Strategies for Managing the Privacy Landscape

Ramon Casadesus-Masanell
Harvard Business School

Andres Hervas-Drane
Cass Business School

November 14, 2019

ABSTRACT

Firms use consumer personal information to improve their products and services. Personal information is open to misuse, however, and when exploited for undesired or unexpected purposes reduces consumer's trust in the firm and their willingness to provide personal information. How should firms manage consumer privacy? We present a framework to help firms identify their privacy impact on consumers and respond appropriately. We argue that firms should consider the full spectrum of entities they interact with and which can exploit consumer personal information, which includes: the political environment (government), the security environment (hackers), the market environment (third party firms), and the social environment (peers). Firms should pursue strategies to maximize the privacy impact consumers derive across these domains, augmenting sources of positive impact and mitigating those that generate negative impact. Successful strategies for managing privacy combine four approaches: balanced cooperation with government, heightened security against hackers, limited disclosure to third party firms, and moderated propagation with peers.

KEYWORDS: Consumer Privacy, Privacy Threats, Strategy Framework, Strategy Interactions

1. Introduction

The collection and exploitation of personal information has become a critical aspect of business. Information about consumers enables firms to create better and more personalized products and services, generating value for organizations and individuals alike. However, the collection and exploitation of personal information can also be harmful for consumers when used for undesired or unexpected purposes. Surveys indicate that concerns over the misuse and safety of personal information have a chilling effect on consumer's willingness to transact business online and share personal data.[1]

Firms face an increasingly pressing and daunting challenge: how to leverage personal information to provide the kind of products and service features consumers want while minimizing the threats. In this paper, we argue that firms can tackle this challenge by expanding the scope of privacy management to encompass external players: those entities operating outside the firm's boundaries that can access consumer information through the firm and whose actions have an impact on consumers.

Figure 1 depicts the impact of external players and the role of the firm in the context of consumer privacy. Information exploitation by external players can have a positive impact on consumers (for example, advertisers introduce people to things they want to know about) but can also have a negative impact (such as when the ads or the communication are distracting or upsetting). The latter is often due to conflicts of interest between consumers, the firm, and external players. When the negative impact intensifies and

[1] The U.S. Department of Commerce reported that privacy and security concerns have stopped 45% of U.S. online households from "conducting financial transactions, buying goods or services, posting on social networks, or expressing opinions on controversial or political issues via the Internet." See "Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities," *US Department of Commerce NTIA blog*, May 13 2016, https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities. Similar effects have been reported for consumer search activity based on revelations of government surveillance. See A. Marthews and C. E. Tucker, "Government Surveillance and Internet Search Behavior," *working paper*, February 2017, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412564.

overrides the positive elements, this reduces consumer trust in the firm and the demand for its products and services. Eventually, this reduces the provision of personal information to the firm, an essential input, weakening the firm's ability to create value in the marketplace and placing it at a competitive disadvantage vis-à-vis competitors with superior privacy management.

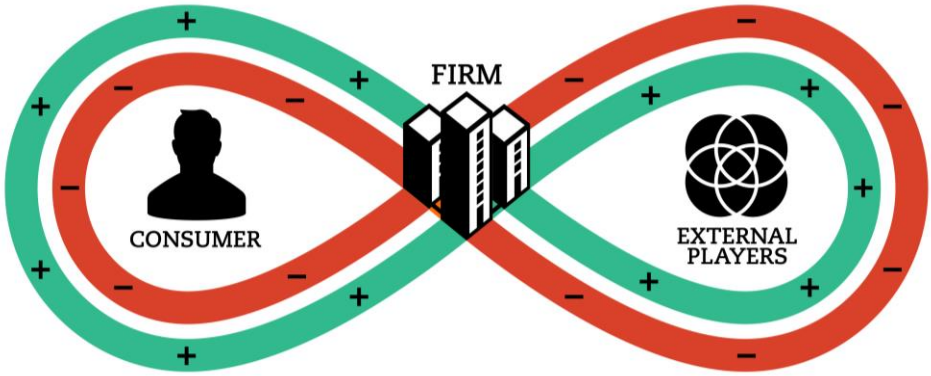


Figure 1: The Firm as a Personal Information Gateway
Caption: Firms act as personal information gateways between the consumer (on the left) and external players (on the right). The exploitation of personal information by external players can generate positive impact (as depicted by the green) when it aligns with consumer expectations and creates value, but can generate negative impact (as depicted by the red) when it diverges from consumer expectations and causes harm.

Yet, despite the growing importance of privacy management for business, we lack a theoretical toolset to identify sources of positive and negative impact and to evaluate strategy responses. Without such a toolset, firms can fail to recognize their privacy impact on consumers or implement suboptimal strategies. We have developed a framework to help managers navigate these challenges in what we call the *privacy landscape*. Our framework encompasses the key external players that firms need to account for to manage their privacy impact on consumers and enables superior privacy management – an essential capability that can improve firm performance. Our goal is to provide a comprehensive tool to assist managers with strategic decision making on consumer privacy.

We develop the privacy landscape framework by drawing from our own work on consumer privacy and business models across several industries. A key building block is Casadesus-Masanell and Hervas-Drane (2015), where we study fundamental privacy trade-offs by analyzing the information provision choices of consumers and the information exploitation choices of firms.

