field of online communications, the European Commission proposed a major legislative change to replace the existing legal framework with a new Data Protection Regulation (EC 2012). As a Directive, the 1995 legislation serves as guidance that is adaptable by member states through national data protection authorities. The new legislation will be a Regulation, applied in the same way across all EU Member States. The idea is to harmonise EU data protection through the Regulation.

The proposed measures can be divided into two groups. The first group caters for data and privacy protection in its focus on (1) consent (unlike the Directive, the Regulation requires users to opt-in rather than opt-out of data collection); (2) a right to be forgotten (a user has a right to request to delete personal data – and links to it – that is outdated or irrelevant); and (3) a demand for data controllers (organisations and businesses involved in processing personal data) to be transparent and pro-active in their compliance with data protection requirements (EC 2012a)..

Given that one of the European Commission priorities for 2015 is the Digital Single Market[7], the second group of proposed measures could be viewed as aiming to enable the EU Single Market by encouraging free flows of data. These include (1) the concept of a 'one-stop shop' applicable to data controllers operating across Europe and being supervised solely by a data protection authority of a country where their headquarters are located (currently data protection authorities of countries where complaints are made against a data controller deal with the data controller); (2) relaxed registration rules for data controllers (EC 2012a).

To be enacted, both chambers of the European legislative body – the European Parliament and the Council of Ministers – must adopt the proposed Regulation. In March 2014, two months before the European Parliament was dissolved for the election, it voted in favour of the Regulation (EC 2014).. However, despite the hopes of those pushing the law forward, the Council could not reach a common position on the Regulation voted for by the Parliament (EU 2014, Levy-Abegnoli 2015). It would seem that the EU Justice Ministers (who comprise the Council) could not agree on how to enforce businesses to comply with the new law. In particular, the UK Justice Minister argued that 'the Commission both overestimates the benefits achieved through harmonised EU data protection law and fails to address the full costs and unintended consequences of its own proposals, by only considering administrative costs. Our analysis addresses some of these failings by considering in full the impact of the proposed regime, including the additional costs for businesses, including small and medium enterprises, the additional costs to supervisory authorities, conducting data protection impact assessments and complying with other new obligations.'(UK 2012, 2013)

Throughout 2014-15 the Council had met to negotiate its position on the proposed law; in June 2015 the Council finally agreed on its approach to the Regulation and negotiations between the (newly elected) Parliament, the European Commission, and the Council are currently under way (EC 2015, 2015a).

At various moments of the development of this Regulation the online data industry has also commented on it. For example, in their response to the initial draft of the Regulation, the British Bankers' Association highlighted that it 'contains a number of requirements that do not necessarily bring any significant benefit to the individual, and yet impose very onerous requirements on both data controllers and customers' (BBA 2012). Another response came from the Industry Coalition for Data Protection, which is comprised of 15 associations of European businesses, stating the Regulation draft 'missed an opportunity to reconcile effective privacy safeguards with rules protecting the conduct of business— both fundamental rights under the EU charter' (ICDP 2013).

In this way, both EU and US attempts to regulate the online data industry are caught up in numerous debates around the online data industry self-regulation and the need to protect consumers and citizens through the development and enactment of privacy and data protection laws. The central concern that the regulators deal with involves reconciling privacy and control over online personal data with economic growth.

However, an alternative to regulating the online data industry into addressing issues raised by data mining, scraping and monetizing, has been provided by online data firms that have sought to change the terms of the online data trade.

Entrepreneurs, start-ups, and data intensive firms

Amid the seemingly unresolved legal and policy disputes over how to reconcile privacy (data protection)[8] and economic growth, there are voices that insist they have found a solution. A number of data-focused businesses and online start-ups argue that data protection and growth are not mutually exclusive. These firms develop software products that could be assembled under an umbrella term 'personal data control products'. There is 'the upside opportunity for privacy', insists Liz Brandt, a CEO of Ctrl-Shift, a business consultancy and market research company based in London. If economic growth is driven by technological innovations, she reasons, the same could be said about online privacy: it could be driven by innovative technologies that take privacy to a different level of public recognition (Ctrl-Shift 2014).

A variety of products have been developed in Europe and the US such as tracking protection and data vaults[9]. Tracking protection proposes to do just that – it protects a user from being tracked online. And although it disables tracking, a user retains the ability to choose whether she wants to keep certain trackers active if she prefers them to use her information to improve services she is interested in. There are a number of tracking protection products available such as Disconnect, DoNotTrackMe, Ghostery[10].

