INTERNET POLICY REVIEW
Journal on internet regulation

Volume 7 | Issue 2

Algorithmic governance and the need for consumer empowerment in data-driven markets

Stefan Larsson
Department of technology and society, Lund University, Sweden, stefan.larsson@lantm.lth.se

Published on 15 May 2018 | DOI: 10.14763/2018.2.791

Abstract: The present article argues that the fact that personal data holds great value, in combination with a lack of transparency in its commercial use, leads to a need for consumer policy that strengthens consumer protection. The widespread practice of user agreements and consent-based regulation of personal data collection is not satisfactory for balancing these information-asymmetric markets. The lack of transparency deriving from the complex and massive datafication of consumers – where consumers are profiled, data is brokered and the algorithmically automated decision-making is opaque – speaks to the need for improved supervision at a more structural level above and beyond the individual consumer's choices, preferably by more active consumer protection authorities.

Keywords: Automated decision-making, Consumer profiling, Consumer protection, Informed Consent, Transparency

Article information

Received: 12 Dec 2017 **Reviewed:** 08 Mar 2018 **Published:** 15 May 2018

Funding: Parts of this article are based on prior work conducted for and funded by the Swedish Consumer Agency.
Competing interests: The author has declared that no competing interests exist that have influenced the text.

URL:
http://policyreview.info/articles/analysis/algorithmic-governance-and-need-consumer-empowerment-data-driven-markets

Citation: Larsson, S. (2018). Algorithmic governance and the need for consumer empowerment in data-driven markets. *Internet Policy Review*, *7*(2). DOI: 10.14763/2018.2.791

INTRODUCTION: PERSONAL DATA AS CURRENCY

The Cambridge Analytica case, where third-party app developers gained access to a large amount of Facebook users' data and used it for political campaigning, has not only spurred much debate on the need for algorithmic governance of platforms in our current status of networked publics, but also stresses the need for consumer empowerment in data-driven markets overall. The case highlights a lack of transparency that the ecology of actors collecting,

handling and sharing personal data for various purposes ultimately mean for consumers and thereby also the difficulties in assessing the true value of the data collected. However, the lack of transparency and lack of consumers being informed over the data-handling is not an anomaly only true for some specific cases, but rather the norm for a data-driven economy. The main argument here therefore addresses the need for consumer empowerment in terms of transparency and ill-functioning notions of consent, in general, and methodological capabilities of consumer protection agencies, in particular.

In other words, from a consumer protection perspective, the data-driven economy poses great challenges in terms of the application of consumer regulations to information asymmetric relations – where one party has more or better information than the other, and the use of personalised services that include transactions of personal data (Larsson, 2017a; 2017c; Rhoen, 2016). Part of this regulatory challenge is arguably of a conceptual nature; that is, the practice of and supervision by consumer protection authorities is likely dependent on how the transactions, relations and conditions of the market are understood (cf. Larsson, 2017b). Given that the role, use and transactions of personal data is both opaque and part of an increasingly complex setting in what law professor Frank Pasquale has described as an "era of runaway data" (Pasquale, 2015), the need for a clarified description and understanding of the transactional character of personal data in the digital economy is called for. The main reason, here, is to be able to point out weaknesses in consumer protection, specifically with regards to imbalances or asymmetries in both information and power between consumers and digital service providers, how to deal with calls for transparency as well as the lack of consumer awareness when taking part in consent-based data collection.

There is little doubt that personal data do indeed hold significant value in the digital economy, and therefore can be understood as a sort of currency for services that are for free on the consumer level (cf. Schwartz, 2004; Spiekermann & Korunovska; Larsson & Ledendal, 2017). The notion of personal data *as currency*, in a context of consumer protection, is used here as a means to stress that 1) it carries transactional value for services that may be for free in a direct monetary sense; and 2) it is hard for consumers to assess what the value is – given the travel, trade and repurposing of much personal data (cf. Christl, 2017) – and hence to what extent the bargain is fair, and 3) it could therefore be a way to reconceptualise "free", data-collecting services, in order to trigger consumer protection for market practices otherwise not dealt with by consumer protection agencies.