Our work also builds on the growing management and economics literature on consumer privacy. A first block of literature has explored its impact on the marketplace mechanism. Shy and Stenbacka (2015) and Montes, Sand-Zantman, and Valletti (2019) analyze the implications of consumer privacy for competition among firms, and Campbell, Goldfarb, and Tucker (2015) analyze the impact of privacy regulation. In another strand of the literature, Villas-Boas (2004), Taylor (2004), and Acquisti and Varian (2005) analyze price discrimination schemes based on consumer provision of information. The literature on multisided platforms is key to understand the firm's intermediation between consumers and some external players. McIntyre and Srinivasan (2016) provide a literature review and Hagiu (2014) discusses key managerial choices.

Another block of the literature has explored the implications of consumer privacy in social media. Toubia and Stephen (2013) and Hewett et al. (2016) examine the drivers and patterns of information provision by consumers and firms, respectively. Halberstam and Knight (2016) and Pfeffer, Zorbach, and Carley (2014) analyze peer interactions and the propagation of information in social networks. Godey et al. (2016) and Tucker (2014) analyze the effectiveness of firm activity on these services and the impact of privacy controls.

A third literature block has considered the various security challenges related to the management of personal information. Anderson and Moore (2006) identify the general economics tradeoffs and Spiekermann et al. (2015) discuss key privacy challenges. Roberds and Schreft (2009) as well as Angst et al.

(2017) analyze the incentives of malicious actors and the effectiveness of preventive measures. Upton and Creese (2014) and DalleMule and Davenport (2017) propose cybersecurity best-practices and discuss their fit within the organization's data strategy. The role of government is considered by Abelson et al. (2015).

We have used the above body of work to identify the main sources of positive and negative consumer impact arising from the exploitation of personal information, as well as the incentives of the various players involved. We structure our framework by categorizing the external players that generate this impact into four separate domains. We then examine the firm's interaction with these external players to identify the key tensions present in each domain and formulate strategy recommendations to address them. Our analysis of these domains is also informed by our own company case studies, where we have analyzed how several elements of the framework operate.[2]

The contribution of our present work is twofold. First, our framework aims to encompass all the external domains relevant to the strategic management of consumer privacy. While the market and security environments have received much attention in the literature, the social and political environments have received comparatively little from a privacy standpoint. By focusing on the impact that information exploitation by all external players has on the consumer, our framework provides structure and clarity on the scope of privacy management and the challenges it comprises.

Second, our framework helps to identify and resolve strategy interactions spanning several domains. The literature has, for the most part, considered these different domains in isolation. We explore the interactions that arise between the different domains and find that they are key to effective privacy management in the most complex cases. Analysis of these interactions also explains the connections between various consumer data related phenomena and privacy management. To the best of our knowledge, our framework is the first to formalize this aspect of privacy management.

The rest of the paper is structured as follows. In the next section, we introduce the elements of the framework. We identify four domains or types of external players and provide guidance for the firm to assess the relative importance of each domain (see Table 1). We then examine each of the four domains in isolation, and consider how each external player generates positive and negative privacy impact for consumers. In Section 3 we turn to the application of the framework. We characterize a core privacy strategy for the firm to maximize privacy impact in each domain (see Table 2) and produce several privacy landscape representations (see Table 3). We then consider the impact of strategy interactions across domains by examining a high-profile case, that of Facebook and Cambridge Analytica, and provide examples of additional interactions (see Table 4). We conclude in Section 4.

2. The Privacy Landscape Framework

We structure the privacy landscape into four domains corresponding to these external players: government (political environment); hackers (security environment); third parties (market environment); and peers (social environment). These players access the personal information of consumers through the firm and their actions, in turn, have an impact on consumers. To understand the firm's privacy landscape, managers need to assess the relative importance or weight of each domain. In general, this varies across industries and firms. We highlight the factors that contribute to positive and negative consumer impact in Table 1 by considering the nature of the consumer information the firm holds and the purposes for which it can be exploited.

[Insert Table 1 about here]

In what follows we examine the incentives of external players in each domain and the ways in which they can impact consumers. We also propose a core strategy for the firm to maximize privacy impact in each domain. External players operate outside the boundaries of the typical firm but not outside its sphere of influence, so their impact can be shaped by the firm's choices. A firm aiming to maximize consumer privacy impact must take advantage of positive elements and mitigate sources of negative impact.

[2] Our case studies include in-depth analysis of the strategies deployed by Amazon, Apple, eBay, Netflix, Spotify, Uber, and Walmart among other large companies. See for instance Aversa, Hervas-Drane, and Evenou (2019) and Casadesus-Masanell and Elterman (2019).

2.1 The Political Environment

Governments play a pivotal role in the privacy landscape. They have the ability to access consumer information from the firm and to mandate data collection and retention policies. Governments can use this information to improve public services. The population's lifestyle habits can be used to enhance healthcare provision, financial activity records can be used to improve taxation, and mobility patterns can help optimize infrastructure investments or identify security threats. These public services have a strong positive impact on society and this provides a clear rationale for information exploitation by government.

