Consumer privacy and the future of data-based innovation and marketing

Citation: Bleier, Alexander et al. "Consumer privacy and the future of data-based innovation and marketing." International Journal of Research in Marketing 37, 3 (September 2020): 466-480 © 2020 Elsevier B.V.

As Published: http://dx.doi.org/10.1016/j.ijresmar.2020.03.006

Publisher: Elsevier BV

Persistent URL: https://hdl.handle.net/1721.1/130533

Version: Author's final manuscript: final author's manuscript post peer review, without publisher's formatting or copy editing

Consumer privacy and the future of data-based innovation and marketing

Alexander Bleier, Avi Goldfarb, Catherine Tucker

March 18, 2020

Abstract

Digitization makes it easier for firms to build their innovation and marketing efforts around consumers' personal data. In this research, we employ a privacy perspective based on contextual integrity to examine how such practices can trigger privacy concerns. We propose that small entrepreneurial firms are often at a particular disadvantage compared to large incumbent firms. At the same time, we also highlight that there are several strategies firms can use to mitigate privacy concerns and that in some circumstances, privacy concerns may also exert positive effects on data-driven marketing by stimulating privacy innovation and providing a source of competitive advantage.

It is often said that marketing needs to be data-driven (e.g., Wedel and Kannan, 2016). As the process of digitization reduces the costs of collecting, parsing, and storing data, it allows many areas of marketing to embrace data to an unprecedented degree (Goldfarb and Tucker, 2019b). It is not just marketing that has benefited, but also broader innovation across product categories (e.g., Manyika et al., 2011). Consumer data is increasingly a foundation on which firms build their business models to compete in sectors such as health, advertising, security, e-commerce, transportation, and banking (Jia et al., 2018). Firms use consumer data for everything from the development of new ideas for products and services (e.g., Porter and Heppelmann, 2014) to selling them to prospective target customers (e.g., Bleier and Eisenbeiss, 2015b).

This individual-level data can inform managerial decision making and facilitate economic success (McAfee and Brynjolfsson, 2012). For instance, Google combines consumer data across its various products such as Gmail, Calendar, Docs, Maps, Chrome, Voice, YouTube, and, of course, Google Search, to profile consumers, provide advertisers with targeting opportunities, and develop new products. Increasingly, start-ups also rely on consumer data. For example, Innovaccer,[1] launched in 2014, is a healthcare data activation firm that integrates and analyzes patient data from various sources to provide stakeholders with important information to improve patient care.

When discussing data-based innovation and marketing, it is also commonplace to express that 'privacy' may be a concern; however, that concern can be merely symbolic, attracting a few token nods of assent with no real focus on how to achieve it. However, in this paper we emphasize that privacy deserves more than peripheral consideration. We argue that notions of privacy are, and will be, crucial for influencing both the pace and direction of data-driven innovation and marketing in the coming decades.

Consumers' concern for privacy influences firms in various ways, including direct losses in

[1] `https://innovaccer.com/`

revenue due to lost sales (e.g., Pavlou et al., 2007), litigation risks (e.g., Son and Kim, 2008), data foreclosure (e.g., Jiang et al., 2013), and curtailed strategic scope due to privacy regulation (e.g., Goldfarb and Tucker, 2011d). These effects often weigh more heavily on smaller firms and their data-based innovation and marketing efforts than on larger incumbents (e.g., Campbell et al., 2015). While this is important for firms to realize, it is equally important for policy makers, as it demonstrates the inherent tensions between policies aiming to promote innovation, entrepreneurship, and consumer privacy.

Innovation policy seeks to ensure that the right incentives, such as a patenting system, are in place so that firms and individuals invest time and money into innovation (Jaffe et al., 2001). Entrepreneurship policy aims to ensure that the small size of entrepreneurial start-ups does not disadvantage them relative to large incumbents, either when dealing with capital markets or compliance costs. Privacy policy is mainly concerned with the question of how to protect citizens from unwanted intrusion by firms or governments (Goldfarb and Tucker, 2012a). Today, the process of digitization forces these policy areas together. As data collection, parsing, and storage costs fall, firms can gather data cheaply about anyone who may be of commercial interest, and personalize their offerings based on that data. This has greatly expanded the potential technological frontier of what firms can do or hope to achieve when serving their customers. However, this also means that the activities of innovative and marketing-oriented firms whose business models rely on the collection and usage of individual-level data now impinge on privacy policy. The question arises of how to create a regulatory environment that allows firms of all sizes to prosper by pushing the frontier on data-based innovation and marketing, while at the same time ensuring that consumer privacy remains protected (FTC, 2010).

In this study, we investigate the relationships between data-based innovation, marketing, and consumers' privacy concerns. We first discuss a perspective of privacy based on contextual integrity that views privacy as a right to appropriate flows of personal information within

a given social context (Nissenbaum, 2004). We then examine how data-based innovation and marketing can breach contextual integrity and thereby trigger consumers' privacy concerns. Next, we elaborate how such privacy concerns in turn pose challenges for further developments in innovation and marketing practice, especially for small entrepreneurial firms. We argue that there is a direct link from privacy as contextual integrity to the challenges privacy concerns create for these new small firms. In light of these challenges, we discuss a number of factors that can mitigate privacy concerns and thereby help reduce potential threats to data-based innovation and marketing. In addition, some privacy concerns create opportunities. We refer to these opportunities in the form of privacy innovation and privacy as a source of competitive advantage. We conclude with directions for future research. Figure 1 summarizes our conceptual framework.

[Insert Figure 1 about here]

1 Consumer privacy as contextual integrity

Privacy, traditionally perceived as the right to be let alone (Warren and Brandeis, 1890), is a concept that has proven difficult to conceptualize and define (Martin and Murphy, 2017; Smith et al., 2011). Even though several studies aim to provide a precise definition, drawing on concepts such as information control or awareness of data practices (e.g., Beke et al., 2018; Bélanger et al., 2002; Caudill and Murphy, 2000; Foxman and Kilcoyne, 1993; Goodwin, 1991; Stone et al., 1983), others suggest that privacy is highly contextual and does not lend itself to one general definition (e.g., Smith et al., 2011; Pavlou, 2011; Stewart, 2017). To nevertheless help explain why, for example, the use of technology-based systems can provoke anxiety, fear, and resistance in the name of privacy, Nissenbaum (2004, p. 155) introduces an information privacy theory based on "contextual integrity" which states that a "right to privacy is neither a right to secrecy nor a right to control but a right to appropriate

flow of personal information" (Nissenbaum, 2010). At the core, the idea is that someone who transmits information about someone else, should be constrained in how and where they can transmit that information. The appropriateness of such information flows is governed by context-relative informational norms that define how information is expected to flow within a social context such as health care, education, employment, or the marketplace (Nissenbaum, 2004). When informational flows adhere to entrenched norms, contextual integrity is intact, while disruptions may result in a violation of privacy.

A privacy perspective based on contextual integrity suggests that to preserve privacy, a person does not have to have explicit control over their data as long as information flows remain appropriate. This also implies that general characterizations of privacy concerns in terms of consumers' beliefs about the collection, exploitation, and protection of their data or awareness and control over privacy practices (e.g., Malhotra et al., 2004; Pavlou et al., 2007; Smith et al., 1996) that do not at the same time consider who is involved or the specific information shared between them might prove insufficient.

While a contextual integrity perspective offers several advantages for evaluating privacy-sensitive circumstances compared to other approaches, it is also not without its flaws. Norms over data flow can be ambiguous, change over time, or differ between cultures. Yet, despite these shortcomings, contextual integrity today finds widespread application in disciplines such as computer science and law (e.g., Apthorpe et al., 2018; Criado and Such, 2015; Kim, 2014). Marketing research has, however, by and large not yet adopted this privacy perspective. In the next section, we therefore illustrate how the lens of contextual integrity can help assess how novel information flows from data-based innovation and marketing can trigger privacy concerns.

2 How data-based innovation and marketing can cause privacy concerns

Today, rapid technological advances reduce the cost for firms to collect and exploit consumer data (Goldfarb and Tucker, 2019a). As a result, novel information flows emerge that may threaten consumer privacy, as data is put to new uses and in new contexts (Acquisti et al., 2016; Nissenbaum, 2018).

Online tracking and connected devices have generated new opportunities for data collection and analysis. Online browsing behavior is often used to target products and advertising. Netflix, for example, collects viewing information from its millions of customers to personalize recommendations and develop new, innovative content, recently even through interactive episodes (Marman, 2019). Using individual viewing information to improve the customer experience is commonly accepted practice in service of contextual goals, but Netflix saw privacy concerns erupt when it appeared as if race was informing its recommendations (Iqbal, 2018). While such information was not directly collected, race was inferred (seemingly out of context) from viewing choices. In retargeted adverising, firms target ads for specific products to consumers that have already shown some interest in the product using data on their browsing behavior (e.g., Bleier and Eisenbeiss, 2015b; Lambrecht and Tucker, 2013). Repurposing past browsing behavior in a new context can raise privacy concerns; however, the extent to which retargeting makes users concerned about privacy, rather than being perceived as providing valuable information, also depends on how much consumers trust the advertising firm (Bleier and Eisenbeiss, 2015a).