Taking Ghostery as an example, it contains profiles of over 2019 online trackers helping users 'to make informed decisions' on how to stay private online without impinging the working of products and services used[11]. Given the vast and growing business of online tracking, Ghostery operates a feature called GhostRank. This enables users to opt-in to donate an anonymous version of data on how they are tracked to Ghostery while retaining the rest of their personal data. This improves Ghostery's ability to block tracking as it gets notified about new trackers. This kind of on-going development is required to keep privacy products up to date. The donated tracking data, in turn, also becomes a product. Ghostery, Inc – an owner of Ghostery

(formerly known as Evidon, or 'The Better Advertising Project') – analyses the tracking data and sells reports on this data to advertising businesses so they can optimise their return on investment.

Another example of personal data control products can be broadly called data vaults.[12] The data vault is a secure store of personal information that is made available to the user who retains control of her data. For instance, data can be securely locked but also made mobile, for example, on all devices the data owner uses, and 'across the web'[13]. However, companies developing products that could be classified as data vaults do not merely seek to consolidate users' data. In a similar manner to tracking protection products, data vaults help make individuals aware of how and by whom their data is used. At the same time data vault products do not just conceal information – they can also equip data sharing: 'There is already a market [for online users' data] out there, and it's working, and it's pretty efficient […] - you just don't participate in that.' Instead a data vault claims to enable a user to get their share of the personal data market, as it 'understands the types of data that you feel safe and comfortable trading, and they also understand what an advertiser wants, and can [trade] automatically' (from an interview with a New York-based start-up founder).

For example, a product developed by a UK based company Allfiled,[14] provides individual customers with data vaults to assemble and manage their data. At the same time the company has also developed a product for their business customer - a consumer website MoneySavingExpert.com (now part of the MoneySupermarket Group). This tool helps individuals to find the best deal on the market for a product they want, such as energy tariffs or insurance.[15] The website compares the deals their users currently have with deals available (by using data provided by the users that is stored in a vault and is updated by the users, only revealing information the users wished to be revealed in order to get the best deal on the market). To enable the comparison Allfiled equips the website with data vaults for websites users. As our interviewee explains: '[A vault] knows the deal you're on, and it asks the question, "If

I can find you a better deal, how much would it take to make you switch? […] And it allows you to pick a number, and insert that into personal data store at your convenience, so you decide it's your energy, your money, you decide how and where you're going to spend it"'.

Another example is provided by Datacoup. Their product involves an attempt to build 'the world's first personal data marketplace'[16]. The product claims to allow online users to integrate their personal data online (including their financial data) in order to build a profile that has a certain monetary value that depends on how much and what type of data it contains. It is then purchased by the start-up in order to build a market – a Platform – that could interest potential data purchasers (retailers, financial services, etc.). Once the data is purchased, US-based users are paid directly to accounts linked to their profiles.

The products outlined here do not take a conventional approach to online privacy that assumes a juxtaposition of 'the private' and 'the public'. Instead, these products try to address the challenge of reconciling privacy with growth through notions of control. Rather than concealing personal data, these products offer users the opportunity to maintain a form of control over data by retaining it, opening up the possibility to share certain aspects of data in order to receive a return. These products each put in place an expectation of reciprocity in the relationship between a service or product provider and user. An individual user 'should decide who sees their data, and how much of it they see and when they see it, who they trust, so it's almost like turning the clock back to the last century, when you would go to your local baker and you would buy bread from him because he always gave you a great loaf' (from an interview with a UK-based entrepreneur).

Neither do these products and services simply block data. Instead they offer various means to participate in controlled data exchanges: 'we recognised early on that if we […] block everything by default, it would keep things from working on the web like people expect them to work. Whereas if we show you what's happening, it leads people down a road of saying, "Okay, I see all of this happening", then they make a

decision. […] So our sort of tag line is knowledge and control is people's privacy – knowledge plus control equals privacy. You can't just have control, right? You can't just block. Because without understanding what you're blocking… Blocking is not meaning more private (from an interview with a senior product manager at a New York-based company).

The personal data control products described here (tracking protection and data vaults) address the same challenge that European and US regulators face in their attempts to provide a legal framework for online personal data protection and privacy. By developing a range of software that will enable online users to control their data as well as share it to their benefit, the entrepreneurs argue that economic growth could be equally driven by personal data under control of those who produce as it currently is through being monetised by those who collect it.