Governments also use personal information in ways that have a direct impact on individual consumers. This impact is positive when personal information reduces administrative burdens or provides entitlement to benefit payments. But it can be detrimental if personal information triggers a tax-fraud investigation or hinders a security clearance review. Government activity exhibits the properties of a commons problem because there is an underlying tension between the individual and collective interest; information exploitation for the collective benefit can be detrimental to some individuals. Moreover, governments can misuse personal information. Access to personal data enables governments to impinge on free speech and individual rights, and facilitates political profiling, monitoring, and manipulation. For all these reasons, consumers often perceive the individual impact of government to be negative. These risks can undermine consumer's willingness to engage with the firm's product or service, particularly if they anticipate that their personal information will be used by government to their detriment.[3]

In dealing with the political environment, the firm should adopt a strategy of *balanced cooperation* with government. That is, the firm should weigh the benefits of facilitating government access to consumer information against the negative impact it can generate. On the one hand, the firm must cooperate with government by complying with legal access requests for consumer information. The firm should also share consumer information when this improves the provision of public services or has the potential to generate positive impact for consumers. On the other hand, the firm must carefully weigh government requests for consumer information when compliance is not mandatory and there is risk of negative impact from targeted action. If the potential for negative impact is high, it may be preferable to challenge the requests, or even eliminate products or services with high compliance costs.[4]

2.2 The Security Environment

For most organizations storing personal information of any value, it is all but certain that hackers will attempt to breach their systems to access it. Data thieves and organized criminals pursue unauthorized access to consumer information and are driven by the goal of financial gain. Rogue employees, subcontractors, and state-sponsored organizations can also operate as hackers when pursuing unauthorized access. These attacks generate negative impact on consumers through financial losses, identity theft, or reputational damage when sensitive information is publicly disclosed.[5] Hacking activity seldomly has a positive impact on consumers,

---

[3] Consider for example the fraud investigation pursued by the Manhattan, New York District Attorney in 2013. The district attorney served Facebook with 381 warrants seeking photos, private messages, and other personal information from 134 Facebook user profiles. The Facebook data showed people who claimed to be physically disabled performing a variety of activities such as fishing, martial arts, and even jet skiing. Access to this information helped public authorities monitor disability benefits and deter fraud. But the findings and the subsequent stories in the media likely had a chilling effect on other individuals who may have worried about the unintended consequences of sharing their activity on social media, an undesirable outcome for Facebook. See "Charges for 106 in Huge Fraud Over Disability," New York Times, January 7 2014, https://www.nytimes.com/2014/01/08/nyregion/retired-new-york-officers-and-firefighters-charged-in-social-security-scheme.html.

[4] A high-profile example is that of Google's exit from the Chinese search engine market in 2010. The firm stated that it was the victim of a "sophisticated cyber attack originating from China. [...] these attacks and the surveillance they uncovered – combined with attempts over the last year to further limit free speech on the web in China including the persistent blocking of websites such as Facebook, Twitter, YouTube, Google Docs and Blogger – had led us to conclude that we could no longer continue censoring our results on Google.cn." See "A new approach to China: an update," Official Google blog, March 22 2010, https://googleblog.blogspot.com/2010/03/new-approach-to-china-update.html.

[5] The security breach of AdultFriendFinder.com in 2015 provides a good example of the reputational damage hackers can cause. Founded in 1996, the online dating service stored sensitive information about past and present users covering a period of almost 20 years. The hackers gained access to email addresses, ages, zip codes, sexual orientations, and other sensitive personal details – then published the information of 3.9 million users on the Internet. See "Adult dating site hack exposes millions of users," Channel 4, May 21 2015, https://www.channel4.com/news/adult-friendfinder-dating-hack-internet-dark-web.

with the exception of cases where there is a public interest (revelations of government corruption or crime, for instance).

The firm should adopt a strategy of *heightened security* against hackers, by securing personal information to minimize unauthorized access. Firms tend to underinvest in cybersecurity because they internalize the cost of a breach on their business but not the costs it generates for consumers. The firm also needs to signal its cybersecurity commitment to consumers. Stating that personal data is safe or delaying the disclosure of security breaches will not be enough to assuage consumers. The firm can signal its commitment by showcasing its cybersecurity investments, adopting costly pledges against security breaches, and building a strong security track record over time.

2.3 The Market Environment

Most businesses share consumer information with third party firms such as payment processing intermediaries, fraud prevention services, or subcontractors providing ancillary services. These commercial partners contribute to improve the firm's operations, so this disclosure of information is generally aligned with consumer expectations. However, firms also disclose consumer information for revenue-generating purposes by engaging in data sharing agreements, targeted advertising, or providing referrals to third parties. For example, firms disclose personal information when they allow data brokers to track and profile their customers or when they process personal information to display targeted ads.[6]

Third parties on the receiving end of disclosure can have a positive impact on consumers. They can foster synergies across different products and services, generate complementary transaction opportunities, or create awareness about products and services suited to consumer needs. However, third parties can also have harmful effects. Commercial interruptions impose attention costs on consumers and are often perceived to be annoying. Unsolicited offers based on personal events (for example, a divorce or an illness) can be distressing. And third parties can also exploit personal information to engage in price discrimination, which results in some consumers being charged higher prices.[7]

The firm should adopt a strategy of *limited disclosure* to third parties, by weighing the benefits of disclosing consumer information against the negative consumer impact it generates. Disclosure allows the firm to tap into new revenue streams, and high levels of disclosure can be profitable and desirable when it generates positive impact for consumers. But when disclosure is harmful to consumers, because it generates distraction, distress, or detrimental consequences (such as higher prices), there is an underlying conflict of interest the firm should carefully consider. The firm could compensate consumers for disclosure, or could limit disclosure and sacrifice revenues. In the worst cases, the firm could cease disclosure altogether. Evidence of negative impact includes consumer adoption of ad-blocking technology, unwillingness to link accounts and identity across services, and increased opt-outs from activity tracking and automated reporting mechanisms or efforts to thwart such systems.[8]

---

[6] We use the term disclosure to refer to the exploitation of consumer information for revenue-generating purposes. Note that some forms of exploitation do not imply information sharing with third parties (i.e., consumer information need not be disclosed in full to the third party). For example, the targeting tools provided to advertisers may not allow them to observe the identity of target consumers. Nonetheless, we expect the outcome to approximate that of information sharing because the firm exploiting the information will account for the objectives of advertisers to maximize the revenues generated in the process.