Connected devices also have generated new types of data, and new types of privacy concerns. As more products are equipped with sensors that track location, usage, condition, and other information, marketers can offer new products and features that seem to deliver higher quality (Hoffman and Novak, 2018; Porter and Heppelmann, 2014). However, such

products and features also allow consumer information to be used in new contexts, potentially threatening entrenched norms and generating privacy concerns. Personal health or fitness trackers, for instance, feed consumer data directly into the cloud to facilitate consumer activity dashboards and comparisons with peers. If this data gets used for a purpose other than fitness tracking, such as for insurance or credit scoring, the new context for the data would likely raise privacy concerns. A similar example is the smart home device. The iRobot vacuum raised privacy concerns when the firm reportedly planned to sell floor map data to third parties (Astor, 2017). When used purely to improve a robot's performance, gathering floor map data serves contextual goals and would not likely be seen as a privacy infringement. However, selling such information onward for other purposes would likely violate entrenched norms and give rise to privacy concerns.

Many of the above examples focus on collecting new types of data, and then using that data in a way that was unanticipated by the consumer. However, novel combinations and applications of data are a cornerstone of innovation over the past decade (Lenard and Rubin, 2013). For example, Acquisti and Gross (2009) showed that public data can predict social security numbers, Crandall et al. (2010) showed that hidden social connections can be inferred from public social media, and Wang and Kosinski (2018) claimed to be able to identify sexual orientation from Facebook profile pictures.

Therefore, the ability to fuse and analyze disparate data sources allows firms to identify consumers' preferences that the consumers would not have been able to voice if asked directly, at the risk of triggering privacy concerns. This suggests a trade-off between privacy and innovation.

3 How privacy concerns affect firms and the future of data-based innovation and marketing

This discussion suggests that novel information flows from data-based innovation and marketing can trigger privacy concerns. In this section, we examine how such concerns can in turn affect firms and future developments in these data-intensive fields. A particular observation here is that privacy concerns often affect smaller entrepreneurial firms much more than large incumbents, and that this may determine which firms benefit from consumer data. Smaller firms have more incentives to disrupt, but they often do not possess the required resources to finance major innovations. As an example, Chandy and Tellis (2000) show for consumer durables and office products that incumbents do not introduce fewer radical innovations than smaller firms. However, Baumol (2005) argues that breakthrough innovations are mainly driven by independent entrepreneurs. In general, the less immediate the effects of privacy concerns are on firms, the more they disadvantage small and entrepreneurial firms compared to larger corporations.

3.1 Direct loss of revenue

Privacy concerns affect firms most immediately through a direct loss of revenue, because consumers choose not to respond to or buy from firms that seem to threaten their privacy. For example, consumers might abandon their plans of buying a specific smart home assistant, if they fear the firm will sell information about their usage habits to advertising firms. Correspondingly, Pavlou et al. (2007) find that privacy concerns reduce consumers' purchase likelihood. Further research shows how privacy concerns lead consumers to not take advantage of online personalization services (Baruh et al., 2017; Chellappa and Sin, 2005) or pay a premium to buy from websites that effectively protect their privacy (Tsai et al., 2011).

Moreover, privacy concerns may harm the profits of firms whose monetization models

are fueled by digital advertising, by reducing consumers' likelihood of clicking on banner ads (Bleier and Eisenbeiss, 2015a; Tucker, 2014). In addition, consumers frustrated with personalized online ads might also opt out from receiving targeted advertisements or use ad-blocking technology, which can create losses for targeted advertising-supported platforms (Schumann et al., 2014). Recent research shows the negative effects of ad-blocking on future website traffic (Shiller et al., 2018). Johnson et al. (2018) further quantify the lost expenditures from behaviorally targeted advertising with a point estimate of $8.58 per American opt-out consumer.

Last, these direct effects may affect stock market value. Most research here focuses on the direct effect of data breaches on stock market value (Acquisti et al., 2006; Miller and Tucker, 2011b). Teasing apart privacy management (rather than data security management) and firm valuation seems a promising area for future work.

In general, there is no reason to believe that smaller entrepreneurial firms and large incumbents would be affected systematically differently in terms of direct effects on revenues, though larger public firms may see the effects of privacy risks more swiftly through changes in their share price.

3.2 Risk of litigation

Though consumers may avoid a specific firm in response to privacy concerns, they may also take legal action (Son and Kim, 2008). For example, Google and Facebook were both sued over submitting consumers' photos to biometric scanning.[2] Solove and Schwartz (2014) notes that cases involving privacy are increasingly common in the US court system, though to our knowledge there has been no detailed study on the extent to which lawsuits are focused on large or small firms or on how they relate to the innovative intent of the target firm. It

[2]One of the key contested questions in this case was whether there needed to be actual harm for the plaintiffs to prevail (Roberts, 2019).

seems relatively uncontroversial to assume that privacy risks are at their greatest when new and large-scale data is being collected about consumers, though of course it is precisely that kind of context where we might expect to see the most data-based innovation and marketing activity.

One industry that has seen substantive legal activity due to both privacy and security concerns is the smart toys industry. In 2018, kids' electronics maker VTech was fined $650,000 for a data breach in which the personal information of millions of children was exposed. VTech had collected this data including children's names, birthdays, and genders without their parents' consent and stored it without encryption on its servers (Paul, 2018). This shows that litigation risk may be higher when firms target consumer segments that enjoy greater privacy protection, such as children.

Litigation, typically associated with substantial cost to firms, is a particular threat for smaller firms, because, on a per-case basis, larger firms possess more resources to defend themselves. As such, large firms might also be more likely to fight any lawsuit more aggressively, to deter future litigation (Dixon et al., 2006). The potential for negative effects of litigation on innovation and entrepreneurship has been noted in general (Dixon et al., 2006), and in specific types of litigation such as patent litigation (Kiebzak et al., 2016) or liability litigation (Galasso and Luo, 2018), though the latter paper notes that liability rules could be designed to encourage innovation if focused on harm rather than specifically on harm from change. Moreover, research shows that ongoing litigation risk can reduce the potential initial value of firms going public (Lowry and Shu, 2002). Altogether, it appears that smaller firms are at a disadvantage when privacy concerns become strong enough that customers consider legal measures.

3.3 Data foreclosure

Data-based innovation and marketing rely by definition on consumers' individual-level data. When firms' access to this source of input is curtailed, its innovation and marketing suffer. Privacy concerns drive this effect in different ways. The first is the well-established finding that privacy concerns cause customers to be less motivated to share personal information with firms (e.g. Awad and Krishnan, 2006; Dinev and Hart, 2006; Jiang et al., 2013; Stutzman et al., 2013). In addition, consumers may remove their data from a firm's database or provide false information in response to privacy concerns (Son and Kim, 2008). This particular practice might weigh especially hard on smaller firms, because they typically have fewer data points to verify and cross-validate consumers' information, and consumers may be more distrustful of a small firm than a big firm.

Second, firms may try and respond to consumer privacy concerns by building so-called 'walled gardens.' Walled gardens are closed ecosystems, controlled by a single operator. An example is Apple, which requires users to obtain apps from its App Store where it "curates" the apps available for download. Apple also recently introduced a tracking block on its Safari Internet browser which effectively prevents ad agencies from collecting consumer data for advertising.

As well as creating walled gardens, firms may simply cut off access to data for other firms in the ecosystem. For example, to preserve privacy Google will no longer provide marketers with log-level user data and IDs that would allow them to use this information in their own applications independent from Google. Instead, advertisers now have to rely on Google's Ads Data Hub, a data warehouse where ad exposure data is housed and can only be connected to Google's own solutions for attribution, analytics, and data management (Kihn, 2018). This makes it harder for smaller firms to develop and use their own applications. Similarly, Facebook announced that it would improve user privacy and end its "Partner Categories" ad tools that allowed outside data brokers to directly target specific user groups based on

their third-party data. This may protect consumer privacy, but also highlights the tension between the aims of competition policy and privacy policy.

Therefore, another potential implication of consumer privacy concerns is that they may inhibit the ability of new entrants and smaller firms to access consumer data, and this in turn may increase the importance of digital walled gardens (Campbell et al., 2015). For example, many customers spend a lot of time on the Twitter platform, and this familiarity may lead them to readily provide Twitter with their data. However, they might feel uneasy if Twitter were to announce it was sharing that data with a new and untested entrant in the digital advertising ecosystem. Therefore, consumer preferences for privacy may lead firms to not share their data with other firms and in particular to be less likely to partner with new firms. This tension is an important example of how viewing privacy as contextual integrity makes it clear that privacy concerns affect small entrepreneurial firms more than large incumbents.

3.4 Privacy regulation

When facing greater privacy concerns, consumers may look to lawmakers to implement stricter regulation to help alleviate their concerns (Milberg et al., 2000). In fact, without regulation, overall privacy may decline over time and become more and more costly for consumers to maintain (Rust et al., 2002). The general goal of privacy regulation is to limit the extent to which firms can track and use consumers' personal information. Since this data increasingly fuels innovation and marketing, it should be no surprise that privacy regulation will affect the future development of these fields.

3.4.1 Privacy regulation and the scope of data-based innovation and marketing

One of the areas where the effects of privacy regulation have been best documented is in digital online advertising. There are three reasons for this. First, digital online advertising is by its very nature designed to be readily monitored and measured by researchers (Goldfarb

and Tucker, 2011a). Second, as it was one of the sectors that pioneered the use of digital data, it was also one of the first to experience systematic attempts at regulation. Third, there are very likely negative effects of privacy regulation on the effectiveness of online advertising by simple revealed preference, in the sense that advertisers use data for a reason. As set out by Evans (2009) and Lenard and Rubin (2009), there is a trade-off between the use of online customer data and the effectiveness of advertising. One tension that exists in work documenting the effects of privacy regulation on advertising is that it is easy to dismiss whether there are any real effects from a loss of advertising effectiveness. This is because there is often ambiguity in policy discussions about whether it is 'good' or 'bad' for consumers if advertising markets work well. Advertising markets suffer, but if advertising is not welfare-enhancing, that might not matter (Benkler, 2018).