For example, at the end of January 2012, the European Commission presented the proposal for the comprehensive reform of EU data protection provisions, which resulted in, among other things, the Data Protection Regulation (also known as GDPR) which comes into force in May 2018. In connection with this, EU Commissioner Viviane Reding described personal data as "the currency of today's digital market".[1] She did this by emphasising the importance of trust and the confidence that is lacking in order for the digital markets to work satisfactorily. She argued that what was needed was a strong, clear and uniform legal framework that could enhance the potential of the digital single market. The EU Commissioner revisited the same argument two years later: "In an increasingly digital society, personal data has become a new form of currency. The biggest challenge for political and business leaders is to establish the trust that enables that currency to keep flowing". In other words, this view is one of the stated motives that underlie strengthened individual protection for personal data in a digital context, described as a prerequisite for market development and growth.

This approach – that personal data has a central value in the digital economy and in practice can

function as a currency – has become a fairly common view of many analysts of the computer-driven economy. For example, this notion is developed in a report from 2012 – *The Value of Our Digital Identity* – from the consulting firm Boston Consulting Group (BCG). BCG's perspective, as in Reding's referral to an internal digital market, is to strive for trust that keeps the data flowing and in use, which can be described as a transaction-promoting perspective. A conclusion of the BCG study, which included 3,000 European participants, is that consumers want to share their data if the benefits and the privacy management are appropriate (2012). That is, consumers may be more willing to share data if companies can implement confidentiality tools that provide choice and control, establish user-friendliness, and provide a sufficient benefit in exchange. However, this rather optimistic account of free will and users' abilities to make informed choices in relation to the multitude of agreements being made in an everyday digital context is questioned in a number of studies, for example described by Turow et al. (2015) as "the tradeoff fallacy" with regards to consumers in stores, reading privacy agreements (Cranor et al., 2014) and, specifically, social networking sites (Bechmann, 2014), which will be returned to below.

A problematic imbalance pointed out by Sarah Spiekermann and Jana Korunovska (2016), who research social and ethical problems of computer systems, is that there is a big difference in how individuals perceive the value of their personal information, on the one hand, and industrial players that utilise personal data as a central source of value, on the other:

> Analysts, investors and entrepreneurs have recognized the value of personal data for Internet economics. Personal data is viewed as 'the oil' of the digital economy. Yet, ordinary people are barely aware of this. Marketers collect personal data at minimal cost in exchange for free services (Spiekermann & Korunovska, 2016, p. 1).

The value of personal data is further underlined by the fact that many online companies see their stock prices as a direct function of the data they have on their users (Spiekermann & Korunovska, 2016). As a sign of this, the top five companies with the largest absolute increase in market capitalisation in 2009-2017 were – among other commonalities – all consumer-focused data-driven tech companies: Apple, Alphabet (Google), Amazon, Microsoft, and Facebook (PwC, 2017). By March 2017, these five data-driven companies had taken five of the top six spots in terms of global market capitalisation, overtaking the oil companies and to some extent the financial institutions that were at the top only a decade ago (Larsson, 2017a). In sum, personal data holds great value for those who can utilise it, which at the same time entails a challenge to consumer protection since this value is not easily understood by consumers, leading to questions of consumer empowerment in terms of transparency, the role of consent, and how consumer protection authorities could improve their methods when supervising data-driven business practices.

THE PURPOSE

The article develops the argument of consumer empowerment and algorithmic governance in data-driven markets, and asks what this means for consumer protection policies and for the role of consumer protection authorities in terms of their supervision:

- What role does consumers' consent play for data collection, and what main weaknesses does it pose?

- How transparent can and should collection of consumer's data be and how should transparency be understood in this context?
- What do algorithmically mediated and personalised services – dependent on consumer profiling – entail for methods of consumer protection supervision?

The article describes the current state of the knowledge on digital consumer profiling based in a forward-looking, if critical and consumer-based, perspective. This is then related to findings on consumer attitudes and sentiment. To what extent do consumers find the personal data collection to be problematic or worrying? This means pointing out some of the more important operators and more significant emerging markets in order to thereafter analyse, based in a policy relevant perspective, the most important aspects of consumer protection – a key issue being the wide use of user agreements to regulate what has become a strong information asymmetry in some of the data-driven markets.