[7] Consumers are generally uncomfortable with price discrimination practices that set prices based on consumer identity, as illustrated by the Amazon.com backlash in 2000 that led the firm to announce it would not set prices on its website based on customer demographics. See "Amazon apologizes for price-testing program that angered customers," Computer World, September 28 2000, https://www.computerworld.com/article/2588337/amazon-apologizes-for-price-testing-program-that-angered-customers.html.

[8] Recent regulatory initiatives such as the European Union's General Data Protection Regulation require firms to explain disclosure practices to consumers and obtain their explicit consent. These regulations are designed to foster consumer awareness about how their personal information is exploited and strengthen their control over the process. While the regulations do not alter the fundamental tradeoffs generated by disclosure, and their longer-term implications for marketplace practices are yet to be tested, we expect them to discipline the disclosure choices of firms and curb some of the worst practices. In the cases where it is difficult for firms to obtain consumer consent, firms can offer consumers a choice: a free or subsidized tier for those who consent to more disclosure and a paid or premium tier for those who prefer not to.

2.4 The Social Environment

Consumers interact with a broad range of peers on social platforms including friends, family members, business associates, and other users in communities and forums. Consumers propagate personal information in these interactions by building their user profiles, posting about their experiences, and replying to the posts of others. Peer interactions are valuable to consumers and generate positive impact. They are also the lifeblood of social platforms such as Facebook or Twitter and are relevant to firms that use these platforms to reach and communicate with consumers. When firms provide customer service or run social media campaigns on these platforms, they are directly exposed to the peer connections consumers have established there.

Peer interactions can also have a negative impact on consumers, and this often arises when personal information propagates to undesired recipients. Differences over political preferences or religious values can trigger disagreements with friends, and professional views can trigger conflicts of interest with work colleagues. In extreme cases, the propagation of opinions that a vocal community disapproves can spur episodes of harassment or cyberbullying. Social media users are becoming more aware of these negative effects as they gain experience and pay closer attention to what they post and share with their peers.[9] But firms must also account for these risks, as their interactions with consumers on social platforms can propagate personal information to peers.

The firm should adopt a strategy of *moderated propagation* with peers, by weighing the benefits of propagating consumer information against the negative impact it can generate. While propagating personal information with peers can be desirable for the firm, as there are obvious benefits to generating buzz on social platforms by engaging and interacting with lots of consumers, it is harmful for consumers when it triggers negative interactions with peers. There is an underlying conflict of interest because the benefits of engagement can accrue to the firm (through brand recognition and product prominence) while the risks of negative peer interactions are often borne by consumers. The firm should internalize this risk of negative impact by moderating its level of propagation, even when this limits the intensity of engagement and reduces the returns of marketing efforts. The firm can achieve this by carefully selecting the topics of engagement, leading the conversation to ensure it adheres to prevailing social norms and expectations, and adopting practices to limit the public exposure of consumers.

3. Applying the Framework

Our framework can be applied to analyze the firm's strategy response to the privacy landscape it operates in. Once the weight of each domain has been evaluated (see Table 1) the next step is to identify privacy strategies to tackle the challenges present. These strategies should maximize consumer privacy impact by taking advantage of opportunities to increase positive impact and mitigating privacy threats to reduce negative impact. The four core strategies outlined in the preceding section are designed to achieve this, and in Table 2 we characterize their properties as well as key tactics and challenges for implementation.

[Insert Table 2 about here]

The firm also needs to consider strategy interactions across domains, which can undermine overall privacy performance. A strategy interaction arises when a strategy designed to maximize privacy impact in one domain affects the privacy impact generated in other domains, that is, it interacts with the strategies deployed for other domains. These interactions can arise because there are several external players and many ways in which they can access and exploit consumer information, so strategy choices can have unintended or unanticipated consequences on other external players. Interactions increase the complexity of the firm's strategy problem because domains can no longer be considered in isolation.

In Table 3, we represent the privacy landscapes of four firms operating in different industries. The more domains command a high weight for the firm, the higher the risk of strategy interactions arising. As

[9] A substantial number of consumers have experienced the negative effects of social media. In a January 2017 Pew Research Poll, 41% of adults reported having experienced online harassment, with 58% of them reporting that the most recent incident took place on social media. See "Online harassment in focus: Most recent experience," Pew Research Center, July 11 2017, http://www.pewinternet.org/2017/07/11/online-harassment-in-focus-most-recent-experience/#fn-19049-3.

showcased by these examples, managers need to deal with different sets of strategies and different sets of potential strategy interactions.

[Insert Table 3 about here]

To understand how strategy interactions can pan out, consider the case of Facebook and Cambridge Analytica. Facebook's privacy landscape (see Table 3) is particularly complex given that many domains command a high weight. Cambridge Analytica was a British data consulting firm that reportedly accessed the data of 87 million Facebook users through a Facebook app, and then exploited the data to target users with political ads.