Conclusion

This brief report has considered contemporary recognition and possible futures for online data protection and privacy. In doing so, it has explored global personal data monetization, the development of data protection regulation in Europe and the US, and market-based responses to the widely shared public concern with online data protection. Rather than a traditional concern for privacy involving the invasion of a particular space or an opposition between the private and the public, what we can note instead are concerns with control, monetization, and data ownership. At the same time, we find a strong and clear voice among the data brokerage industry suggesting that concerns for privacy risk restricting economic growth. And a variety of solutions are proposed which each look to reconcile privacy and economic growth in different ways. Although no single solution has emerged as a major market presence, it seems that a shared concern is emerging around the asymmetric distribution of profits made through utilising personal data, embodied by the soaring personal data industry. This seems central to responses from regulators in the US and Europe. And although these responses are specific to the geographical regions and conditions through which they emerged, they are similar in their emphasis on recognizing value in economic growth fuelled by technological innovations in the information economy as well as the necessity of legal provisions that would enable customers and citizens to get control over their personal data.

Current attempts to restore a kind of balance of power between data collectors (for example, data brokers and service providers) and data producers (online users, consumers, customers) are still in their infancy. Personal data entrepreneurs do not seek to stop the online data industry, but instead transform the market for personal data into a 'personal data economy' (Chahal 2014). In this way, the future of privacy would be as a market good, reattaching property rights to users and consumers through forms of control in order to foster new forms of data exchange. If this were to emerge as a viable future for the online data industry, privacy would become the future of marketing.

Notes

1. http://investor.google.com/financial/tables.html; http://investor.fb.com/releasedetail.cfm?ReleaseID=893395, accessed 29 July 2015
2. For more details see e.g. Tene and Polonetsky (2012), Schmierer (2011), FTC (2014), Angwin and Steel (2011), Nettleton (2014).
3. Invented in early 1990s, a cookie was a helpful tool for online commerce, as it allowed to remember a number of products placed in a virtual shopping trolley by the same customer through setting an ID for customer, which was held in a cookie sent together with a webpage a browser requested. At present there are different types of cookies, e.g. HTTP or browser cookies (can be deleted) and flash cookies that are not controlled by web browser privacy settings and can restore deleted cookies (Mohamed 2009).
4. Among them are the Consumer Federation of America, Electronic Privacy Information Centre, etc.).
5. https://www.govtrack.us/congress/bills/113/s2025, accessed 17 July 2015. On the re-introduction of the bill see here: https://www.congress.gov/bill/114th-congress/senate-bill/668/all-info, accessed 30 July 2015.
6. For example, by classifying them into low income categories that might affect their ability to obtain certain services. The same point was made with regard to the Internet of Things, where personal data flowing from appliances and devices and its subsequent classification can potentially 'lead to a growing number of people being unable to afford full insurance protection of products' (Ambasna-Jones 2015).
7. http://ec.europa.eu/priorities/digital-single-market/index_en.htm, accessed 29 July 2015
8. Privacy and data protection both aim at safeguarding personal data; however, data protection laws and regulations are concerned with protecting 'publicly available' personal data, whereas privacy laws and regulations are applied to private personal data. Given the nature of data mining and monetization that converts 'public' data back into personal, both terms are relevant here.
9. The classification is rather crude but it serves the purpose of introducing the scope of the products. For media coverage of the products see Angwin and Steel (2011), Brustein (2012), Robin (2013), Sullivan (2012).
10. https://disconnect.me/; http://www.abine.com/donottrackme.html; https://www.ghostery.com/en/. These products differ from Do-Not-Track plug-ins available for Internet Explorer, Chrome, Mozilla browsers, because - as a request and not an obligation - the browser plug-ins cannot effectively block online trackers since it is not enforceable as trackers can still collect data.
11. The number of trackers in the database as of 31 July 2015 (https://www.ghostery.com/en/our-solutions/ghostery-add-on/).
12. A data vault is a generic term for a variety of products. They are known to be called - and this list is not exhaustive - 'infomediaries' (Hagel and Rayport 1997), 'personal data services' (Reed 2010), 'personal information management services (PIMs)' (Ctrl-Shift 2014), 'personal clouds' (Buddycloud.com), 'vendor relationship management (VRM)' as opposed to customer relationship management (CMR) (Searls 2012).
13. See, for example, products developed by Dashlane (https://www.dashlane.com/), or Personal (https://www.personal.com/)
14. https://www.allfiled.com; similar products are developed by Mydex (https://mydex.org/), Payoga (http://www.paoga.com), Qiy (https://www.qiy.nl/), Azigo (https://azigo.com/my/).
15. Its 'Energy Club' members amount to nearly 1,7m people in July 2015 (http://www.moneysavingexpert.com/cheapenergyclub, accessed 31 July 2015).
16. https://datacoup.com/

References

Ambasna-Jones, M. 2015. 'The Smart Home and a Data Underclass', *Guardian*. 3 August.