CONSUMER PROFILING, RISKS OF MISUSE, AND CONSUMERS' SENTIMENTS ON DATA COLLECTION

One of the reasons for collecting large amounts of consumer data is to improve consumer profiling, that is, the practice of obtaining an understanding of consumers to form an underlying data basis for strategic decisions and, for example, marketing or product design. It is part of a development that can be described as industries' attempt to create a "seamless, personalised digital customer journey" (cf. Edelman & Singer, 2015). This means combining information linked to an individual using methods that match specific consumer behaviour, demographic or psychographic characteristics (Harrison & Ti Gray, 2012; Hildebrandt, 2008). Profiling has become important not least in the marketing industry where this "new" kind of advertising can be described as "consumer-centric", meaning it focuses on individuals (cf. Brown et al., 2016). In order to accomplish this, it is data-driven, i.e., effectuated by monitoring consumers' actual internet-mediated behaviour – possibly in real time – in combination with collected data of previous behaviour, with the purpose of predicting future behaviour.

Profiles are used to categorise customers or customer segments in order to separate, for instance, the most profitable from the least, which information then comprises the strategic, underlying data used for marketing and other decisions. Consumers are therefore routinely studied, registered, analysed and ranked and may be offered both different prices and, to some extent, different services, depending on the individually associated information ("the data"), and their place of residence (Kitchin & Lauriault, 2014).

The field involved in collecting individual consumer information and profiling has also been described, using somewhat more negative connotations, as a growing "surveillance economy" (cf. Singh & Lyon, 2013; Teknologirådet & Datatilsynet, 2016) that also may lead to a misuse of consumer data. In an Australian and American context, Harrison and Ti Gray (2012) demonstrate how credit companies and banks use individual consumer profiling not only to identify the needs of individuals but also their weaknesses. This means among other things that they can specifically focus on consumers who will not be able to manage their credit payments during the interest-free period. This type of credit card user is also more profitable than users who do not incur credit card related interest costs. This entails, in other words, the identification of profitable customers that other operators might rate as being economically vulnerable (Stone, 2008). Others have shown a link between the increase in consumer credit and financial institutions' access to consumer information (Sanchez, 2009), which emphasises the need for

further research on digital consumption, credit and risks of over-indebtedness (cf. Larsson et al., 2016).

Studies conducted in an American market context show that consumers may be resigned about being able to influence traders' use of their personal information rather than satisfied with the discounts they receive in exchange (Turow et al., 2015). A number of studies show that users are concerned about not having control over their Internet generated data as well as the fact that their information could be used in situations that are quite different to where the information was originally collected or shared (Lilley et al., 2012; Pew, 2014; cf. Halbert & Larsson, 2015). According to a Swedish study, 60% of the Swedish population is opposed to news companies collecting data to enhance the user experience (Appelgren & Leckner, 2016). Other studies conclude that consumers are concerned that third parties such as advertisers or other commercial operators may be able to access their personal information (for example, Kshetri 2014, Narayanaswamy & McGrath 2014, Pew Research Center 2014). Overall, this indicates that consumer data is a key issue in much of the current market changes, and that this area and these relationships are complex and need further study.

ONLINE USER AGREEMENTS AND THE CONSENT DILEMMA

The main model utilised by data-driven services for the regulation of how to collect and handle consumers' personal data is through user agreements based on the notion of informed consent. Formally, the users agree to the collection of their data. Critics, however, argue that this kind of "privacy self-management" does not provide meaningful control and that there is a need to move beyond relying too heavily on it (Solove, 2013). At least three main critical aspects can be put forward here.

Firstly, part of the challenge – as this model has become so common for our everyday digital practices – lies in what can be described as an *information overflow* of consent agreements and what has been called an "autonomy fatigue" (Greenstein, 2017, p. 404). For example, the Norwegian Consumer Council (Forbrukerrådet) recently conducted a reading of the terms and conditions of apps that are commonly found on the average smartphone – they then broadcast the reading in real time on the internet.[2] It took 31 hours, 49 minutes and 11 seconds to read through the 250,000 words-long agreements, the iTunes agreement taking the longest at over three hours. Combined with all the other services utilised by an average digital consumer, it is simply not possible to even read the agreements, also stated in a rather early study by McDonald & Cranor (2008).

Secondly, part of the challenge likely lies in the fact that there are incentives for data collecting companies to be unclear about how much data is collected and how it is used: for example, Cranor et al. (2014) have studied 75 privacy policies from companies that store data on behaviour in digital contexts. They conclude that many of them lack important consumer relevant data management. This includes the collection and use of sensitive information and tracking data that can be used to identify individuals. Similarly, a study on privacy agreement texts and cookie consent information collected from 60 news sites in three countries (US, UK, and Sweden) shows that news sites "paternalistically" infer a wider consent from users than what can reasonably be expected, as a utilisation of "passive" consent. The reasons for collecting data can, according to Appelgren, therefore be said to be paternalistic in both a positive sense

(i.e., beneficial to users) as well as in a negative sense, as choices may be imposed on users although users have not actively agreed, and potentially resulting in an undesired outcome.