Developers supplying apps on Facebook are third parties to Facebook. The firm's third party strategy exhibited a high level of disclosure, providing app developers with access to the personal information of their app users and also to that of their app users' friends on the platform. This access to personal information over peer connections could be used to improve the social features of apps. But it could also be abused to harvest personal information on a large scale. The app that harvested information for Cambridge Analytica was installed by approximately 250,000 users, but these users had Facebook friends and the app accessed their personal information through the peer connections on the social platform.[10]

Political advertising on Facebook operated in the same fashion as commercial advertising. Facebook allowed advertisers to narrowly define their target audience and rewarded ads that drew user engagement, serving them to more users at the same cost. This mechanism was designed for commercial advertising and may have unintended consequences when applied to political advertising.[11] Cambridge Analytica exploited the trove of consumer information it harvested by targeting political messages on behalf of its clients during high-stakes campaigns, including the 2016 US presidential election and 2016 UK referendum on European Union membership.

Cambridge Analytica's actions generated substantial negative impact on Facebook users. Millions of users discovered that their personal information had been accessed without their consent through apps installed by their peers, contrary to Facebook claims that that their personal information was safeguarded. They were also exposed to political messages designed to mobilize and polarize users on the social platform, generating negative interactions among peers due to differences in political preferences. In retrospective, Facebook failed to anticipate or underestimated the negative impact that strategy interactions between third parties, political actors, and peers could generate. CEO Mark Zuckerberg admitted as much to users when stating that "we have a responsibility to protect your data" and "developers built shady apps that abused people's data."[12] Following Facebook's earning report in July 2018 where the effect of these revelations was disclosed, the company's shares dropped by 20% generating the largest one-day loss on record for a publicly listed company.

Facebook attempted to resolve these strategy interactions by limiting disclosure with third parties and reducing cooperation with political actors. On the one hand, Facebook restricted app developer access to consumer information, monitoring how apps access personal information over peer connections and introducing user controls to restrict it. Tens of thousands of apps were suspended and integration with high-profile services such as Sony's PlayStation network were halted.[13] On the other hand, Facebook designed

---

[10] The app was presented as a personality survey and users were told the data would be used for academic purposes in exchange for a small sum. The app was developed by Global Science Research, a firm founded by Aleksandr Kogan, a psychology professor at Cambridge University, who began harvesting data for Cambridge Analytica in 2014. See K. Collins and G. J. X. Dance, "How Researchers Learned to Use Facebook 'Likes' to Sway Your Thinking," The New York Times, March 20 2018, https://www.nytimes.com/2018/03/20/technology/facebook-cambridge-behavior-model.html.

[11] Michael Franz, co-executive director of the Wesleyan Media Project, noted that it "would incentivize [political] campaigns to not only target their messages, but to target them in ways that would further inflame and polarize opinions, not only as a mechanism to increase support among your base, but also as a mechanism to make it cost-efficient." See "How Facebook rewards polarizing political ads," The Verge, October 11 2017, https://www.theverge.com/2017/10/11/16449976/facebook-political-ads-trump-russia-election-news-feed.

[12] See Mark Zuckerberg's public posts on Facebook dated March 21 2018, https://www.facebook.com/zuck/posts/10104712037900071, as well as December 5 2018, https://www.facebook.com/zuck/posts/10105559172610321.

[13] See "How to Prevent Facebook Apps from Accessing Your Profile Information," Intego, March 27 2018, https://www.intego.com/mac-security-blog/how-to-prevent-facebook-apps-from-accessing-your-profile-information. See also "An Update on Our App Developer Investigation," Facebook Newsroom, September 20 2019,

specific rules for political advertising, including prescreening of political advertisers and displaying disclaimers on political ads to identify their source.[14] In short, Facebook's attempted to mitigate harmful strategy interactions by redesigning its third party and government strategies.

Strategy interactions are key to understanding the complexity of the privacy landscape. The Cambridge Analytica debacle and Facebook's responses cannot be understood without careful analysis of how Facebook's strategy choices affected the external players involved and their impact on consumers. Had these strategy interactions been evaluated more carefully in the design of the service, Facebook could have likely prevented this fiasco.

[Insert Table 4 about here]

In Table 4 we identify key types of strategy interactions depending on which external player plays a leading role or triggers them, and provide additional examples. Resolving these interactions sometimes requires firms to forego revenues, like Facebook does when restricting political advertising or BBC News when dropping ad networks. In other cases, it requires increased spending in some areas as is the case of WeChat when policing user activity or Amazon when monitoring the integrity of product reviews.

To be sure, not all firms face high-stake interactions such as those featured in Table 4. In many cases, firms face a less challenging privacy landscape and can manage consumer privacy by implementing core strategies to address each domain in isolation. However, when relevant strategy interactions arise, affected strategies need to be carefully evaluated and redesigned to maximize overall privacy impact for consumers. In the worst scenarios, redesigning the core product or service may be the only viable solution.[15]

4. Closing remarks

Consumer privacy presents a complex strategic problem. Firms accumulating and exploiting personal information need to manage privacy, and our framework provides a roadmap to do so. A first step is a wide-ranging assessment of the political, security, market, and social environments the firm operates in, by examining the impact that external players in each of these four domains can have on consumers through the firm's product or service. A second step is the adoption of core strategies to promote positive elements and mitigate negative ones within each domain. The third step is to identify possible interactions that arise between these strategies and which may compromise the firm's overall privacy performance. The challenge for firms is to design and implement strategies in ways that account for these interactions, with the overarching goal of maximizing their overall privacy impact on consumers.

Our analysis reveals a general privacy rule: one size does not fit all. Because privacy landscapes differ, firms need to adopt strategy responses tailored to the privacy landscape they operate in. Moreover, the need for strategy responses that address the privacy concerns of consumers will continue to evolve with changes in regulation, security, technology, and social norms. New avenues to collect personal information, for instance through wearable devices that record biometric information or smart home devices that monitor private spaces, will generate new benefits for consumers but also new threats. Delivering the benefits while mitigating the threats is the ongoing challenge for privacy management. Organizations that seize control of their privacy landscape will find ways to address this challenge and maintain consumer's trust.

