Strategies for Seizing the Privacy Landscape

Ramon Casadesus-Masanell
Harvard Business School

Andres Hervas-Drane
Cass Business School

December 19, 2017

Introduction

Managing consumer information in the digital age has become an important strategic consideration for firms and is fueling discussions in boardrooms across a wide array of industries. The decreasing cost of storing, processing, and transmitting data has led firms to accumulate an ever greater stock of consumer personal information. Exploiting this information enables firms to provide better products and services, for example by personalizing product design and service delivery to cater to individual preferences. These forms of information exploitation have become an important driver of value creation, benefitting consumers and reinforcing their willingness to provide personal information in the market.

Some forms of information exploitation, however, have a negative impact on consumers. The exploitation of personal information for purposes different from those anticipated by consumers when providing their information, or for which consumers have not provided explicit consent, can generate consumer harm. These forms of exploitation trigger privacy concerns and reduce consumers' willingness to provide personal information to the firm. Recent research confirms the chilling effect of privacy concerns. 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." [1] Thus, the firm's challenge when managing consumer privacy is to minimize this negative impact on its products and services.

However, managing consumer privacy can be difficult. Consider, for example, the Beacon advertising program launched by Facebook in November 2007. Beacon was a feature that shared information about users' activities on third-party sites with their friends via their

[1] See "Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities," NTIA blog, U.S. Department of Commerce, May 13, 2016. Similar effects for consumer search activity based on revelations of government surveillance are reported by Marthews and Tucker (2015).

Facebook news feeds. A wide range of user activities were tracked and reported, including making purchases, posting items for sale, achieving high scores in online games, saving recipes, and watching videos. The goal of the program was to foster user interactions and create new advertising opportunities around these activities.

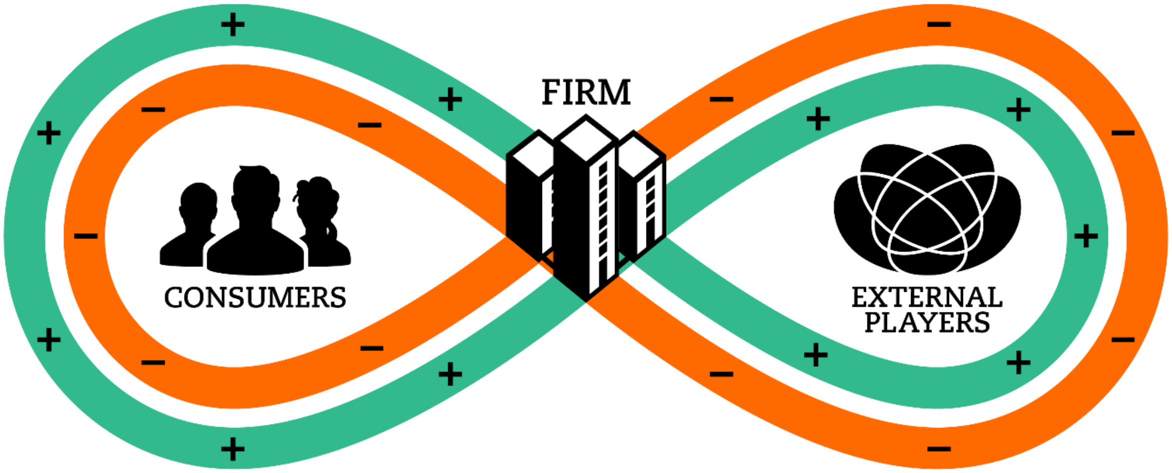
Facebook users were automatically enrolled in the Beacon program, and many found that it disclosed information they would rather not share. One young woman, a Harry Potter fan, was notified through Beacon that her sister had purchased a Harry Potter trivia game, which ruined the surprise of her Christmas gift. In another instance, a college student was dismayed when both of the women he was dating showed up at the movie theater for a date that was intended for only one of them, each having seen a notification about the ticket purchase and show time on her news feed.[2] Users also found the notifications associated with Beacon to be insufficient. The settings were difficult to find and to navigate, and opting out of the program was perceived to be a complex task.