Goldfarb and Tucker (2011d) measure the effects of some of the first major legislation which addressed the question of the use of digital data in advertising, the European 'E-Privacy Directive' (EC/2002/58). The directive limited firms' ability to track users' online behavior and made it more difficult for a specific advertiser to collect and use data about consumer browsing behavior on other websites. The directive was seen as being stricter than those in the US and elsewhere at that point in time (Baumer et al., 2004). To measure its effects, the study analyzes the responses of 3.3 million people to 9,596 online display (banner) advertising campaigns to explore how this privacy regulation influenced advertising effectiveness in the EU relative to the rest of the world. The results show that display ads became 65 percent less effective at changing stated purchase intent among those surveyed after the directive was enacted relative to other countries.

More recently, Johnson et al. (2018) investigate industry self-regulation in the case of the AdChoices program launched in 2010. This program gives consumers "notice and choice" about the usage of their personal information for advertising purposes. Advertisers in this program show the AdChoices logo in the top-right corner of their display banner ads. Con-

sumers can click on the logo to receive information about how their browsing information is used for the creation of personalized banner ads. They can opt out from having their information collected and used for personalization, and only see standard ads in the future.

In a theoretical model, Campbell et al. (2015) find that requiring firms to provide notice and gain consent from consumers to collect, parse, and store their data disadvantages smaller firms. This occurs because firms with more easily verifiable benefits to offer consumers in return for their data find it easier to obtain consent. Again, smaller firms collect data in a narrower context. Therefore, even though "notice and consent" may impose costs on all firms, small and new firms are disproportionately harmed, because they do not have a convincing scale of products and history of operations in exchange for consent.

In addition to these effects on online advertising, Lerner (2012) shows consequences for innovation in the digital advertising space. Specifically, he documents that the E-Privacy Directive was associated with a relative decline in venture capital funding of entrepreneurial ventures in digital advertising. In addition, Lambrecht (2017) finds that following the introduction of the directive in 2002, venture capital investments into online news, online advertising, and cloud computing decreased substantially in the EU relative to the US.

A more recent regulatory milestone was the enactment of Europe's 'General Data Protection Regulation' (GDPR)[3] in May 2018. The aim of this policy is to strengthen the privacy rights of EU citizens and residents by giving them more control over the collection, usage, and protection of their personal data online. To this end, the GDPR expands not only the scope of protected consumers, but also the definition of personal data. Compared to prior regulations that considered consumers' names and addresses as personal data, the GDPR regards any information that directly or indirectly relates to an identified or identifiable natural person, for example also IP addresses, as personal data. These changes significantly

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504

increase the number of data-reliant firms inside or outside the EU that are affected by this regulation. In addition, the GDPR introduces novel rules that require firms to obtain consent for the usage of consumer's personal information through intelligible and easily accessible forms that provide information about the usage of consumers' data upon consent. Further adjustments and clarifications include rights of data access and erasure as well as rules for privacy by design. The GDPR also set new penalty standards as violations can result in fines up to 20 million euros or 4% of the firm's global revenue. Similar to Lambrecht (2017), Jia et al. (2018) investigate the short-run impact of the GDPR on investment in new and emerging technology firms. Using data on technology-venture related activity in the EU and US, they demonstrate that, as a result of the GDPR, investments in EU ventures decreased compared to US ventures. The environment for entrepreneurial innovators has thus become tougher in Europe.

Another sector that heavily relies on data-based innovation is digital health. This industry promises to revolutionize the quality of patient care through the collection and parsing of data (Miller and Tucker, 2017). Digital technologies like electronic medical records systems help hospitals use patient data by improving the monitoring of patient care and the accuracy of patient medical histories. Here, startups like Ada Health[4] allow patients to share their symptoms to allow AI-generated personalized diagnoses and suggestions. It is not surprising that regulation that restricts the use of patient data on privacy grounds limits the effectiveness and development of such technologies.

Last, early work such as Miller and Tucker (2009, 2011a) emphasizes that state privacy regulation can reduce adoption of an electronic medical records system because it lessens the network benefits to hospitals from their ability to exchange and build on existing digital data, and that this has real effects on health outcomes such as the survival rates of high-risk neonates. Miller and Tucker (2018) builds on these findings to show that the same tension

[4] `https://www.ada.com/`

exists in the adoption of newer technologies such as genetic testing. Though these studies do not look at the difference between large and small firms, another paper, (Miller and Tucker, 2017), does document that in general the existence of privacy regulations tend to lead to both data silos and the adoption of less compatible software, disadvantaging smaller healthcare providers.

3.4.2 Privacy regulation and the shape and direction of data-based innovation and marketing

Much of the work on the economic influence of privacy regulation focuses on understanding the scope and size of its effects. However, additional research highlights that privacy regulation may also affect the direction of data-based innovation and marketing. Goldfarb and Tucker (2011d), for instance, also find that websites with general content (e.g., news and media services), unrelated to specific product categories, experienced larger decreases in ad effectiveness after the E-Privacy Directive passed than websites with more specific content (e.g., travel or parenting websites). Customers at travel and parenting websites have already identified themselves as being in a particular target market, so it is less important for those websites to use data on previous browsing behavior to target ads. This would shape incentives for entrepreneurs contemplating entering the digital advertising space, in that they would be more likely to find profitable business models if they produced easily monetizable content, rather than relying on data or its exchange to be supported by digital advertising as discussed by Schumann et al. (2014). Some sites might cease publishing general political news in favor of content that is more easily tied to a specific audience, like travel or parenting content (Goldfarb and Tucker, 2012b). As another substitution effect in online advertising, Goldfarb and Tucker (2011c) observe that search engine prices for specific keywords were higher in states where lawyers could not directly contact prospective clients, indicating how firms might adjust their practices to changes in privacy regulation.

A further finding from Goldfarb and Tucker (2011d) is that non-intrusive text-based ads were most affected by the regulation. By contrast, advertising which relied on visual gimmicks to attract attention (rather than using data to ensure relevance) was only negligibly affected, since gimmicky ads operate differently (Goldfarb and Tucker, 2011b). Privacy regulation may therefore lead innovation in digital advertising to focus on non-data-based means of attracting attention, rather than using data to increase ad relevance or usefulness.

Similarly, digital platforms may be reluctant to seed new technologies or innovative efforts with existing customer data. For example, when Google attempted to innovate in the social network space with its Google Buzz product, it used its data about Gmail's most-mailed contacts to seed contact information. However, this use of existing data to build critical mass in an adjacent market courted criticism from a privacy perspective (FTC, 2011). This emphasizes that even for larger firms, innovating into new areas using existing customer data may be hampered by consumer privacy concerns.

A specific regulation designed to influence future marketing practice towards children was the 'Childrens Online Privacy Protection Act' (COPPA)[5], enacted in 2000. Its goal was to protect the privacy rights of children online by requiring all firms that collect personal information from young children to post a privacy policy on their website and obtain parental permission. Cai and Zhao (2013) investigate over 100 children's websites and show that only half of them and only a quarter of websites advertising on children's websites complied with the COPPA requirements. At the same time, the industry has also responded to issues of children's online privacy protection through its self-regulatory body, the Children's Advertising Review Unit (CARU)[6] which provides firms with concrete guidelines. Miyazaki et al. (2009) study such self-regulatory safeguards and derive implications for the advertising industry which are perhaps more likely to shape its future.

[5] https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

[6] http://www.caru.org/guidelines/index.aspx

The GDPR will also affect innovation in AI applications. For instance, Article 12 requires firms to either explain individual algorithmic decisions or provide general information about how the algorithms arrive at decisions, thereby creating a likely trade-off between accuracy and transparency. Moreover, the regulation restricts firms from using data for any other purpose than that for which it has been collected, making it harder for them to engage in AI-driven innovation (Wallace and Castro, 2018). One specifically affected area of AI innovation is robotics. For instance, personal care robots are often placed at the disposal of a person in need by third parties, which raises questions of consent, especially since the machine will likely learn about the person's highly privacy-sensitive health parameters.

Miller and Tucker (2017) further suggest that hospitals that are subject to privacy regulation may be more likely to invest in digital technologies that are incompatible with neighboring hospitals. Privacy regulation can therefore shape the type of innovation or digital technology that is developed.

Of course, compared to smaller firms, larger firms are more able to influence the course of public policy and regulations in their favor. For instance, large firms are more likely to possess the necessary resources to engage politically (Schuler and Rehbein, 1997). In addition, lawmakers might also be more receptive to their input compared to that of smaller firms, because they can provide extensive policy details as well as numerous constituents (Schuler et al., 2002). Last, larger firms often have more experience influencing public policy, which younger firms typically lack (Hillman and Hitt, 1999).

In addition, once a regulation is passed, its associated cost of compliance weighs heavier on smaller entrepreneurial firms. For instance, Julie Bernard, CMO of mobile marketer Verve, notes that, "The implications and ramifications of GDPR compliance will challenge numerous organizations (...) with resources on scales smaller than, say—and in particular—Facebook and Google." Her firm might shutter its operations in Europe due to the GDPR (Kottasová, 2018). Similar outcomes have been shown with other forms of regulation (e.g., environmental

or pharmaceutical) where incumbents can acquire strategic advantage through compliance against smaller firms and potential new entrants (Dean and Brown, 1995; Thomas, 1990).