---

https://newsroom.fb.com/news/2019/09/an-update-on-our-app-developer-investigation and "Cleaning Up Data Access for Partners," Facebook Newsroom, July 24 2019, https://newsroom.fb.com/news/2019/07/cleaning-up-data-access.

[14] See "Protecting Elections in the EU," Facebook Newsroom, March 28 2019, https://newsroom.fb.com/news/2019/03/ads-transparency-in-the-eu. Facebook has so far been unwilling to moderate the content of political ads, however. See "Facebook Doesn't Want to Censor Political Ads Over Accuracy, Executive Says," Wall Street Journal, October 22 2019, https://www.wsj.com/articles/facebook-doesnt-want-to-censor-political-ads-over-accuracy-executive-says-11571720440.

[15] For example, many cloud computing providers adopt the role of a custodian, storing consumer information but relinquishing the ability to process it by delegating the encryption keys to consumers. This prevents the firm from exploiting consumer information to generate positive privacy impact, but also precludes sources of negative impact that could dissuade consumers from adopting these services.

Table 1: Mapping your Privacy Landscape

<table>
<tr><td colspan="2">The following factors contribute to the weight or saliency of each domain for the firm. Each factor can generate positive (+) or negative (-) privacy impact on consumers, though in some cases the impact is ambiguous (+/-) because it varies across consumers or depends on the specific circumstances. Domains with the most potential for positive or negative impact should receive greater weight than those where the potential for impact is lower.</td></tr>
<tr><td>The political environment is salient when:

(+) Consumer information can improve and tailor the provision of public services (e.g., individual health metrics and lifestyle choices)

(+) Consumer information can be aggregated to improve the overall efficiency of public services (e.g., population mobility patterns, lifestyle trends, seasonal effects)

(+/-) Consumer information may be exploited by public authorities for targeted interventions (e.g., financial transactions could be reviewed for taxation purposes)

(-) Consumer information may facilitate profiling by political or ideological affinity (e.g., political discussion threads in forums or social media)

(-) Product or service provides effective channels to monitor the communications of individuals and deliver targeted messages (e.g., mobile telephone providers)

(+/-) The firm has a large market share or a market leadership position. Large firms provide access to larger stocks of personal information and can set precedents for the sector.</td><td>The security environment is salient when:

(-) Consumer information has financial value for hackers (e.g., credit card and billing information)

(-) Consumer information has reputational or intelligence value for hackers (e.g., personal correspondence could allow targets to be shamed)

(-) Product or service provides effective means to circumvent security protections (e.g., an email account may be used to reset passwords linked to that account)

(-) Consumer information reveals physical location or travel plans that could inform hackers (e.g., calendar information)

(+/-) Information relates to specific individuals or events that are relevant to the public interest (e.g., whistleblowing of government corruption)

(+/-) Firm has a large market share or is a market leader. Large firms provide access to larger stocks of personal information.</td></tr>
<tr><td>The market environment is salient when:

(+) Consumer information improves integration across products and services (e.g., single login functionality and profile sharing across services)

(+) Consumer information facilitates personalization of products and services (e.g., past correspondence improves predictive capabilities for text input)

(+/-) Consumer information facilitates demographic segmentation based on age, gender, income, address, etc.

(+/-) Consumer information identifies product preferences (e.g., product purchase history with a retailer)

(+/-) Consumer information identifies life events (e.g., relocation, marriage, childbirth) or behaviors (e.g., frequent travel, fitness activities, gaming)

(-) Consumer information relates to sensitive areas where commercial activity is unwelcome (e.g., illnesses, divorce)

(+/-) Product or service provides effective placement for advertisements or sponsored messages (e.g., sponsored results on search engines and shopping sites)</td><td>The social environment is salient when:

(+) Consumer information identifies peer connections (e.g., contact lists, group memberships and affiliations)

(+) Consumer information generates opportunities for interaction with peers (e.g., birthdates, anniversaries, life events)

(-) Consumer information is local or private within the social network (e.g., messages that concern personal or professional relationships with peers)

(-) Consumer information is socially sensitive or relates to divisive topics (e.g., opinions on politics, faith, or lifestyle choices)

(-) Product or service attracts younger audience or polarizing topics (e.g., teenage content, celebrity gossip)

(+/-) Nature of product or service is conducive to peer interactions (e.g., experience goods, media consumption, services with positive network effects)

(+/-) Design of product or service promotes peer interactions (e.g., community features, integration with social platforms)</td></tr>
</table>