Thirdly, part of the challenge likely also lies in the fact that emerging personal data-driven markets are complex, automated and swift – and thereby intransparent in practice. For example, the Norwegian data protection authority, Datatilsynet, conducted a study in 2015 on the amount of data collected when visiting the front page of six Norwegian newspapers (Datatilsynet, 2015). On average, the study found, between 100 and 200 web cookies were placed on any computer used to visit these homepages, information about the visitor's IP address was sent to 356 servers, and an average of 46 third parties were "present" during each visit. One of the reasons for the presence of so many parties was the programmatic ad exchange taking place behind the web page in so-called programmatic advertising (cf. Busch, 2016), which involves increasing real-time bidding for selling advertisements that is dependent on profiling and targeting the individual visitor. However, none of the six newspapers provided their audience with any information relating to the presence of this large selection of third-party companies (Datatilsynet, 2015; Larsson, 2017c).

Each of these three examples point to the flawed notion of the individual consumer being able to, in a meaningful way, make informed choices with regards to the multitude of user agreements in play for an average digital consumer.

Media scholar and digital sociologist Anja Bechmann subsequently posits that "the consent culture of the internet has turned into a blind non-informed consent culture" (Bechmann, 2014, p. 21; cf. Joergensen, 2014). The fact remains that user agreements play a central role in regulating the handling of personal customer data between commercial parties and individuals, and that this striving for awareness is further emphasised by the GDPR. This leads to questions of how active consumer protection authorities preferably should be in empowering the "non-informed" but *formally* consenting consumers (Larsson & Ledendal, 2017). This question relates to how these practices apply not only to a privacy discourse but also to a discourse of consumer rights and power imbalances in the markets (Larsson, 2017a).

COMPLEXITY, OPACITY AND THE BROKERING OF DATA

A challenge from a consumer protection perspective regards the increasing complexity on data-driven markets, fuelled by both a lack of transparency – often behind proprietary software – and the fact that the data is traded and brokered. Media scholar Mark Andrejevic has commented on "the spreading of prediction markets" (2013, p. 68–70) in *Infoglut*, and Pasquale, too, stresses the need to become more knowledgeable about how personal data is collected, analysed and traded, and the "need to hold business and government to the same standard of openness that they impose upon us – and complement their scrutiny with new forms of accountability" (2015, p. 57). A recent report on how companies collect, combine, analyse, trade, and use personal data on billions of consumers, from an Austrian research institute, describes how pre-existing practices of commercial consumer data collection have rapidly evolved into pervasive networks of digital tracking and profiling, and a "vast and complex landscape of corporate players continuously monitors the lives of billions" (Christl, 2017, p. 65). The data broker industry is of particular interest here (cf. Larsson, 2017a). For example, *Acxiom* reportedly manages 15,000 customer databases and 2.5 billion customer relationships for 7,000 clients, including 47 of the Fortune 100 companies (Christl, 2017). *Oracle*, another rising giant on the data broker horizon, has acquired companies like *Datalogix*, *AddThis*, *Crosswise* and *BlueKai* in order to be able to

track billions of purchase transactions from grocery chains, users on millions of websites, a billion mobiles, the combination of PCs, phones, tablets, and TVs, as well as online message boards (Christl, 2017, p. 59; cf. Larsson, 2017a). The Federal Trade Commission in the US – to emphasise the opaque character of these practices – has stated that there is a "fundamental lack of transparency about data broker industry practices" (FTC, 2014, p. vii).

The complexity of how data travels thereby leads to a fundamental challenge for consumer and data protection. As "prediction markets" spread, more types of industries will develop a more refined, personalised relationship to consumers, which can be both to the consumers' benefit but also their detriment. Reliance on big data sets that can be complemented in real-time to analyse the specific consumers' conditions is increasingly being used for anything from purchase predictions by retail stores, to credit scoring by lenders, to death predictions by insurers (Siegel, 2016). Data brokers provide for profiling – as in the Acxiom example above – in partnerships with all kinds of companies ranging from Facebook, Google, Twitter to banks, insurance and airline companies (Christl, 2017). One specific problem relates to data being erroneous – as it happens. Legal scholars Mikella Hurley and Julius Adebayo (2017) have argued, in relation to credit scoring based on large amounts of collected and analysed data:

> Consumers have limited ability to identify and contest unfair credit decisions, and little chance to understand what steps they should take to improve their credit. Recent studies have also questioned the accuracy of the data used by these tools, in some cases identifying serious flaws that have a substantial bearing on lending decisions.