On the other hand, smaller firms might be more flexible to respond to implied changes of regulation, especially in data-based innovation and marketing, while larger firms, especially in industries such as automotive, are often less flexible due to "path dependencies" where innovation decisions are made with stricter long-term implications (Acquisti et al., 2016). Also, in the specific case of the GDPR, regulators acknowledge the relationship between privacy regulation and entrepreneurial activity, in that they included special provisions for Small and Medium Enterprises (SMEs). For example, SMEs will not have to appoint a data protection officer nor conduct impact assessments unless there is a perceived high risk from the data collected. This policy is thus one of the first to recognize that the relative costs of privacy compliance are higher for smaller compared to larger firms (Commission, Commission). Moreover, enforcement seems to, at least so far, still be somewhat lax with startups (Martin and Matt, 2018), while, for instance, Google has been fined $57 million for violations and Facebook has also been targeted (Dillet, 2019).

This discussion suggests that consumer privacy concerns can affect the future of data-based innovation and marketing. In particular, more immediate effects, such as through a direct loss of revenue, tend to affect small and large firms to similar extents. By contrast, less immediate effects, such as through litigation, data foreclosure, or privacy regulation, typically impose stronger negative effects on smaller firms. These observations are especially relevant with respect to the kinds of firms that will be able to shape the future of these important data-intensive fields.

4 Factors that mitigate privacy concerns from data-based innovation and marketing

We have discussed how data-based innovation and marketing can trigger privacy concerns and how these may in turn affect the ability of firms to engage in these practices. Next, we highlight relevant mitigators of privacy concerns in the literature and anchor them in the concept of contextual integrity.

4.1 Trust

A central aspect of contextual integrity is who shares information about whom with whom, and thus the relationship between involved parties in a given context. Typically, one of the most determining factors of any relationship is the extent to which the involved parties trust each other. Trust refers to one's "willingness to rely on an exchange partner in whom one has confidence" (Moorman et al., 1992, p. 315) and positive expectations about another's intentions or behaviors (Rousseau et al., 1998). Specifically, in a customer-firm context, trust describes customers' beliefs about a firm's competence, benevolence, and integrity (McKnight et al., 2002).

A large stream of research examines the importance of trust for business built on customer data, such as e-commerce (e.g. Sheehan and Hoy, 2000; Urban et al., 2000, 2009). As firms collect more and more information about consumers, trust might serve as an instrument to help consumers believe that a firm will adhere to entrenched contextual norms and not use their data inappropriately. This idea aligns well with Pavlou et al. (2007)'s notion that privacy concerns typically arise as a result of beliefs that a firm is unable or unwilling to protect a consumer's personal information; the plethora of ways in which firms collect and use consumers' personal data today leave consumers uncertain and vulnerable to firms' actions, and this can trigger privacy concerns (Dinev and Hart, 2004). However, jointly considering

all parameters of contextual integrity, trust might also serve other purposes. For example, trust may affect the transmission principles tied to specific attributes of information flows. For instance, Bleier and Eisenbeiss (2015a) find that trust can reduce privacy concerns in response to personalized advertising, holding other parameters constant. Therefore, a more-trusted firm may use certain personal information for advertising purposes, which constitutes a change in transmission principles for certain attributes, while a less-trusted firm may not. In line with this finding, trust also leads consumers to more readily disclose personal data to firms in various contexts (e.g. Anderson and Agarwal, 2011; Hoffman et al., 1999; McKnight et al., 2002; Schoenbachler and Gordon, 2002) and increases consumers' likelihood of using personalization services (Chellappa and Sin, 2005). Correspondingly, Kalaignanam et al. (2018) find that trustworthiness is a key determinant of whether website personalization is economically beneficial for firms.

Therefore, it might be useful for firms to assess their trustworthiness among consumers before engaging in certain data-intensive innovation or marketing operations.

4.2 Culture and demographics

Given that entrenched contextual norms can differ between cultures (Nissenbaum, 2004), what constitutes an appropriate information flow in one country or society might be considered a breach of norms in another. A prominent example is Google Street View, which, compared to the US, faced much heavier headwinds in Europe where the firm had to blur faces and license plates as well as notify the public before sending its camera-equipped cars onto the streets, and limit the amount of time it stored clear images of faces and license plates (Cain Miller and O'Brien, 2013). Culture and other demographic characteristics thus influence the extent to which data-based innovation and marketing may trigger privacy concerns.

Based on a survey of 595 internal auditors from 19 countries, Milberg et al. (2000) find for

example that cultural values determine the extent to which consumers are concerned about their information privacy. Similarly, Goldfarb and Tucker (2012c) show that younger people are in general less concerned about their privacy than older people, a gap that continues to widen. Athey et al. (2017) moreover find that younger people are more willing to share their data with start-ups compared to larger firms or the government. These findings highlight that first, norms are subject to changes over time and with the evolution of technology, and that second, they may also differ between cultures.

While firms cannot directly control consumer culture and demographics, they can determine which target population to structure their data-intensive business plans around, and adjust their strategic positioning and operations accordingly to manage privacy concerns.

4.3 Information sensitivity

Next to the involved parties in a specific flow of information, the actual data that is involved is an important factor for contextual integrity. As such, it matters whether a vacuum robot transmits how long it took to clean a house or the exact floor plan of all rooms; even seemingly innocuous data can lead to privacy concerns when it transfers up the data food chain. A large stream of research investigates consumers' privacy perceptions about information flows with different levels of data sensitivity, often conceptualized as the perceived level of intimacy attached to data (Lwin et al., 2007) or the potential loss associated with its disclosure (Mothersbaugh et al., 2012). In general, consumers appear, for instance, less willing to provide firms with financial or personally identifying information compared to demographic or media consumption information (Cranor et al., 2000; Phelps et al., 2000). Similarly, flows involving consumers' social security numbers can lead to substantial concerns about privacy (Sheehan and Hoy, 2000) and firms' requests for more sensitive data can trigger higher risk beliefs and discomfort as well as lower intentions to reveal such data (Malhotra et al., 2004; Mothersbaugh et al., 2012).

In a more recent study, Milne et al. (2017) develop a taxonomy of information types based on consumers' associated risk categories, sensitivity, and willingness to provide such data. Thus, even though whether a specific type of information transmitted poses a breach of contextual norms hinges on all factors of a given information flow, exploiting less sensitive information might be helpful for firms to maintain contextual integrity and minimize privacy concerns.

4.4 Control

To preserve contextual integrity, the conditions and restrictions of information flow are as important as the specific information involved (Martin and Nissenbaum, 2016). The literature discusses several transmission principles such as "confidentiality," "reciprocity," "desert," "with permission of subject," "with notice," or "required by law" (e.g., Apthorpe et al., 2018; Barth et al., 2006; Benthall et al., 2017), but one of the most extensively investigated principles is consumer control. Malhotra et al. (2004) show, for instance, how consumers' loss of control over how firms collect and handle their personal information induces privacy concerns. In addition, Tucker (2014) uses field experiment data to evaluate the effect of Facebook giving users increased control over their privacy settings. The study finds that after Facebook allowed users more control, personalized advertising (mentioning specific details about a user in the ad copy) became more effective. These results align with Dinev and Hart (2004), showing that the ability to control the usage of their private information reduces consumers' privacy concerns, and Xu et al. (2012), finding that perceived control over personal information also reduces consumers' privacy concerns in response to location-aware mobile-coupon services. Increasing consumers' control over their data also boosts purchase intentions (Phelps et al., 2000). Last, privacy protection can have differential effects on the adoption of genetic testing. Miller and Tucker (2018) suggests that approaches focused on "notice and consent" without empowering patients tend to deter adoption, whereas ap-

proaches that focus on empowering patients to control their own data encourage adoption.

The provision of privacy controls may, however, also have countervailing effects. In the context of crowdfunding campaigns, Burtch et al. (2015) show that granting contributors less control over their private information, that is, whether their name and/or contribution amount appears on the platform, leads to an increases in conversion probability but a reduction in contributions, conditional on conversion. Given the increasing complexity of firm's data collection and exploitation practices, there are also concerns that consumers cannot effectively self-manage their privacy anymore (Solove, 2012; Nissenbaum, 2011). Giving consumers control over their personal information can also lead to increased willingness to disclose sensitive information, thereby leaving those consumers more vulnerable than with less control (Brandimarte et al., 2012; Mothersbaugh et al., 2012).

Firms may therefore grant consumers more or less control in accordance with other flow-determining parameters, such as the type of data involved and the amount of trust that consumers place in them.

4.5 Transparency

Highly personalized ads often trigger privacy concerns when consumers do not understand the data processes leading to their creation and might suspect potentially inappropriate flows of information (Acquisti et al., 2016). As such, several studies show that privacy concerns arise if consumers notice firms exploiting their data beyond the original transaction purpose for which it was collected (e.g. Foxman and Kilcoyne, 1993; Nowak and Phelps, 1997). In line with this notion, Aguirre et al. (2015) find that, compared to overtly-collected consumer information, using covertly-collected data for ad personalization heightens consumers' perceived vulnerability. In the face of privacy concerns, consumers also increasingly turn to privacy notices on websites (Awad and Krishnan, 2006; Milne and Culnan, 2004) and may even pay a premium to purchase from websites that disclose their privacy policies (Tsai et al.,

2011). Providing such data privacy statements might then in general lead consumers to more willingly disclose personal information (Hui et al., 2007), while asking them for more sensitive information reduces the dampening effect of posting privacy policies on privacy concerns (Lwin et al., 2007).

In the realm of information privacy, transparency is often interlinked with control (e.g., Foxman and Kilcoyne, 1993). An example is the popular concept of "notice-and-consent," or informed consent, requiring firms to inform consumers about their data practices and only proceed with processing consumers' information if they opt in. The resulting "transparency paradox" might leave consumers with too little information to sufficiently understand what firms actually do with their data before opting in (Barocas and Nissenbaum, 2014). In addition, Kim et al. (2019) also show how transparency can reveal to consumers the inappropriateness of a specific flow of information and thereby cause privacy concerns, lowering ad effectiveness.