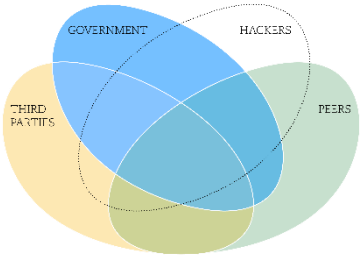
Table 2: Core Privacy Strategies

	Political environment	**Security environment**	**Market environment**	**Social environment**
Positive consumer impact	Improved provision of public services	Safe and protected products and services	Quality of service, personalization, complementary products and services	Positive interactions with peers (family, friends, business contacts, other users)
Negative consumer impact	Public penalties and fines, political profiling, repression	Financial loss, identity theft, reputational damage	Commercial interruptions, sensitive profiling, price discrimination	Disagreements, conflicts of interest, harassment
Core strategy	*Balanced cooperation with Government:* Maximize benefit to public services and minimize targeted action against consumers	*Heightened security against Hackers:* Minimize risk of security breaches and unauthorized access to consumer information	*Limited disclosure to Third parties:* Maximize quality-improving and revenue-generating disclosure, minimize commercial downsides for consumers	*Moderated propagation with Peers:* Maximize consumer engagement on social platforms, minimize negative peer interactions
Tactics to generate positive impact	Cooperate by sharing consumer information relevant to public services, engage with policymakers to promote beneficial applications of consumer information	Strengthen protection of consumer information, monitor information flows to preempt attacks, Implement bounty programs to reward reporting of security vulnerabilities	Disclose consumer information to improve product or service, engage in revenue-generating disclosure (data sharing, advertising, referral programs) where negative consumer impact can be tolerated	Propagate consumer information to promote product or service on social platforms, lead and guide the conversation, comply with social norms and expectations
Tactics to mitigate negative impact	Minimize politically sensitive information, anonymize consumer information, report government access requests	Create emergency response teams, report security breaches, redress consumers in case of breach	Police commercial intrusiveness by third parties, prevent profiling based on sensitive information (e.g. illness), provide consumer control over disclosure (premium tier) or compensate consumers for disclosure (reward programs)	Avoid polarizing topics, moderate consumer participation in the conversation, limit public exposure of consumers
Cost	Lobbying, public policy engagement	Security investments, damage compensation	Lower disclosure revenues, restricted commercial partnerships	Lower marketing effectiveness, cost of moderating activity on social platforms
Strategic constraints	Compliance with legal requirements, coherence across jurisdictions	Reliance on external security infrastructure, delegation of security efforts to consumers	Reliance on third party services, ad-blocking technologies, design of multiple consumer service tiers	Governance of social platforms, viral effects

Table 3: Privacy Landscape Representations

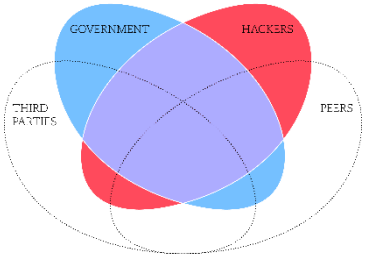
This exhibit represents the privacy landscapes of four different firms. To represent the landscapes, we have assigned a color to each domain: blue for government, red for hackers, yellow for third parties, and green for peers. In each representation, the color intensity reflects the importance of the domain to the particular firm, and cases where the domain has low importance are represented with little or no color. In the outer region of each representation, the weight of each domain can be assessed in isolation; toward the center, the intersections between the colored areas identify the strategy interactions that arise. The larger the number of colored intersections, the higher the complexity of the landscape.[16]

Movistar (Telecommunications)



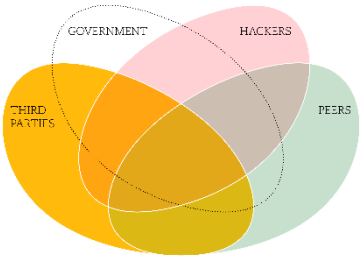
Governments exhibit a high weight for telecommunications operators as they monitor and intervene their networks. Commercial third-parties and peers have medium weight, given initiatives by operators to profile and share subscriber data as well as the social component present in the service.

Barclays (Retail banking)



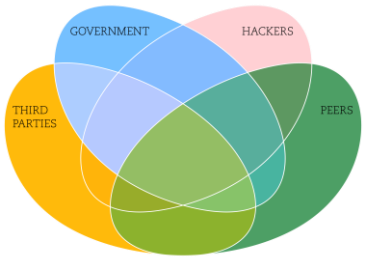
Governments and hackers both command a high weight for banks. Banking activity is monitored by governments and is a prime target for hackers. Third-parties have a low weight because traditional retail banking is subject to regulatory restrictions that limit consumer information sharing.

Amazon (Online retail)



Third-parties exhibit a high weight for online retailers due to the valuable opportunities for consumer profiling and advertising. Hackers and peers have medium weight. Hackers may target retail accounts as they contain billing information and can be used to place orders. Peers are gaining relevance with the social component of online retail.

Facebook (Social platform)



Governments, third-parties and peers command a high weight for social platforms. This is due to valuable opportunities for political advertising, for commercial advertising, and the strong social component of the service. Hackers command medium weight because user accounts are valuable targets to gain access to other linked accounts.

[16] The goal of our representations is to produce a visual map of all intersections between the four domains: this includes domains in isolation, intersections of two domains, three domains, and intersection of all four. In total, 15 distinct areas. This is equivalent to a Venn diagram with four sets. We use an oval or petal shape to represent each domain (rather than, say, a circle) given that symmetric Venn diagrams do not exist for the case of four sets, as shown by Griggs, Killian and Savage (2004).