An anti-Beacon petition quickly gained 50,000 signatures, and Facebook soon switched from an “opt-out” system for the service to an “opt-in” system in which users had to explicitly approve the release of information to their news feeds.[3] However, user concerns persisted, prompting Facebook to withdraw the program only a month after its launch. In 2008, a class action lawsuit was filed against Facebook and other participating companies, and in 2009, Facebook officially shut down the defunct initiative as part of a settlement for the case.

As this example illustrates, consumer privacy requires a difficult balancing act even for industry leaders. Privacy is a complex problem because there is an array of external players to the firm – including advertisers and peers on social networks – that can impact consumers through the firm’s product or service. While these players can have a positive impact on consumers, and this is the rationale for their participation, under some circumstances they can generate a negative impact. The following figure illustrates the argument:

[2] See “Facebook Retreats on Online Tracking,” New York Times, Nov. 30, 2007. See also “Facebook’s Beacon of Despair,” Huffington Post blog, Nov. 30, 2007.

[3] See “The Evolution of Facebook’s Beacon," Bits blog, New York Times, Nov. 29, 2007.



The firm acts as a personal information gateway between consumers (on the left) and external players (on the right). When the exploitation of personal information is aligned with consumer expectations and generates positive impact (the green value flow), this reinforces the provision of information by consumers and increases the value of the firm's product or service. When exploitation diverges from consumer expectations and generates consumer harm, there is negative impact (the red value flow), which reduces consumers' willingness to provide personal information and use the firm's product or service. Privacy concerns therefore result in less value creation and inferior value capture and profit for the firm.

In this article, we develop the *privacy landscape* framework to help you identify the sources of negative impact (the red flow above) and strategies to minimize it. The privacy landscape consists of those entities external to the firm that may access consumer personal information through the firm. These external players operate outside the boundaries of the firm but not outside the firm's scope of influence. The firm must identify the sources of potential consumer disutility that stem from exploitation of personal information by these players. It must adopt strategic choices that shape the privacy landscape in ways beneficial to consumers, mitigating consumer privacy concerns and increasing value creation and value capture. In short, our goal is to produce a tool that will increase your awareness of privacy threats and help you identify challenges and plan your responses.

The privacy landscape is most relevant to firms competing in industries with information-intensive products or services. Firms in these industries recognize consumer information as an essential input and tend to hold large stocks of personal information. Such industries include social networking (Facebook, Twitter); telecommunications (Telefonica, Verizon); e-commerce (Amazon, eBay); online media (Netflix, Spotify); insurance (AXA, Prudential); banking (Bank of America, Santander); and the internet of things (Ecobee, Nest). In these industries, a superior response to the privacy landscape (superior privacy management) can lead to a privacy-based competitive advantage.

The managerial and economics literature has recently begun to examine the impact of consumer privacy on the firm. Early contributions explored the marketplace implications of personal information being used for price discrimination.[4] More recent contributions have considered the implications for multisided platforms and competition.[5] A related and growing body of literature analyzes the impact of privacy on advertising, though the focus is mainly on the efficiency of the advertising mechanism. Few contributions, in contrast, have explored the strategic implications for the firm in the context of social networking,[6] or the strategic implications of consumer privacy in the security or political contexts. Moreover, the literature has largely considered these aspects of consumer privacy in isolation. We are not aware of previous work that has explored the interdependencies that arise among them.

We proceed by reviewing how the exploitation of personal information by external players in the privacy landscape impacts consumers. In each case, we identify a *core strategy* that addresses the tradeoffs present and enables the firm to mitigate negative consumer impact. We consider four domains or sets of players: the government (i.e., the political environment); hackers (i.e., the security environment); third parties the firm interacts with in the marketplace (i.e., the market environment); and the peer networks of consumers (i.e., the social environment). Sidebar 1 represents the privacy landscape, and Sidebar 2 summarizes factors contributing to negative impact in each domain. We also discuss *strategy interdependencies* that can be identified by the framework and that must be addressed for effective privacy management. Sidebar 3 provides examples for firms in different industries, and Sidebar 4 provides graphical representations for the interdependencies in these examples.