So, the complexity of the market, the "ecosystem" of "runaway" data in essence describes what Nancy King and Jay Forder point out in a study on data analytics and consumer profiling (2016); i.e., that many of the companies dealing with consumers' personal data gain access through secondary sources and use the information for purposes not known at the time of original collection (King & Forder, 2016). This further stresses the lack of possibilities for consumers to be informed about the uses of their data. Consequently, as consumer services – including credit scoring addressed by Hurley & Adebayo (2017) – becomes algorithmically mediated and automated, there is little chance for the individual consumer to assess if the outcome is reasonable, to counter if it is based on erroneous data, or even to clearly outline the inherent assumptions of the designed decision-making at hand. The black box of algorithmic decisions (cf. Pasquale, 2015), utilising secondary sources of data in consumer markets, is a clear challenge to consumer protection and the authorities representing it. How are they to detect if individual targeting – be it for ads or services – is based on illegal discriminatory grounds or exploiting particularly vulnerable groups?

Rhoen (2016), mentioned above, presents a socio-legally based analysis of how legal instruments can become more effective at improving consumer protection and the collection and use of consumer data (cf. Helveston, 2016). Rhoen (2016, pp. 6-8) argues, in a review of consumer protection and data protection legislation at the EU level, that a broader application of consumer protection regulation to user agreements may increase accountability for operators who collect and manage personal data, and in extension lead to increased codetermination for consumers. These consequences would, in that case, reduce the institutionalised power of the data managing parties in favour of the consumer. At the same time, however, Rhoen (2016, p. 8) points out that this can only be achieved if consumer protection legislation is applied pragmatically, which is partly the responsibility of the concerned supervisory authorities.

The European Data Protection Supervisor, EDPS, also points out the need for supervisory authorities – such as data protection and consumer protection authorities – to gain better insights into how data collection and covert profiling occurs (EDPS, 2015, p. 10), i.e., to study "the black box" (Pasquale, 2015). EDPS emphasises the lack of transparency involved and the challenges this entails also for governmental supervision; it is difficult to distinguish between advantages and intrusions when the data collection process and uses thereof are not visible (cf. King & Forder, 2016).

CONCLUSIONS

As shown, when it comes to the widespread practice of user agreements as a means to regulate the personal data collection, use and trade, the model seems flawed, particularly with regards to the notion of consumers making informed decisions. A wide array of studies show consumers' concerns when it comes to the collection of their data, as well as the resignation or powerlessness to counter or take control over it. This relates to a widespread datafication (Larsson, 2017c) and quantification (Larsson, 2017d) of consumers, leading to a lack of transparency in data-driven markets, clouded by proprietary software and complex automated decision-making as the data travels, mediated by data brokers and others. This speaks to the need for an implementation of consumer policy that helps consumers recognise the perils of the new information landscape without being overwhelmed with information. Furthermore, and this is perhaps more important to point out, it speaks for the need to regulate consumer rights at a level that is not as strongly dependent on the consumers' individual awareness. Pasquale, for example, also bears witness to this in relation to data brokers, stating that it is "unrealistic to expect individuals to inquire, broker by broker, about their files. Instead, we need to require brokers to make targeted disclosures to consumers. Uncovering problems in Big Data (or decision models based on that data) should not be a burden we expect individuals to solve on their own" (Pasquale, 2017).

Thus, given the overlapping character of personal data in the digital economy, there are a number of reasons why the data protection authorities and consumer-oriented authorities need to interact on a continuous and ongoing basis. Not the least the fact that personal data holds much of the value in a data-driven economy, combined with the fact that it is inherently hard for consumers to assess the bargain between data sharing and service access. This speaks for more structural solutions rather than depending on the consumers abilities of making informed choices about their personal data.