Table 4: Strategy Interactions

Lead external player	Type of interaction	Example	Negative impact on consumers	Firm's strategy response
Government	*Government control:* Access and monitoring of consumer information by government is facilitated by peers and commercial entities	*WeChat:* Consumers communicate with peers on the messaging service and are subject to government eavesdropping	Consumers face penalties if they are found to breach government policies, peers reluctant to engage on sensitive topics	WeChat scans user conversations and blocks messages relating to topics considered to be sensitive by the Chinese government
Hackers	*Hacker exploitation:* Malicious actors gain access to consumer information through third parties, peers, or government	*BBC News:* Hackers masquerade as advertisers and post malicious ads (malvertising) to install malware on the computers of unsuspecting readers	Consumers are exposed to advertising distractions as well as security breaches due to malicious ads	The BBC supervises the trustworthiness of advertising networks it carries ads from and educates users by reminding them to keep their systems updated
Third parties	*Commercial intrusion:* Commercial activity exploits consumer information to intrude on peer interactions and public sphere	*Facebook:* A third party (Cambridge Analytica) exploits peer connections to harvest consumer information and targets users with political advertising	Consumers discover that peer connections compromise their personal information, face negative interactions with peers due to differences in political preferences	Facebook monitors third party access to consumer information and allows users to restrict it, prescreens political advertisers and discloses the source when displaying political ads.
Peers	*Peer trust:* Peer communities are used by third parties, government, or hackers to access or manipulate consumer information	*Amazon:* Online retailer hosts fake and biased product reviews produced by third parties impersonating shoppers or consumers rewarded to post positive reviews	Consumers find product reviews to be unhelpful, reducing the value of Amazon's shopping community and the peer interactions it generates	Amazon removes reviews that are deemed to be fake or biased, highlights and promotes consumer reviews that correspond to verified purchases, and terminates seller accounts that are found to breach review policies

Acknowledgements
We thank Charles Baden-Fuller for helpful comments and discussion as well as participants at City Unruliversity, the IESE Digital Economy Frontiers Workshop, the Cass Strategy Workshop, Télécom ParisTech, and the SKEMA Business Models Workshop. We also thank Luis Llabrés for his graphics design work.

References

Abelson, H., R. Anderson, S. M. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, M. Green, S. Landau, P. G. Neumann, R. L. Rivest, J. I. Schiller, B. Schneier, M. A. Specter, D. J. Weitzner (2015), "Keys under doormats: mandating insecurity by requiring government access to all data and communications," *Journal of cybersecurity* 1:1 69-79.

Acquisti, A. and H. R. Varian (2005), "Conditioning prices on purchase history," *Marketing Science* 24:3 367-381.

Anderson, R. and T. Moore (2006), "The Economics of Information Security," *Science* 314:5799 610-613.

Angst, C. M., E. S. Block, J. D'Arcy, and K. Kelley (2017), "When Do IT Security Investments Matter? Accounting for the Influence of Institutional Factors in the Context of Healthcare Data Breaches," *MIS Quarterly* 41:3 893-916.

Aversa, P., A. Hervas-Drane, and M. Evenou (2019), "Business model responses to digital piracy," *California Management Review* 61:2 30-58.

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

Casadesus-Masanell, R. and K. Elterman (2019), "Walmart's Omnichannel Strategy: Revolution or Miscalculation?" *Harvard Business School Case 720-370*.

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

DalleMule, L. and T. H. Davenport (2017), "What's Your Data Strategy?" *Harvard Business Review*, May-June 2017 issue.

Godey, B., A. Manthiou, D. Pederzoli, J. Rokka, G. Aiello, R. Donvito, and R. Singh (2016), "Social media marketing efforts of luxury brands: Influence on brand equity and consumer behavior," *Journal of Business Research* 69:12 5833-5841.

Griggs, J., C. E. Killian and C. D. Savage (2004), "Venn Diagrams and Symmetric Chain Decompositions in the Boolean Lattice," *Electronic Journal of Combinatorics* 11:1 R2.

Hagiu, A. (2014), "Strategic Decisions for Multisided Platforms," *MIT Sloan Management Review*, Winter 2014 issue.

Halberstam, Y. and B. Knight (2016), "Homophily, group size, and the diffusion of political information in social networks: Evidence from Twitter," *Journal of Public Economics* 143 73-88.

Hewett, K., W. Rand, R. T. Rust, and H. J. van Heerde (2016), "Brand Buzz in the Echoverse," *Journal of Marketing* 80:3 1-24.

McIntyre, D. P. and A. Srinivasan (2016), "Networks, platforms, and strategy: Emerging views and next steps," *Strategic Management Journal* 38:1 141–160.

Montes, R., W. Sand-Zantman, and T. Valletti (2019), "The Value of Personal Information in Online Markets with Endogenous Privacy," *Management Science* 65:3 955-1453.

Pfeffer, J., T. Zorbach, and K. M. Carley (2014), "Understanding online firestorms: Negative word-of-mouth dynamics in social media networks," *Journal of Marketing Communications* 20:1-2 117-128.

Roberds, W. and S. L. Schreft (2009), "Data breaches and identity theft," *Journal of Monetary Economics* 56:7 918-929.

Shy, O. and R. Stenbacka (2015), "Customer Privacy and Competition," *Journal of Economics and Management Strategy* 25:3 539-562.

Spiekermann, S., A. Acquisti, R. Böhme, and K.-L. Hui (2015), "The challenges of personal data markets and privacy," *Electronic Markets* 25:2 161–167.

Taylor, C. R. (2004), "Consumer privacy and the market for customer information," *RAND Journal of Economics* 35:4 631-650.

Toubia, O. and A. T. Stephen (2013), "Intrinsic vs. image-related utility in social media: Why do people contribute content to Twitter?" *Marketing Science* 32:3 368–392.

Tucker, C. E. (2014), "Social Networks, Personalized Advertising, and Privacy Controls," *Journal of Marketing Research* 51:5 546-562.

Upton, D. M. and S. Creese (2014), "The Danger from Within," *Harvard Business Review*, September 2014 issue.

Villas-Boas, J. M. (2004), "Price cycles in markets with customer recognition," *RAND Journal of Economics* 35:3 486-501.