Providing the right information about firms' usage of personal consumer data for innovation and marketing efforts can thus be one important step to mitigating privacy concerns.

4.6 Privacy calculus

Although certain innovation and marketing practices may cause privacy concerns, consumers might be willing to tolerate them if the perceived value they receive in return is sufficiently high (Sheehan and Hoy, 2000). The literature referring to early work (e.g., Culnan and Armstrong, 1999; Laufer and Wolfe, 1977), often discusses this trade-off as the *privacy calculus* (e.g., Dinev and Hart, 2004). Accordingly, consumers weigh the risks associated with the release of personal information to a firm against expected benefits such as financial rewards, personalization, and social adjustment benefits (Smith et al., 2011). In this sense, they "trade away information for a more valued incentive" Caudill and Murphy (2000, p. 8).

Chellappa and Sin (2005) investigate, for instance, how consumers trade off perceived benefits of personalized goods and services against associated privacy concerns that can arise as a result of personalization. In their setting, consumers valued personalization much higher than concerns for privacy when determining the usage of personalization services. Similarly, Dinev and Hart (2006) employ a privacy calculus view to explain consumers' willingness to provide personal information in order to transact online. Schumann et al. (2014) also find that consumers might accept targeted advertising in exchange for free Web services and Tsai et al. (2011) show that consumers are willing to pay a premium to purchase from firms that provide better privacy protection.

Instead of working to decrease consumers' privacy concerns, firms might therefore also aim to attenuate the negative effects of such perceptions by providing increased value in exchange, for instance through better service or lower prices - though that is admittedly tough if the price is already zero. Relatedly, research has started to investigate the monetary value that consumers place on their privacy, for instance with respect to the secondary use of their personal information (Hann et al., 2002; Hirschprung et al., 2016). More recent work by Kim et al. (2019) also examines "Privacy over Personalization" as a construct to capture the trade-off between consumers' simultaneous desire for more privacy, but also greater personalization of communications. A related aspect is the so-called *privacy paradox*, according to which people often state to care about privacy, but at the same time freely relinquish private information online (Barnes, 2006).

5 Positive effects of privacy concerns on data-based innovation and marketing

The previous discussion outlined the negative effects of consumer privacy concerns on data-based innovation and marketing, especially for smaller firms, and some steps marketers can

take to reduce these concerns. However, even though these challenges may seem substantial, they can also pose opportunities. In this section, we focus on two key positive outcomes of privacy concerns for firms, namely privacy innovation as a new domain of business, and competitive advantages the market grants firms that cater to consumers' privacy concerns.

5.1 Privacy innovation

In addition to their negative effects on the future development of data-based innovation and marketing, privacy concerns may also exert positive externalities, for instance by creating incentives that spur new forms of innovation, namely privacy innovation. This observation is in line with the Porter hypothesis, according to which properly designed regulation can trigger innovation that may partially or more than fully offset the cost of compliance (Porter and Van der Linde, 1995). In particular, firms have started to develop novel products that help protect consumer privacy. One prominent example is the development and application of blockchain technologies. On the face of it, to mention blockchain as a privacy-protecting innovation seems off-point, because blockchain technology such as bitcoin at its heart has a public permissionless database, where all transactions are completely public. However, there are other applications of blockchain technology which may be useful for resolving digital privacy concerns. First is the use of blockchain for institutions that manage personal data and identities (Mainelli, 2017). As described by Zyskind et al. (2015), the emphasis of such a system could be on ensuring that users own and control their personal data. An example of this kind of innovation is the Publiq network[7], which aims to provide an alternative financing method for advertising and monetization of digital content, which would help protect the privacy of its users. However, as noted by Marthews and Tucker (2019), the potential for persistence of data within a blockchain context itself suggests risks to a consumer's privacy.

Moreover, a multi-billion dollar industry is currently built around data brokers that buy

[7] `https://publiq.network/`

patients' health data from doctors and hospitals, anonymize it, and sell it to other firms to guide their pharma investments or better target their advertising (Tanner, 2016). In an effort to grant consumers the right to legal ownership of their human data, start-up Hu-manity.co[8] built a blockchain-based app that allows users to transparently manage, for instance, their geospatial data, driver and vehicle history, spending habits, medical history, and recreational habits as legal property on a blockchain. This confers on users the legal characteristics of ownership over their data, such as involvement in sale, negotiations of fair market value, and sharing, instead of simply being tracked by firms (Business Wire, 2018). Relatedly, Adjerid et al. (2016) find that while privacy regulation alone can lead to a decrease in planning and operational health information exchanges, when coupled with incentives, privacy regulation with requirements for patient consent can actually have positive effects on the development of health information exchanges efforts. Besides developing technical solutions, entrepreneurs might also turn consulting for regulations into a business model, such as start-up Lexemo[9].

In addition, academic research has started to investigate privacy-conserving solutions for innovation and marketing. For example, smartphones combine online tracking with smart, connected products and thus offer a fertile ground for privacy innovation. In this realm, Sutanto et al. (2013) develop a personalized mobile advertising application that, however, retains users' information locally on their smartphones. Similarly, Enck et al. (2014) introduce a system that monitors the usage of private consumer information by third-party apps on their smartphones as input for privacy-preserving services. Further studies propose privacy-conserving blockchain-based communication frameworks for products such as smart homes (Song et al., 2017) or smart cities (Biswas and Muthukkumarasamy, 2016).

Thus, innovation in privacy can generate both direct and indirect benefits to firms, providing new opportunities for entrepreneurs while lessening the negative effects of privacy

[8] https://hu-manity.co/

[9] https://www.lexemo.com

issues on both firms and consumers.

5.2 Privacy as a competitive advantage

As privacy is becoming increasingly important to consumers, firms catering to this need can gain a competitive advantage over those that do not. As such, Goldfarb and Tucker (2013) discuss how firms can leverage consumer privacy as an opportunity to provide their customers with delightful experiences. Moreover, Casadesus-Masanell and Hervas-Drane (2015, p. 230) state that "firms can exploit consumer heterogeneity by differentiating in their levels of information disclosure and can profit from doing so even though this sacrifices disclosure revenues." They show that privacy can soften competition when consumers have different perspectives over privacy so that firms can differentiate their privacy practices. In addition, Lee et al. (2011) show that asymmetric privacy protection (only exercised by some firms) may reduce market competition, because it allows a protecting firm to expand the customer segment it caters to without having to compete with another firm for the remaining customers that are less concerned about their privacy.

Employing privacy innovations can bestow particular competitive benefits. One such example is search engine DuckDuckGo[10]. The firm distinguishes itself from other search engines by not collecting or sharing its users' personal information and showing every user the same results for a given query, as if it was their first visit to the website. This way, DuckDuckGo has established itself a unique positioning. In support of such a business strategy that relies on less consumer data, Chiou and Tucker (2017) show that when search engines attempted to comply with new EU guidelines regarding length of personally identifiable data storage, there was very little effect in terms of accuracy of search queries - which was measured by whether the consumer had to return immediately to the search engine and make another query. Therefore, storing individualized search engine records for more than six months

[10] `https://duckduckgo.com/`

seems to confer little advantage to search accuracy relative to anonymized records. This may be because so many search queries are new and dynamically evolving that historic data is less useful for predicting what a consumer desires to find than more recent data.

In general, numerous firms seek to gain a competitive advantage by highlighting that competitors care less about customer privacy, for instance when Microsoft accused Google of misusing consumer information (Casadesus-Masanell and Hervas-Drane, 2015), or adopt privacy-friendly technology such as Google now offering DuckDuckGo as a default search engine option in many markets (Zhou, 2019). Correspondingly, Martin and Murphy (2017) develop a set of best practices for firms to gain a competitive edge through good privacy practices. A competitive advantage may then not only materialize in terms of higher sales or market share, but also increased access to consumer data. For instance, Culnan and Armstrong (1999) show that consumers are more willing to grant marketers permission to use their information when the firm treats their information fairly. In sum, firms catering to consumers' privacy concerns may obtain a favorable market positioning relative to others that pay only minor attention to such concerns. Privacy can create opportunities.

6 Conclusions and directions for future research

This paper discusses how data-based innovation and marketing can trigger consumers' privacy concerns from a contextual integrity perspective and how such concerns can in turn influence the future of these data-intensive fields. With firms increasingly able to collect and process large quantities of information about individuals, the outlined relationships can be expected to intensify. Therefore, firms need to carefully evaluate their usage of consumer data to fuel their innovation and marketing efforts. It is important to avoid the temptation to exploit any data that becomes available with any method without contemplating the potentially associated risks. Just because a novel way of even more closely personalizing ads to

consumers is feasible does not mean it aligns with entrenched contextual norms. As a result, it may trigger privacy concerns with substantial repercussions.

One important aspect that policy makers may consider is the extent to which privacy concerns exert stronger effects on smaller firms engaging in data-based innovation and marketing efforts compared to large incumbents doing so. We argue that the outsized impact on new small firms directly follows once privacy is seen through a lens of contextual integrity. Privacy concerns generally, rather than privacy regulation in particular, often help large incumbents relative to small entrants. The literature suggests that these two types of firms contribute differently to the overall innovation landscape of an economy. Policy makers should be aware that certain well-intended regulations might have undesired downstream effects. For instance, if start-ups find it increasingly hard to establish themselves in Europe due to the burdens of tight regulation (e.g., Kottasová, 2018), they might take their talent elsewhere, negatively influencing the European economy and its competitive outlook. Government authorities should thus recognize that the ongoing digitization process requires them to harmonize innovation policy and policy on entrepreneurship with privacy policy to provide the right incentives for firms that want to engage in data-based innovation and marketing while at the same time protecting consumer privacy.