About the Research

This article is based on the authors' broader research agenda regarding privacy and business models for technology-intensive firms. Our work spans several papers that use economic modeling to analyze the fundamental trade-offs firms face in this area (including, for instance, consumer provision of personal information, revenue source multiplicity, advertising model choices, and consumer feedback-based pricing). Our work also spans several case studies based on in-depth analysis of the strategies deployed by leading firms in the sector (Amazon, eBay, Apple, Uber). We build on this earlier work to develop a framework that reconciles the various trade-offs generated by consumer privacy with the rich set of strategies adopted by firms in the industry. Our goal is to provide a comprehensive tool to assist with strategic decision-making in the realm of consumer privacy.

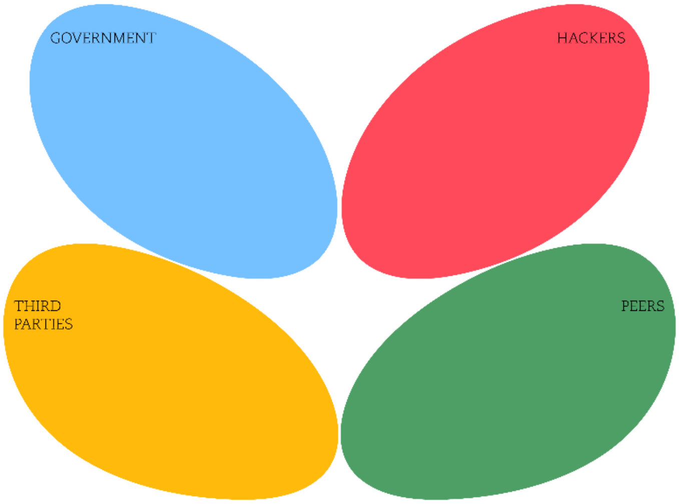
[4] Villas-Boas (2004), Taylor (2004), and Acquisti and Varian (2005) provide early contributions in this area. Price discrimination results in some consumers being charged higher prices, so these consumers have little incentive to provide personal information, as this facilitates discrimination by the firm.

[5] Recent contributions include Casadesus-Masanell and Hervas-Drane (2015), which analyzes how firms compete when exploiting consumer privacy as a source of differentiation; and Campbell, Goldfarb, and Tucker (2015); as well as Shy and Stenbacka (2015); which analyze the impact of different privacy-related regulatory regimes on competition.

[6] A notable exception is Tucker (2014), which analyzes the effectiveness of ads both targeted and tailored with personal information in a social network.

Sidebar 1: The Privacy Landscape Framework

The privacy landscape is composed of the political, security, market, and social environments. The set of players or entities operating in these domains, which can access consumer personal information through the firm, includes the government, hackers, third parties, and peers. The four domains or environments are depicted below as distinct areas, which will be useful for visualizing the relevant strategy interdependencies that arise between them. In Sidebar 2 we provide guidance on how to assess the weight of each domain in your industry depending on the potential for negative consumer impact. We provide specific industry examples in Sidebar 3, and depict the interdependencies using the representation below in Sidebar 4. In this article, we focus on mitigating negative consumer impact to inform the privacy strategy of the firm. However, it is important to acknowledge that information exploitation by external players can also be beneficial to consumers, so a firm aiming to maximize the value of its product or service must take advantage of positive elements, in addition to pinpointing and mitigating the sources of negative impact.



The Political Environment

The government plays an important role in the privacy landscape because it can access consumer information and mandate data collection and retention policies. The relationship between the government and the firm can vary significantly across jurisdictions, and is affected by both the market power of the firm and the nature of the consumer information it accumulates. Government can have a positive impact by improving the provision of public services. It can exploit consumer information to improve national security, taxation, public health, and essential infrastructure.

Government can also have a negative impact on individuals by exploiting consumer information. This negative impact tends to arise from targeted actions such as audits, fines, or the assignment of public duties. While there are public benefits associated with these forms of exploitation, affected consumers perceive the impact to be negative (i.e., there is a commons problem).[7] Governments can also misuse consumer information. Extensive monitoring can limit free speech and individual freedoms, or be used to fine-tune propaganda campaigns and orchestrate political manipulation.