Angwin, J, and E. Steel. 2011. "Web's Hot New Commodity: Privacy". *Wall Street Journal*, February 27, Available at <http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html>

(BBA) British Bankers' Association. 2012. 'Views on the Proposed European Union General Data Protection Regulation'. Available at < https://www.bba.org.uk/policy/retail/managing-customer-data-and-information/data-protection/bba-position-on-proposed-eu-dp-regulations/>, accessed 29 July 2015.

Brill, J. 2013. "Demanding Transparency from Data Brokers." *Washington Post*. August 15. http://www.washingtonpost.com/opinions/demanding-transparency-from-data-brokers/2013/08/15/00609680-0382-11e3-9259-e2aafe5a5f84_story.html

Brustein, J. 2012. "Start-Ups Aim to Help Users Put a Price on Their Personal Data." *The New York Times*, February 12. Available at <http://www.nytimes.com/2012/02/13/technology/start-ups-aim-to-help-users-put-a-price-on-their-personal-data.htm>

Chahal, M. 2014. "Taking back control: the personal data economy", Marketing Week, March 12, available at < http://www.marketingweek.com/2014/03/12/taking-back-control-the-personal-data-economy/>, accessed March 19, 2014.

Constine, J. 2014. "Facebook Lets Advertisers Tap Purchase Data Partners To Target Customers, Categories Like Car-Buyers." *TechCrunch*. Accessed August 29. http://techcrunch.com/2013/02/27/facebook-ad-data-providers/.

Ctrl-Shift. 2014. *The Personal Information Economy*. An industry event organized by Ctrl-Shift. London, March 20. <http://personalinformationeconomy.ctrl-shift.co.uk/>

Ctrl-Shift. 2014a. *Personal Information Management Services: An Analysis of An Emerging Market*. Available at <https://www.ctrl-shift.co.uk/news/2014/07/28/executive-summary-personal-information-management-services-an-analysis-of-an-emerging-market/>, accessed July 29, 2014

Delo, C. 2013. "Facebook to Partner With Acxiom, Epsilon to Match Store Purchases With User Profiles." *AdvertisingAge*. February 22. http://adage.com/article/digital/facebook-partner-acxiom-epsilon-match-store-purchases-user-profiles/239967/

(EC) European Commission. 2012. 'Commission proposes a comprehensive reform of the data protection rules', 25 January. Available at <http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm>.

(EC) European Commission. 2012a. *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*. Available at <http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf>.

(EC) European Commission. 2014. 'Progress on EU data protection reform now irreversible following European Parliament vote', 12 March. Available at <http://europa.eu/rapid/press-release_MEMO-14-186_en.htm>.

(EC) European Commission. 2015. 'Commission proposal on new data protection rules to boost EU Digital Single Market supported by Justice Ministers'. 15 June. Available at <http://hb.betterregulation.com/external/Commission%20proposal%20on%20new%20data%20protection%20rules%20to%20boost%20EU%20Digital%20Single%20Market%20supported%20by%20Justice%20Ministers%2015%2006%202015%20EU%20PR.pdf>.

(EC) European Commission. 2015a. *Remarks by Commissioner Jourová after the launch of the Data protection regulation trilogue.* 24 June. Available at <http://europa.eu/rapid/press-release_STATEMENT-15-5257_en.htm>.

(EU) European Union. 1995. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.* Available at <http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:31995L0046>.

(EU) European Union. 2002. *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).* Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML>.

(EU) European Union. 2009. *Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services*. Available at < http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32009L0136>.

(EU) European Union 2014. Debate in Council. 4 December. Available at <http://www.europarl.europa.eu/oeil/popups/summary.do?id=1369996&t=e&l=en>.

FTC. 2009. "Federal Trade Commission Staff Report: Self-Regulatory Principles For Online Behavioral Advertising: Tracking, Targeting, and Technology." http://www.ftc.gov/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral

FTC. 2014. *Data Brokers: A Call for Transparency and Accountability*. Washington, DC: Federal Trade Commission. http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

Goel, V. 2014. “With New Ad Platform, Facebook Opens Gates to Its Vault of User Data.” *The New York Times*, September 28. http://www.nytimes.com/2014/09/29/business/with-new-ad-platform-facebook-opens-the-gates-to-its-vault-of-consumer-data.html

Hagel, J. and J. Rayport. 1997. “The Coming Battle for Customer Information.” *Harvard Business Review* 1997 (January-February): 5–11

Hamburger, T. 2014. “Consumer Privacy Rights Need Urgent Protection in Washington, Activists Say.” *Washington Post*. February 24. http://www.washingtonpost.com/politics/consumer-privacy-rights-need-urgent-protection-in-washington-activists-say/2014/02/24/1764ba22-9cb7-11e3-975d-107dfef7b668_story.html

(ICDP) Industry Coalition for Data Protection. 2013. ‘Industry Concerned Over Negative Impact of Albrecht Draft Report’. Available at <http://www.digitaleurope.org/Portals/0/Documents/Digital%20Economy/Privacy%20&%20Security/ICDP_Albrecht_PR_090113.pdf>, accessed 29 July 2015.