We have also shown the positive effects that privacy concerns can spark, from privacy innovation to using privacy as a competitive advantage. A privacy perspective based on contextual integrity may provide clear guidance to firms and their data-intensive efforts. In particular, it may help find the balance between the technically possible and defensible for outcomes that improve firm profits as well as consumer welfare.

Last, while we attempted to bring together insights from the literature as it exists as well as current industry examples, it is clear that there are many gaps. We therefore end this paper by suggesting some fruitful directions for new research:

- We still know surprisingly little about how privacy concerns and regulation affect new

versus established firms. Unanswered questions include: How aware are start-ups and incumbents of the specific challenges posed by privacy concerns and how do they plan to meet them? Or, how much does it shape the direction of their activity or even their location decisions?

- To which extent does privacy-focused litigation and regulatory oversight have differential effects on smaller and larger firms empirically?

- How do privacy and security concerns as well as compliance costs affect innovation and entrepreneurship in data-sensitive developing industries, such as smart toys?

- How might firms account for ethical dilemmas posed by technological advances in their firm policies (Lobschat et al., 2019)?

- How do international privacy protections affect incentives for entrepreneurial firms and innovators to explore or avoid global markets?

- Firms may gain profitability improvements from targeting and personalizing marketing activities to consumers at increasing levels of granularity (Zhang and Wedel, 2009). However, it is not clear how to determine the optimal level of granularity and approach to analysis, targeting, and personalization, given costs of compliance, data collection, verification, analytics, and consumers' corresponding privacy response (Wieringa et al., 2019). Under which circumstances should firms settle for less granular data and when should they pursue to exploit information at the individual consumer level? A further driver of profitability might be the specific targeting regime employed (Rafieian and Yoganarasimhan, 2019).

- We also still know little about the relationship between a *lack* of data collection and the shape and direction of innovation (see Nagaraj (2018) for a related discussion). In particular, how may a lack of digital data about various groups of individuals shape

their inclusion in the benefits of digital data? This seems important, because though the digital divide literature has emphasized the division between those who use digital technologies and those who do not, there has as of yet been no attention paid to the implications of a lack of digital data about individuals in the digital ecosystem. Especially in developing countries, there are often few digital records concerning the very poor, and it is unclear how this affects their inclusion in the potential benefits of digital innovation, marketing, and entrepreneurship.

- What is the trade-off between privacy and accuracy? If firms are forced to use less accurate AI systems, will this result in biased and unfair decisions (e.g., marketing models, email filtering, voice recognition, content classification, marketing optimization)?

- How might privacy regulations exert unintended negative effects on consumers and their interactions with firms? For example, consumers having to accept cookies at each website they visit might lead them to compare fewer options before buying, reduce cross-checking across sources to identify fake news, or adopt other behavioral adjustments with associated welfare losses.

Privacy concerns create challenges for firms that often arise because data provided in one context is used in a different context. We have highlighted how privacy concerns affect firms of different size, several strategies that marketers can use to mitigate privacy concerns as well as some particular circumstances in which privacy concerns can create opportunities.

References

Acquisti, A., A. Friedman, and R. Telang (2006). Is there a cost to privacy breaches? an event study. *ICIS 2006 Proceedings*, 94.

Acquisti, A. and R. Gross (2009). Predicting social security numbers from public data. *Proceedings of the National Academy of Sciences*.

Acquisti, A., C. R. Taylor, and L. Wagman (2016). The economics of privacy. *Journal of Economic Literature 54*(2), 442492.

Adjerid, I., A. Acquisti, R. Telang, R. Padman, and J. Adler-Milstein (2016). The impact of privacy regulation and technology incentives: The case of health information exchanges. *Management Science 62*(4), 1042–1063.

Aguirre, E., D. Mahr, D. Grewal, K. de Ruyter, and M. Wetzels (2015). Unraveling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness. *Journal of Retailing 91*(1), 34–49.

Anderson, C. L. and R. Agarwal (2011). The digitization of healthcare: boundary risks, emotion, and consumer willingness to disclose personal health information. *Information Systems Research 22*(3), 469–490.

Apthorpe, N., Y. Shvartzshnaider, A. Mathur, D. Reisman, and N. Feamster (2018). Discovering smart home internet of things privacy norms using contextual integrity. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 2*(2), 59.

Astor, M. (2017). Your Roomba May Be Mapping Your Home, Collecting Data That Could Be Shared. Retrieved February 20, 2019 from https://www.nytimes.com/2017/07/25/technology/roomba-irobot-data-privacy.html.

Athey, S., C. Catalini, and C. Tucker (2017). The digital privacy paradox: Small money, small costs, small talk. Technical report, National Bureau of Economic Research.

Awad, N. F. and M. S. Krishnan (2006). The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS quarterly*, 13–28.

Barnes, S. B. (2006). A privacy paradox: Social networking in the united states. *First Monday 11*(9).

Barocas, S. and H. Nissenbaum (2014). Big datas end run around anonymity and consent. *Privacy, big data, and the public good: Frameworks for engagement 1*, 44–75.

Barth, A., A. Datta, J. C. Mitchell, and H. Nissenbaum (2006). Privacy and contextual integrity: Framework and applications. In *2006 IEEE Symposium on Security and Privacy (S&P'06)*, pp. 15–pp. IEEE.

Baruh, L., E. Secinti, and Z. Cemalcilar (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication 67*(1), 26–53.

Baumer, D. L., J. B. Earp, and J. C. Poindexter (2004). Internet privacy law: a comparison between the United States and the European Union. *Computers & Security 23*(5), 400 – 412.

Baumol, W. J. (2005). Education for innovation: Entrepreneurial breakthroughs versus corporate incremental improvements. *Innovation policy and the economy 5*, 33–56.

Beke, F. T., F. Eggers, P. C. Verhoef, et al. (2018). Consumer informational privacy: Current knowledge and research directions. *Foundations and Trends® in Marketing 11*(1), 1–71.

Bélanger, F., J. S. Hiller, and W. J. Smith (2002). Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. *The journal of strategic Information Systems 11*(3-4), 245–270.

Benkler, Y. (2018). *Network Propaganda*. Oxford University Press, USA.

Benthall, S., S. Gürses, H. Nissenbaum, et al. (2017). *Contextual integrity through the lens of computer science*. Now Publishers.

Biswas, K. and V. Muthukkumarasamy (2016). Securing smart cities using blockchain technology. In *2016 IEEE 18th international conference on high performance computing and communications; IEEE 14th international conference on smart city; IEEE 2nd international conference on data science and systems (HPCC/SmartCity/DSS)*, pp. 1392–1393. IEEE.

Bleier, A. and M. Eisenbeiss (2015a). The importance of trust for personalized online advertising. *Journal of Retailing 91*(3), 390–409.

Bleier, A. and M. Eisenbeiss (2015b). Personalized online advertising effectiveness: The interplay of what, when, and where. *Marketing Science 34*(5), 669–688.

Brandimarte, L., A. Acquisti, and G. Loewenstein (2012). Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science 4*(3), 340–347.

Burtch, G., A. Ghose, and S. Wattal (2015). The hidden cost of accommodating crowdfunder privacy preferences: A randomized field experiment. *Management Science 61*(5), 949–962.

Business Wire (2018). New Company Hu-manity.co Uses Blockchain to Declare a 31st Human Right, Empowering All Humans to Claim Legal Ownership of Inherent Human Data. Retrieved April 24, 2019 from https://www.businesswire.com/news/home/20180605005581/en/New-Company-Humanity.co-Blockchain-Declare-31st-Human.

Cai, X. and X. Zhao (2013). Online advertising on popular childrens websites: Structural features and privacy issues. *Computers in Human Behavior 29*(4), 1510–1518.

Cain Miller, C. and K. J. O'Brien (2013). Germanys Complicated Relationship With Google Street View. Retrieved March 19, 2019 from hhttps://bits.blogs.nytimes.com/2013/04/23/germanys-complicated-relationship-with-google-street-view/.

Campbell, J., A. Goldfarb, and C. Tucker (2015). Privacy regulation and market structure. *Journal of Economics & Management Strategy 24*(1), 47–73.

Casadesus-Masanell, R. and A. Hervas-Drane (2015). Competing with privacy. *Management Science 61*(1), 229–246.

Caudill, E. M. and P. E. Murphy (2000). Consumer online privacy: Legal and ethical issues. *Journal of Public Policy & Marketing 19*(1), 7–19.

Chandy, R. K. and G. J. Tellis (2000). The incumbents curse? incumbency, size, and radical product innovation. *Journal of marketing 64*(3), 1–17.

Chellappa, R. K. and R. G. Sin (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology and Management 6*(2-3), 181–202.

Chiou, L. and C. Tucker (2017, September). Search engines and data retention: Implications for privacy and antitrust. Working Paper 23815, National Bureau of Economic Research.

Commission, E. Agreement on Commission's EU data protection reform will boost Digital Single Market.

Crandall, D. J., L. Backstrom, D. Cosley, S. Suri, D. Huttenlocher, and J. Kleinberg (2010). Inferring social ties from geographic coincidences. *Proceedings of the National Academy of Sciences 107*(52), 22436–22441.

Cranor, L. F., J. Reagle, and M. S. Ackerman (2000). Beyond concern: Understanding net users attitudes about online privacy. *The Internet upheaval: raising questions, seeking answers in communications policy*, 47–70.

Criado, N. and J. M. Such (2015). Implicit contextual integrity in online social networks. *Information Sciences 325*, 48–69.