To illustrate negative impact by government, consider the disability fraud investigation pursued by the Manhattan District Attorney in 2013. As part of the investigation, the D.A. served Facebook with 381 warrants seeking photos, private messages, and other personal information from 134 user profiles. The Facebook data provided evidence of employees who claimed to be physically disabled performing a variety of activities such as fishing, martial arts, and even jet skiing. Access to this information no doubt helped public authorities monitor disability benefits and deter fraud. But the findings and the subsequent reporting in the media likely had a chilling effect on consumers, many of whom feared the future unintended consequences of sharing their activity on social media.

Cooperation is a core strategy for dealing with government. The firm should pursue constructive engagement with political authorities and policy makers to minimize government access to personal consumer information. This can be achieved by complying with the requirements of the political environment only to the full extent of the applicable laws, highlighting consumer privacy concerns in the public engagement agenda, and investing resources to ensure the firm’s presence and participation in the public sphere. Effective cooperation minimizes negative consumer impact but is costly for the firm.

The firm should carefully weigh requests for consumer information that exceed the requirements of applicable laws. When compliance is too costly for the firm in terms of consumer privacy – for instance, when it would burden the firm’s reputation and impact other products or jurisdictions –

[7] In some cases the firm may benefit from targeted action by the government. For example, firms supplying digital content can benefit from fines that render online piracy more costly for consumers. See Casadesus-Masanell, Hervas-Drane, and Mitchell (2006), as well as Casadesus-Masanell and Hervas-Drane (2010).

it may be preferable to withdraw cooperation and cancel (or choose not to launch) the product or service in question.

The best way to implement cooperation is to sustain a constructive dialog with policy makers. Such a dialogue facilitates compliance by reducing communication errors, and generates an opportunity for the firm to provide input and shape new policy initiatives. In addition, it helps to mitigate lack of visibility in government-mandated processes affecting the personal information of consumers.

A famous instance of the cooperation strategy and the tensions it can generate was the encryption dispute between FBI and Apple following a mass shooting in San Bernardino in 2015. Apple was issued a court order to assist U.S. authorities in unlocking an iPhone recovered from one of the shooters. The technology required to do so, which did not yet exist, would provide access to the shooter's personal information. Apple had the technical capacity to fulfil the request, but also realized that this could undermine privacy protections in Apple's future devices and compromise consumer trust in their products. Apple publicly challenged the order, defending the privacy afforded by its products and noting that there was no precedent of compliance with a request of this nature.

The Security Environment

Hackers are entities that pursue unauthorized access to consumer information through the firm. Data thieves and organized criminals are driven by the goal of financial gain, but employees and subcontractors, as well as state-sponsored organizations pursuing unauthorized access, also operate as hackers.[8] Hacking activity generates few benefits for consumers, if any. In some exceptional cases, whistleblowers can expose wrongdoing through unauthorized access or unauthorized publication of information. More generally, the negative impact of hackers on consumers includes financial losses, costs associated with identity theft, and reputational costs.

The security breach of AdultFriendFinder.com provides an example of the damaging impact of hacking on consumers. The site was a casual dating service founded in 1996, and its database, when breached in 2015, held information corresponding to accounts created over a period of almost twenty years. The hackers published on the Internet the personal information of three and a half million past and present users of the site, including email addresses, ages, zip codes, sexual orientations, and other sensitive personal details.

Cybersecurity is a core strategy for dealing with hackers. The firm should secure its information systems to minimize unauthorized access to consumer information. The firm can moderate external threats by monitoring information flows and security events, identifying and raising awareness about security vulnerabilities, and strengthening security response teams. Internal threats can be moderated by adopting policies to control access and sharing of consumer information within the organization, running checks on new and departing employees, and raising physical security. Effective cybersecurity minimizes negative consumer impact but is costly for the firm.

Consumers operate outside the firm’s boundaries but within the cybersecurity perimeter. The communication channels used by consumers to access the firm’s information systems can also be targeted by hackers. The firm can discipline consumer practices by establishing client-side hardware and software requirements for using the service, requiring the use of secure communication channels, and strengthening authentication processes with stronger passwords, limited failed login attempts, and multi-factor authentication.