A recommendation for consumer protection authorities is therefore to develop synergies with, in particular, data protection authorities, to provide expertise on consumer protection. Transparency would likely have to include audits or control of how data-driven and targeting software operates, in order for consumer protection authorities to develop the ability to assess – in-house or perhaps through outsourced expertise – what the combination of algorithms and use of big data sources are leading to, and to discover the use of erroneous data (cf. King & Forder, 2016). This would be a way to propose a "qualified transparency" (Pasquale, 2015, p. 160–165) that may work in line with the need to "equalize the surveillance that is now being aimed disproportionally at the vulnerable" (Pasquale, 2015, p. 57). This could be a way forward to keep the proprietary software and the specific design of algorithms as the business secrets they may need to be, but at the same time provide for a necessary protective mechanism for the worst cases detrimental to consumers.

In the context of fintech firms, Pasquale (2017) witnessed before the United States Senate on the need for regulators to be able to audit machine learning processes to understand, at a minimum, whether suspect sources of data are influencing the decisions affecting consumers, such as credit scores. This would likely require data-driven and digital methods developed by the entities implementing the consumer protection supervision. In order to study the outcomes of automated services based on pattern recognition and to address accountability for these outcomes, a combination of legal and computer scientific expertise would be required. Or, put in a more general manner, in the European context, the methods operating in consumer markets have always called for scrutiny in order to secure the rights of weaker consumer parties. This was the case with traditional marketing and traditional credit scoring, and needs to be the case also for increasingly complex data-driven practices utilising increasingly sophisticated – and opaque – tools for the quantification of consumer preferences and automated responses to consumer interaction.

This article has focused on the collection and use of large sets of data in relation to consumers and their protection. It is therefore based on the assumption that consumer-focused activities in data-driven markets contain just that – data – which in theory can be scrutinised both with regards to its origin, its analysis, and application – which often means an algorithmically mediated automation. This is a field where contemporary consumer protection authorities need to have satisfactory supervisory methods.

In addition, as more and more consumer-related activities in the digital economy come to rely on artificial intelligence (AI) and machine learning, the demands of supervisory methodologies will increasingly face challenges relating to lack of transparency and autonomous agency in consumer-oriented products and services. They may even encounter a computation that is involved in decision-making that amounts to a form of cognition which is hard to explain and understand even for those that design the processes. As a response, perhaps future consumer protection authorities will find ways to utilise not only machine learning but also increasingly intelligent artificial agents to find and counteract inappropriate market behaviour, from a consumer protection point of view.

REFERENCES

Andrejevic, M. (2013). *Infoglut. How too Much Information is Changing the Way We Think and Know*. New York, NY: Routledge.

Appelgren, E. (2017). The Reasons Behind Tracing Audience Behavior: A Matter of Paternalism and Transparency. *International Journal of Communication*, *11*, 2178–2197. Retrieved from http://ijoc.org/index.php/ijoc/article/view/6823

Appelgreen, E., & Leckner, S. (2016). Att dela eller inte dela - användarnas inställning till insamling av personlig data. In J. Ohlsson, H. Oscarsson, & M. Solevid (Eds.), *Ekvilibrium: SOM-undersökningen 2015* (pp. 403-418). Göteborg: SOM-institutet. Available at https://som.gu.se/digitalAssets/1579/1579392_ekvilibrium-inlaga-f--rg.pdf

Bechmann, A. (2014). Non-informed consent cultures: Privacy policies and app contracts on Facebook. *Journal of Media Business Studies*, *11*(1), 21-38. doi:10.1080/16522354.2014.11073574

Boston Consulting Group. (2012). *The Value of Our Digital Identity* (Policy Report). Denver: Liberty Global, Inc. Available at https://www.bcg.com/publications/2012/digital-economy-consumer-insight-value-of-our-digital-identity.aspx

Brown, R.E., Jones, V.K. & Wang, M. (2016). *The New Advertising. Branding, Content and Consumer Relationships in the Data-Driven Social Media Era*. Santa Barbara: Praeger.

Busch, O. (2016) *Programmatic Advertising: The Successful Transformation to Automated, Data- driven Marketing in Real-time*. Cham, CH: Springer. doi:10.1007/978-3-319-25023-6

Cranor, L. F., Hoke, C., Leon, P. G., & Au, A. (2014). Are They Worth Reading? An In-Depth Analysis of Online Advertising Companies' Privacy Policies. Presented at the 42nd Research Conference on Communication, Information and Internet Policy. Available at http://www.contrib.andrew.cmu.edu/~pgl/tprc2014.pdf

Christl, W. (2017). *Corporate Surveillance in Everyday Life: How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions* (Report). Vienna: Cracked Labs. Retrieved from http://crackedlabs.org/en/corporate-surveillance