Culnan, M. and P. Armstrong (1999, Jan-Feb). Information privacy concerns, procedural fairness, and interpersonal trust: An empirical investigation. *Organization Science 10*(1), 104–115.

Dean, T. J. and R. L. Brown (1995). Pollution regulation as a barrier to new firm entry: Initial evidence and implications for future research. *Academy of Management Journal 38*(1), 288–303.

Dillet, R. (2019, January). French data protection watchdog fines google 57*millionunderthegdpr.Techcrunch*.

Dinev, T. and P. Hart (2004). Internet privacy concerns and their antecedents-measurement validity and a regression model. *Behaviour & Information Technology 23*(6), 413–422.

Dinev, T. and P. Hart (2006). An extended privacy calculus model for e-commerce transactions. *Information systems research 17*(1), 61–80.

Dixon, L., S. M. Gates, K. Kapur, S. A. Seabury, and E. Talley (2006). The impact of regulation and litigation on small business and entrepreneurship.

Enck, W., P. Gilbert, S. Han, V. Tendulkar, B.-G. Chun, L. P. Cox, J. Jung, P. McDaniel, and A. N. Sheth (2014). Taintdroid: an information-flow tracking system for realtime privacy monitoring on smartphones. *ACM Transactions on Computer Systems (TOCS) 32*(2), 5.

Evans, D. S. (2009). The online advertising industry: Economics, evolution, and privacy. *Journal of Economic Perspectives 23*(3), 37–60.

Foxman, E. R. and P. Kilcoyne (1993). Information technology, marketing practice, and consumer privacy: Ethical issues. *Journal of Public Policy & Marketing 12*(1), 106–119.

FTC (2010, December). Protecting consumer privacy in an era of rapid change. *Staff Report*.

FTC (2011). FTC Charges Deceptive Privacy Practices in Googles Rollout of Its Buzz Social Network. Retrieved March 25, 2019 from https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz.

Galasso, A. and H. Luo (2018). When does product liability risk chill innovation? evidence from medical implants. *NBER Working Paper No. 25068*.

Goldfarb, A. and C. Tucker (2011a). Chapter 6 - online advertising. Volume 81 of *Advances in Computers*, pp. 289 – 315. Elsevier.

Goldfarb, A. and C. Tucker (2011b, May). Online display advertising: Targeting and obtrusiveness. *Marketing Science 30*, 389–404.

Goldfarb, A. and C. Tucker (2011c). Search engine advertising: Channel substitution when pricing ads to context. *Management Science 57*(3), 458–470.

Goldfarb, A. and C. Tucker (2012a). Privacy and innovation. In *Innovation Policy and the Economy, Volume 12*, NBER Chapters. National Bureau of Economic Research, Inc.

Goldfarb, A. and C. Tucker (2012b). Privacy and innovation. *Innovation Policy and the Economy 12*(1), 65 – 90.

Goldfarb, A. and C. Tucker (2012c). Shifts in privacy concerns. *American Economic Review: Papers and Proceedings 102*(3), 349–53.

Goldfarb, A. and C. Tucker (2013). Why managing customer privacy can be an opportunity. *Sloan Management Review Spring*.

Goldfarb, A. and C. Tucker (2019a). Digital economics. *Journal of Economic Literature 57*(1), 3–43.

Goldfarb, A. and C. Tucker (2019b). *Digital marketing*, pp. 259–290. Elsevier.

Goldfarb, A. and C. E. Tucker (2011d, January). Privacy regulation and online advertising. *Management Science 57*(1), 57–71.

Goodwin, C. (1991). Privacy: Recognition of a consumer right. *Journal of Public Policy & Marketing 10*(1), 149–166.

Hann, I.-H., K.-L. Hui, T. Lee, and I. Png (2002). Online information privacy: Measuring the cost-benefit trade-off. *ICIS 2002 proceedings*, 1.

Hillman, A. J. and M. A. Hitt (1999). Corporate political strategy formulation: A model of approach, participation, and strategy decisions. *Academy of management review 24*(4), 825–842.

Hirschprung, R., E. Toch, F. Bolton, and O. Maimon (2016). A methodology for estimating the value of privacy in information disclosure systems. *Computers in Human Behavior 61*, 443–453.

Hoffman, D. L. and T. P. Novak (2018). Consumer and object experience in the internet of things: An assemblage theory approach. *Journal of Consumer Research 44*(6), 1178–1204.

Hoffman, D. L., T. P. Novak, and M. Peralta (1999). Building consumer trust online. *Communications of the ACM 42*(4), 80–85.

Hui, K.-L., H. H. Teo, and S.-Y. T. Lee (2007). The value of privacy assurance: an exploratory field experiment. *Mis Quarterly*, 19–33.

Iqbal, N. (2018). Film fans see red over Netflix targeted posters for black viewers. Retrieved March 21, 2019 from https://www.theguardian.com/media/2018/oct/20/netflix-film-black-viewers-personalised-marketing-target.

Jaffe, A., J. Lerner, and S. Stern (2001). *Innovation Policy and the Economy Volume 1*. University of Chicago Press.

Jia, J., G. Z. Jin, and L. Wagman (2018). The short-run effects of gdpr on technology venture investment. Technical report, National Bureau of Economic Research.

Jiang, Z., C. S. Heng, and B. C. Choi (2013). Research noteprivacy concerns and privacy-protective behavior in synchronous online social interactions. *Information Systems Research 24*(3), 579–595.

Johnson, G., S. Shriver, and S. Du (2018). Consumer privacy choice in online advertising: Who opts out and at what cost to industry? https://pdfs.semanticscholar.org/51c5/588f9cb3e6aa6c9f26e7172a1d5780e6fef2.pdf.

Kalaignanam, K., T. Kushwaha, and K. Rajavi (2018). How does web personalization create value for online retailers? lower cash flow volatility or enhanced cash flows. *Journal of Retailing 94*(3), 265–279.

Kiebzak, S., G. Rafert, and C. E. Tucker (2016). The effect of patent litigation and patent assertion entities on entrepreneurial activity. *Research Policy 45*(1), 218–231.

Kihn, M. (2018). Did Google Just Kill Independent Attribution? Retrieved March 22, 2019 from https://adexchanger.com/analytics/did-google-just-kill-independent-attribution/.

Kim, N. (2014). Three's a crowd: Towards contextual integrity in third-party data sharing. *Harv. JL & Tech. 28*, 325.

Kim, T., K. Barasz, and L. K. John (2019). Why am i seeing this ad? the effect of ad transparency on ad effectiveness. *Journal of Consumer Research 45*(5), 906–932.

Kottasová, I. (2018). These companies are getting killed by GDPR. Retrieved March 13, 2019 from https://money.cnn.com/2018/05/11/technology/gdpr-tech-companies-losers/index.html.

Lambrecht, A. (2017). E-Privacy Provisions and Venture Capital Investments in the EU. https://www.ceps.eu/sites/default/files/E-Privacy%20Provisions%20and%20Venture%20Capital%20Investments%20in%20the%20EU.PDF.

Lambrecht, A. and C. Tucker (2013). When does retargeting work? Information specificity in online advertising. *Journal of Marketing Research 50*(5), 561–576.

Laufer, R. S. and M. Wolfe (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of social Issues 33*(3), 22–42.

Lee, D.-J., J.-H. Ahn, and Y. Bang (2011). Managing consumer privacy concerns in personalization: a strategic analysis of privacy protection. *Mis Quarterly*, 423–444.

Lenard, T. M. and P. H. Rubin (2009). In Defense of Data: Information and the Costs of Privacy. *Technology Policy Institute Working Paper*.

Lenard, T. M. and P. H. Rubin (2013). The big data revolution: Privacy considerations. *Technology Policy Institute*, 1–2.

Lerner, J. (2012). The impact of privacy policy changes on venture capital investment in online advertising companies. *Analysis Group*, 1–2.

Lobschat, L., B. Mueller, F. Eggers, L. Brandimarte, S. Diefenbach, M. Kroschke, and J. Wirtz (2019). Corporate digital responsibility. *Journal of Business Research*.

Lowry, M. and S. Shu (2002). Litigation risk and IPO underpricing. *Journal of Financial Economics 65*(3), 309–335.

Lwin, M., J. Wirtz, and J. D. Williams (2007). Consumer online privacy concerns and responses: a power–responsibility equilibrium perspective. *Journal of the Academy of Marketing Science 35*(4), 572–585.

Mainelli, M. (2017, October). Blockchain could help us reclaim control of our personal data. *HBR*, 716–745.

Malhotra, N. K., S. S. Kim, and J. Agarwal (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research 15*(4), 336–355.

Manyika, J., M. Chui, B. Brown, J. Bughin, R. Dobbs, C. Roxburgh, and A. H. Byers (2011, June). Big data: The next frontier for innovation, competition, and productivity. Technical report, McKinsey Global Institute.

Marman, J. (2019). Netflix Harnesses Big Data To Profit From Your Tastes. Retrieved October 19, 2019 from https://www.forbes.com/sites/jonmarkman/2019/02/25/netflix-harnesses-big-data-to-profit-from-your-tastes/455a22d266fd.

Marthews, A. and C. Tucker (2019). *Blockchain and Identity Persistence*. Oxford University Press.

Martin, K. and H. Nissenbaum (2016). Measuring privacy: an empirical test using context to expose confounding variables. *Colum. Sci. & Tech. L. Rev. 18*, 176.

Martin, K. D. and P. E. Murphy (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science 45*(2), 135–155.

Martin, N. and C. Matt (2018). Unblackboxing the effects of privacy regulation on startup innovation. In *Proceedings of the 2018 International Conference on Information Systems (ICIS)*. ICIS.