Cybersecurity creates a moral hazard problem because it relies on the efforts of the firm as well as those of consumers. On the one hand, this implies that a firm should signal its cybersecurity commitment to consumers, for example by building a security track record and investing in bounty programs or incentive schemes that reward the reporting of security risks. Such programs help to minimize security breaches and to make a firm’s security performance more visible. On the other hand, the firm must carefully weigh the amount of effort it demands of consumers and consider how the costs generated by security breaches are shared between the

[8] PwC’s 2014 report “US cybercrime: Rising risks, reduced readiness” discusses the nature and impact of external cyber threats across different sectors. Upton and Creese (2014) review the cybersecurity threats originating within organizations.

firm and consumers. Requiring too much effort or increasing exposure to security risks can turn consumers away.

The cybersecurity strategy is exemplified by Tresorit. A late entrant to the cloud storage market for businesses and professionals, Tresorit claims that its service offers industry-leading security. The service is presented as ideal for “business owners to avoid data breaches” and “teams who want to protect confidential data.” Security is critical for cloud storage, given that prospective customers use the service to store and protect valuable information. But given the technical complexity of the service, it is difficult for prospective customers to evaluate the claims. So in 2013, in order to prove its security credentials, Tresorit set up a hacking contest with a $50,000 bounty and invited the hacking community, as well as security researchers from institutions like MIT and Stanford, to find a breach in its system. Almost 500 days later, the prize remained unclaimed.

The Market Environment

Third parties are commercial partners to which the firm may disclose consumer information, such as data brokers, advertisers, and subcontractors. Third parties generate positive impact by offering consumers valuable transaction opportunities and complementary services. But they also have a negative impact. Unsolicited offers impose attention costs on consumers, who may prefer not to be exposed to commercial interruptions. In addition, targeted communications based on personal information may disturb consumers by tapping into sensitive topics or circumstances, such as health conditions or a recent divorce. Third parties can also exploit personal information to engage in price discrimination, which results in some consumers being charged higher prices.[9]

The negative impact that Internet advertising can generate is evidenced by the large number of consumers who install (and in some cases purchase) ad-blocking software to avoid it. This software can block most of the advertisements on popular websites, though it sometimes precludes some websites from operating correctly. According to reporting by the *Financial Times* and *The Wall Street Journal*, about 200 million consumers worldwide use ad-blocking extensions. The percentage of online ads blocked in most countries ranges from 10% to 30%. As spending for online advertising continues to increase, it appears that a growing share of consumers are choosing to opt out.

Disclosure is a core strategy for dealing with third parties. The firm should weigh the profitability of disclosing consumer information to third parties against the negative consumer impact it generates. Disclosing consumer information generates additional revenue streams in the marketplace, but consumers are better off when disclosure is minimized and constrained to the provision requirements of the firm’s product or service. Eliminating negative consumer impact therefore requires the firm to forego disclosure revenues. The firm can resolve this tradeoff by adjusting the level of disclosure and compensating consumers accordingly.

One option is to compensate (or subsidize) consumers for the disclosure of their information. In this case, the firm engages in disclosure but shares the revenues it generates with consumers. Another option is to minimize disclosure of consumer information or eliminate it altogether. By foregoing disclosure of consumer information, the firm renders the service more valuable for consumers and can charge them a higher price. Alternatively, the firm may choose to implement different service tiers and offer consumers a choice. A free or subsidized tier would be subject to disclosure (through third-party advertising, for instance), while a paid tier would preclude any disclosure to third parties.

Microsoft’s Bing search engine provides a good example of how the disclosure strategy can be implemented. Bing operates a rewards program in the United States, and consumers earn

[9] Consumers are generally uncomfortable with price discrimination practices that set prices based on consumer identity, as seen with the Amazon.com backlash in 2000 that led the firm to announce it would not set prices on its website based on customer demographics.

rewards by performing searches on Bing. When using Bing, consumers provide Microsoft with personal information (their search activity and browsing patterns, which identify their interests) and become exposed to third-party advertising. Microsoft displays ads on the Bing search engine webpage as well as on external sites enrolled in the Bing advertising program. The advertising generates revenues for Microsoft but can have a negative impact on consumers. Microsoft helps alleviate this negative impact by sharing the advertising revenues with consumers, offering store gift cards and online service vouchers through the rewards program.