Datatilsynet. (2015). *The Great Data Race: How commercial utilisation of personal data challenges privacy* (Report). Retrieved from https://www.datatilsynet.no/en/about-privacy/reports-on-specific-subjects/the-great-data-race/

Edelman, D.C & Singer, M. (2015, November). Competing on Customer Journeys. *Harvard Business Review*, November Issue. https://hbr.org/2015/11/competing-on-customer-journeys

European Data Protection Supervisor. (2015). *Meeting the challenges of big data: A call for transparency, user control, data protection and accountability* (Opinion No. 7/2015). Brussels: European Data Protection Supervisor. Available at https://edps.europa.eu/data-protection/our-work/publications/opinions/meeting-challenges-big-data_en

Federal Trade Commission. (2014). *Data Brokers. A Call for Transparency and Accountability*. Available at https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

Greenstein, S. (2017, June 1). *Our Humanity Exposed: Predictive Modelling in a Legal Context* (Doctoral Dissertation). Stockholm University, Stockholm. Retrieved from http://www.diva-portal.org/smash/get/diva2:1088890/FULLTEXT01.pdf

Halbert, D. & Larsson, S. (2015). By Policy or Design? Privacy in the US in a Post-Snowden World. *Journal of Law, Technology and Public Policy*, *1*(2), 1-17. Retrieved from https://journal-law-tech-public-policy.scholasticahq.com/article/12-by-policy-or-design-privacy-in-the-us-in-a-post-snowden-world

Harrison, P. & Ti Gray, C. (2012). *Profiling for Profit. A Report on Target Marketing and Profiling Practices in the Credit Industry* (Report). Deakin University and Consumer Action Law Centre. Available at http://dro.deakin.edu.au/eserv/DU:30064922/harrison-profilingfor-2012.pdf

Helveston, M.N. (2016). Consumer Protection in the Age of Big Data. *Washington University Law Review*, *93*(4), 859-917. Available at https://openscholarship.wustl.edu/law_lawreview/vol93/iss4/5/

Hildebrandt, M. (2008). "Defining Profiling: A New Type of Knowledge?". In M. Hildebrandt & S. Gutwirth (Eds.), *Profiling the European Citizen, Cross-Disciplinary Perspectives*. Dordrecht: Springer. doi:10.1007/978-1-4020-6914-7_2

Hurley, M. & Adebayo, J. (2017). Credit Scoring the Era of Big Data. *Yale Journal of Law and Technology*, *18*(1), 148-216. Available at http://digitalcommons.law.yale.edu/yjolt/vol18/iss1/5/

Joergensen, R. (2014). The Unbearable Lightness of User Consent. *Internet Policy Review*, *3*(4). doi:10.14763/2014.4.330

King, N.J. & Forder, J. (2016). Data analytics and consumer profiling: Finding appropriate privacy principles for discovered data, *Computer Law & Security Review*, *32*(5), 696-714. doi:10.1016/j.clsr.2016.05.002

Kitchin, R. & Lauriault, T. P. (2014). *Towards critical data studies: Charting and unpacking data assemblages and their work* (Working Paper No. 2). Maynooth, IE: The Programmable City Project. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2474112

Kshetri, N. (2014). Big data's impact on privacy, security and consumer welfare. *Telecommunications Policy*, *38*(11), 1134-1145. doi:10.1016/j.telpol.2014.10.002

Larsson, S. (2017a). All-seeing giants and blindfolded dwarfs: On information-asymmetries on data-driven markets. In J. Lith (Ed.), *New Economic Models: Tools for Political Decision Makers Dealing with the Changing European Economies*. Brussels, Belgium: European Liberal Forum asbl. Available at http://lup.lub.lu.se/record/bada07c0-3a62-4e12-950d-779178eeccd4

Larsson, S. (2017b). *Conceptions in the Code. How Metaphors Explain Legal Challenges in Digital Times*. Oxford: Oxford University Press.