McAfee, A. and E. Brynjolfsson (2012). Big data: the management revolution. *Harvard business review 90*(10), 60–68.

McKnight, D. H., V. Choudhury, and C. Kacmar (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information systems research 13*(3), 334–359.

Milberg, S. J., H. J. Smith, and S. J. Burke (2000). Information privacy: Corporate management and national regulation. *Organization science 11*(1), 35–57.

Miller, A. and C. Tucker (2011a). Can healthcare information technology save babies? *Journal of Political Economy* (2), 289–324.

Miller, A. R. and C. Tucker (2009, July). Privacy Protection and Technology Diffusion: The Case of Electronic Medical Records. *Management Science 55*(7), 1077–1093.

Miller, A. R. and C. Tucker (2017). Frontiers of health policy: Digital data and personalized medicine. *Innovation Policy and the Economy 17*, 49–75.

Miller, A. R. and C. Tucker (2018). Privacy protection, personalized medicine, and genetic testing. *Management Science 0*(0), null.

Miller, A. R. and C. E. Tucker (2011b). Encryption and the loss of patient data. *Journal of Policy Analysis and Management 30*(3), 534–556.

Milne, G. R. and M. J. Culnan (2004). Strategies for reducing online privacy risks: Why consumers read (or dont read) online privacy notices. *Journal of interactive marketing 18*(3), 15–29.

Milne, G. R., G. Pettinico, F. M. Hajjat, and E. Markos (2017). Information sensitivity typology: Mapping the degree and type of risk consumers perceive in personal data sharing. *Journal of Consumer Affairs 51*(1), 133–161.

Miyazaki, A. D., A. J. Stanaland, and M. O. Lwin (2009). Self-regulatory safeguards and the online privacy of preteen children. *Journal of Advertising 38*(4), 79–91.

Moorman, C., G. Zaltman, and R. Deshpande (1992). Relationships between providers and users of market research: the dynamics of trust within and between organizations. *Journal of marketing research 29*(3), 314–328.

Mothersbaugh, D. L., W. K. Foxx, S. E. Beatty, and S. Wang (2012). Disclosure antecedents in an online service context: The role of sensitivity of information. *Journal of service research 15*(1), 76–98.

Nagaraj, A. (2018). The private impact of public information: Landsat satellite maps and gold exploration. *Working paper, UC Berkeley*.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Wash. L. Rev. 79*, 119.

Nissenbaum, H. (2010). *Privacy in context: technology, policy, and the integrity of social life*. Stanford Law Books.

Nissenbaum, H. (2011). A contextual approach to privacy online. *Daedalus 140*(4), 32–48.

Nissenbaum, H. (2018). Respecting context to protect privacy: Why meaning matters. *Science and engineering ethics 24*(3), 831–852.

Nowak, G. J. and J. Phelps (1997). Direct marketing and the use of individual-level consumer information: Determining how and when privacy matters. *Journal of Direct Marketing 11*(4), 94–108.

Paul, K. (2018). Your childs Wi-Fi-connected toy may be spying on them heres how to prevent it. Retrieved April 16, 2019 from https://www.marketwatch.com/story/dont-buy-a-wi-fi-connected-toy-for-your-child-without-reading-this-2017-07-20.

Pavlou, P. A. (2011). State of the information privacy literature: Where are we now and where should we go? *MIS quarterly*, 977–988.

Pavlou, P. A., H. Liang, and Y. Xue (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS quarterly*, 105–136.

Phelps, J., G. Nowak, and E. Ferrell (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing 19*(1), 27–41.

Porter, M. E. and J. E. Heppelmann (2014). How smart, connected products are transforming competition. *Harvard business review 92*(11), 64–88.

Porter, M. E. and C. Van der Linde (1995). Toward a new conception of the environment-competitiveness relationship. *Journal of economic perspectives 9*(4), 97–118.

Rafieian, O. and H. Yoganarasimhan (2019). Targeting and privacy in mobile advertising. *Available at SSRN 3163806*.

Roberts, J. J. (2019). Google, Facebook, and the Legal Mess Over Face Scanning. Retrieved April 15, 2019 from http://fortune.com/2019/01/04/google-face-scanning-illinois/.

Rousseau, D. M., S. B. Sitkin, R. S. Burt, and C. Camerer (1998). Not so different after all: A cross-discipline view of trust. *Academy of management review 23*(3), 393–404.

Rust, R. T., P. Kannan, and N. Peng (2002). The customer economics of internet privacy. *Journal of the Academy of Marketing Science 30*(4), 455–464.

Schoenbachler, D. D. and G. L. Gordon (2002). Trust and customer willingness to provide information in database-driven relationship marketing. *Journal of interactive marketing 16*(3), 2–16.

Schuler, D. A. and K. Rehbein (1997). The filtering role of the firm in corporate political involvement. *Business & Society 36*(2), 116–139.

Schuler, D. A., K. Rehbein, and R. D. Cramer (2002). Pursuing strategic advantage through political means: A multivariate approach. *Academy of Management Journal 45*(4), 659–672.

Schumann, J. H., F. von Wangenheim, and N. Groene (2014). Targeted online advertising: Using reciprocity appeals to increase acceptance among users of free web services. *Journal of Marketing 78*(1), 59–75.

Sheehan, K. B. and M. G. Hoy (2000). Dimensions of privacy concern among online consumers. *Journal of Public Policy and Marketing 19*, 62–73.

Shiller, B., J. Waldfogel, and J. Ryan (2018). The effect of ad blocking on website traffic and quality. *The RAND Journal of Economics 49*(1), 43–63.

Smith, H. J., T. Dinev, and H. Xu (2011). Information privacy research: an interdisciplinary review. *MIS quarterly 35*(4), 989–1016.

Smith, H. J., S. J. Milberg, and S. J. Burke (1996). Information privacy: Measuring individuals concerns about organizational practices. *MIS Quarterly 20*(2), 167–196.

Solove, D. J. (2012). Introduction: Privacy self-management and the consent dilemma. *Harv. L. Rev. 126*, 1880.

Solove, D. J. and P. Schwartz (2014). *Information privacy law*. Wolters Kluwer Law & Business.

Son, J.-Y. and S. S. Kim (2008). Internet users' information privacy-protective responses: A taxonomy and a nomological model. *MIS quarterly*, 503–529.

Song, T., R. Li, B. Mei, J. Yu, X. Xing, and X. Cheng (2017). A privacy preserving communication protocol for iot applications in smart homes. *IEEE Internet of Things Journal 4*(6), 1844–1852.

Stewart, D. W. (2017). A comment on privacy. *Journal of the academy of marketing science 45*(2), 156–159.

Stone, E. F., H. G. Gueutal, D. G. Gardner, and S. McClure (1983). A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. *Journal of applied psychology 68*(3), 459.

Stutzman, F. D., R. Gross, and A. Acquisti (2013). Silent listeners: The evolution of privacy and disclosure on facebook. *Journal of privacy and confidentiality 4*(2), 2.

Sutanto, J., E. Palme, C.-H. Tan, and C. W. Phang (2013). Addressing the personalization-privacy paradox: an empirical assessment from a field experiment on smartphone users. *Mis Quarterly*, 1141–1164.

Tanner, A. (2016). How Data Brokers Make Money Off Your Medical Records. Retrieved March 17, 2019 from https://www.scientificamerican.com/article/how-data-brokers-make-money-off-your-medical-records/.

Thomas, L. G. (1990). Regulation and firm size: Fda impacts on innovation. *The RAND Journal of Economics*, 497–517.

Tsai, J. Y., S. Egelman, L. Cranor, and A. Acquisti (2011). The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research 22*(2), 254–268.

Tucker, C. E. (2014). Social networks, personalized advertising, and privacy controls. *Journal of Marketing Research 51*(5), 546–562.

Urban, G. L., C. Amyx, and A. Lorenzon (2009). Online trust: state of the art, new frontiers, and research potential. *Journal of interactive marketing 23*(2), 179–190.

Urban, G. L., F. Sultan, and W. J. Qualls (2000). Placing trust at the center of your internet strategy. *Sloan Management Review 42*(1), 39–39.

Wallace, N. and D. Castro (2018). The impact of the eus new data protection regulation on ai. *Centre for Data Innovation: Washington, DC, USA*.

Wang, Y. and M. Kosinski (2018). Deep neural networks are more accurate than humans at detecting sexual orientation from facial images. *Journal of personality and social psychology 114*(2), 246.

Warren, S. D. and L. D. Brandeis (1890, December). The right to privacy. *Harward Law Review 4*(5), 193–220.

Wedel, M. and P. K. Kannan (2016). Marketing analytics for data-rich environments. *Journal of Marketing 80*(6), 97–121.

Wieringa, J., P. Kannan, X. Ma, T. Reutterer, H. Risselada, and B. Skiera (2019). Data analytics in a privacy-concerned world. *Journal of Business Research*.

Xu, H., H.-H. Teo, B. C. Tan, and R. Agarwal (2012). Research noteeffects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: a study of location-based services. *Information Systems Research 23*(4), 1342–1363.

Zhang, J. and M. Wedel (2009). The effectiveness of customized promotions in online and offline stores. *Journal of Marketing Research (JMR) 46*(2), 190 – 206.

Zhou, M. (2019). DuckDuckGo is now a default search engine option in Chrome. Retrieved March 18, 2019 from https://www.cnet.com/news/duckduckgo-is-now-a-default-search-engine-option-in-chrome/.

Zyskind, G., O. Nathan, et al. (2015). Decentralizing privacy: Using blockchain to protect personal data. In *Security and Privacy Workshops (SPW), 2015 IEEE*, pp. 180–184. IEEE.

Figure 1: Conceptual Framework