Levy-Abegnoli, J. 2015. ‘No EU Data Protection Deal “Before End of Year”: Rapporteur on the EU data protection regulation says parliament and council are “heading in two different directions”’. *The Parliament Magazine*. 8 January. Avaiable at <https://www.theparliamentmagazine.eu/articles/news/no-eu-data-protection-deal-end-year>.

Mohamed, N. 2009. “You Deleted Your Cookies? Think Again | Business.” *WIRED*. August 10. http://www.wired.com/2009/08/you-deleted-your-cookies-think-again/.

Nettleton, D. 2014. *Commercial Data Mining: Processing, Analysis and Modeling for Predictive Analytics Projects*. Elsevier.

Neyland, D. 2006. *Privacy, Surveillance and Public Trust*.. Houndmills, Basingstoke, Hampshire England ; New York: Palgrave.

PCAST. 2014. *Big Data and Privacy: A Technological Perspective.* Executive Office of the President President's Council of Advisors on Science and Technology. http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf

Reed, D. 2010. "Out with 'Personal Data Store', In with 'Personal Data Service.'" *Equals Drummond*. http://equalsdrummond.name/2010/10/03/out-with-personal-data-store-in-with-personal-data-service/

Robin, F. 2013. "The Emerging Market That Could Kill the iPhone - Fortune Tech." *CNNMoney*. Available at <http://tech.fortune.cnn.com/2012/08/01/iphone/>

Schmierer, C. 2011. 'Better Late Than Never: How the Online Advertising Industry's Response to Proposed Privacy Legislation Eliminates the Need for Regulation', Richmond Journal of Law and Technology, Vol. XVII (4):1-57

Searls, D. 2012. *Intention Economy: When Customers Take Charge*. Boston, Mass: Harvard Business Review Press

Sullivan, M. 2012. "Personal Data Vaults Put You in Control of Your Data Online." *PC Advisor*. Available at <http://www.pcadvisor.co.uk/news/internet/3369859/personal-data-vaults-put-you-in-control-of-your-data-online/>

Tene, O. and J. Polenetsky. 2012. "To Track or Do Not Track: Advancing Transparency and Individual Control in Online Behavioral Advertising." *Minnesota Journal of Law, Science and Technology* 13: 281-357

(UK) UK Parliament. 2012. *The Parliamentary Under-Secretary of State for Justice (Mrs Helen Grant). Data Protection. Justice.* Written Ministerial Statements. Parliamentary Business. House of Commons. 22 November. Available at <http://www.publications.parliament.uk/pa/cm201213/cmhansrd/cm121122/wmstext/121122m0001.htm>, accessed 29 July 2015.

(UK) UK Ministry of Justice. 2013. *Government response to Justice Select Committee's opinion on the European Union Data Protection framework proposals*. Available at <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/217296/response-eu-data-protection-framework-proposals.pdf>.

US Congress. 2013. *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes*. United States Senate. http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=bd5dad8b-a9e8-4fe9-a2a7-b17f4798ee5a

Waters, R. 2014. 'FT interview with Google co-founder and CEO Larry Page'. 31 October. *Financial Times*. Available at <http://www.ft.com/cms/s/2/3173f19e-5fbc-11e4-8c27-00144feabdc0.html>.

White House. 2012. "Fact Sheet: Plan to Protect Privacy in the Internet Age by Adopting a Consumer Privacy Bill of Rights | The White House." February 23. http://www.whitehouse.gov/the-press-office/2012/02/23/fact-sheet-plan-protect-privacy-internet-age-adopting-consumer-privacy-b

White House. 2014. *Big Data: Seizing Opportunities, Preserving Values*. Available at <https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf>.

Wooley, L. 2013. "DMA Responds to Op-Ed Attacking Commercial Data Use." *Direct Marketing Association*. Accessed April 17. http://blog.thedma.org/2013/08/19/dma-responds-to-op-ed-attacking-commercial-data-use/