Larsson, S. (2017c). Sustaining Legitimacy and Trust in a Data-driven Society. *Ericsson Technology Review*, *94*(1), 40-49. Available at https://lup.lub.lu.se/search/publication/75b9d975-1a58-4145-85c4-efde2e46aa14

Larsson, S. (2017d, July 2). The Quantified Consumer: blind, non-informed and manipulated? *Internet Policy Review*. Retrieved from https://policyreview.info/articles/news/quantified-consumer-blind-non-informed-and-manipulated/696

Larsson, S. & Ledendal, J. (2017). *Personuppgifter som betalningsmedel* (Report No. 2017:4). Karlstad: Konsumentverket. Available at https://www.konsumentverket.se/globalassets/publikationer/produkter-och-tjanster/gemensamt/rapport-2017-4-personuppgifter-som-betalmedel-konsumentverket.pdf

Larsson, S., Svensson, L., & Carlsson, H. (2016). *Digital Consumption and Over-Indebtedness Among Young Adults in Sweden* (LUii Report No. 3). Lund: Lund University Internet Institute. Available at http://portal.research.lu.se/portal/en/publications/digital-consumption-and-overindebtedness-among-young-adults-in-sweden(40a1d8bb-34cd-4540-9cef-205958989908).html

Lilley, S., Grodzinsky, F.S. & Gumbus, A. (2012). Revealing the commercialized and compliant Facebook user. *Journal of Information, Communication and Ethics in Society*, *10*(2), 82–92. doi:10.1108/14779961211226994

McDonald, A.M. & Cranor, L.F. (2008). The Cost of Reading Privacy Policies. *I/S: A Journal of Law and Policy for the Information Society*, *4*(3), 543-568. Available at https://kb.osu.edu/dspace/bitstream/handle/1811/72839/1/ISJLP_V4N3_543.pdf

Narayanaswamy, R. & McGrath, L. (2014). A Holistic Study of Privacy in Social Networking Sites. *Academy of Information and Management Sciences Journal*, *17*(1), 71-85.

Pasquale, F. (2015). *The Black Box Society. The Secret Algorithms That Control Money and Information*. Cambridge, MA: Harvard University Press.

Pasquale, F. (2017, September 12). Exploring the Fintech Landscape. Written Testimony of Frank Pasquale Before the United States Senate Committee on the Banking, Housing, and Urban Affairs. Available at https://www.banking.senate.gov/imo/media/doc/Pasquale%20Testimony%209-12-17.pdf

Pew Research Center. (2014). *Public Perceptions of Privacy and Security in the Post-Snowden Era*. Washington DC: Pew Research Center. Available at http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/

PwC. (2017). Global Top 100 Companies by market capitalisation: 31 March 2017 update. PwC.

Rhoen, M. (2016). Beyond consent: improving data protection through consumer protection law. *Internet Policy Review*, *5*(1). doi:10.14763/2016.1.404

Sanchez, J.M. (2009). *The Role of Information in Consumer Debt and Bankruptcies* (Working Paper No. 09-04). Richmond: The Federal Reserve Bank of Richmond.

Schwartz, P. (2004). Property, Privacy, and Personal Data. *Harvard Law Review*, *117*(7), 2056-2128. doi:10.2307/4093335

Siegel, E. (2016). *Predictive Analytics: The Power to predict who will Click, Buy, or Die*. Hoboken, NJ: Wiley.

Singh, S. & Lyon, D. (2013). Surveilling consumers: the social consequences of data processing

on Amazon.com. In R.W. Belk & R. Llamas (Eds.), *The Routledge Companion to Digital Consumption*. London: Routledge. doi:10.4324/9780203105306

Solove, D.J. (2013). Privacy Self-Management and the Consent Dilemma. *Harvard Law Review*, *126*(7), 1880-1903. Available at https://harvardlawreview.org/2013/05/introduction-privacy-self-management-and-the-consent-dilemma/

Spiekermann, S., & Korunovska, J. (2016). Towards a value theory for personal data. *Journal of Information Technology*, *23*(1), 62-84. doi:10.1057/jit.2016.4

Stone, B. (2008, October 21). Banks Mine Data and Woo Troubled Borrowers. *The New York Times*.

Teknologirådets & Datatilsynet. (2016). *Personvern 2016 – tilstand og trender*. Oslo: Teknologirådets & Datatilsynet. Available at https://www.datatilsynet.no/om-personvern/rapporter-og-utredninger/personvernundersokelser/personvern-2016/

Turow, J., Hennessy, M. & Draper, N. (2015) *The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers and Opening Them Up to Exploitation* (ASC Departmental Paper No. 521). Philadelphia: Annenberg School of Communication, University of Pennsylvania. Available at https://repository.upenn.edu/asc_papers/521/

FOOTNOTES

1. See press release for full details: http://europa.eu/rapid/press-release_IP-14-70_sv.htm

2. http://www.forbrukerradet.no/side/250000-words-of-app-terms-and-conditions/