The Social Environment

Peers include family members, friends, business contacts, and acquaintances with whom consumers interact. Interactions with peers on topics of mutual interest are valuable for consumers and generate positive impact. Consumers invest in these interactions by building their online profiles, sharing information about their experiences, and responding to the experiences of others. Peer interactions are relevant to the firm when the firm provides the communications channel through which they take place (e.g., Facebook and Twitter), or when it participates in the exchange (e.g., runs a social media campaign).[10]

Peers can also have a negative impact. Peers may become the unintended recipients of personal information, generating conflicts of interest. They may also engage in negative social interactions due to opposing views on divisive topics such as politics, ideology, or faith. In addition, peers may engage in cascading negative feedback (i.e., harassment or cyberbullying) facilitated by the accessibility and scale of the online social environment.

The negative impact that peers can generate is illustrated by the self-restraint reported by a large number of social media users. A 2014 report by the Pew Research Center found that 86% of Americans were willing to have an in-person conversation about a divisive topic, but only 42% of Facebook and Twitter users were willing to post about it. Respondents appeared to anticipate that broadcasting their opinions on social media could expose them to disagreements or backlash from their extended peer network.

Diffusion is a core strategy for dealing with peers. The firm should weigh the profitability of diffusing consumer information among peers against the negative consumer impact it generates. A high level of diffusion can be profitable for the firm because it fosters consumer interactions on the highlighted topic and engagement with the product or service. But diffusion is not desirable for consumers if it broadcasts their opinions outside their comfort zone, reaches undesired recipients, or exposes them to negative cascading feedback. Minimizing negative consumer impact therefore requires the firm to moderate diffusion and forego the revenues it generates. The firm can resolve this tradeoff by adjusting the level of diffusion to account for consumer preferences and social norms.

The firm can moderate diffusion by carefully selecting the topics it promotes and by adopting broadcasting practices that limit public exposure. Promoted topics should preferably be non-polarizing, and broadcasting should operate with consumer awareness and consent for the diffusion of their information. The firm can delegate control to consumers by providing them with tools to manage recipients, monitor diffusion, and remove their content when desired. Similarly, the firm may offer consumers the option to control their exposure to specific topics and to the activity of their peers.

[10] Note that peer interactions can also take place on platforms other than social networks, such as discussion forums and product review sections. In fact, retailers have strong incentives to foster these interactions; see Hervas-Drane (2015).

Pepsi’s “Max It Now” social media campaign exemplifies the diffusion strategy. The campaign involved a series of twenty-four challenges, with prizes awarded to fans who tweeted about why they preferred Pepsi Max to Coke Zero, posted photos of themselves with a Pepsi Max, or uploaded their own video commercials for the product. By carefully designing the challenges so that the activity of participants was fun, positive, and well-received by their peers, Pepsi attempted to promote its brand while minimizing the risk of negative impact. The campaign generated 16,000 social media posts promoting Pepsi Max, which were collected by Pepsi on a campaign website.

Sidebar 2: Mapping Your Privacy Landscape

To map the privacy landscape in which you operate, you must assess the weight of each of the four domains. A given domain will carry a larger weight if there is a stronger potential for negative consumer impact. In general, weights vary across industries and firms. In this sidebar, we identify factors that contribute to the weight of the political, security, market, and social environments. In Sidebar 3 below, we illustrate these with specific examples. Having mapped your privacy landscape, you must identify strategies with which to minimize consumer privacy threats. To guide you in this process, we catalog core strategies in the sections analyzing the four domains.

The political environment is particularly salient when:

- Consumer information may be exploited by public authorities for the purpose of targeted interventions (e.g., financial transactions that may be reviewed for taxation purposes)
- Consumer information may facilitate segmentation by political or ideological affinity (e.g., political discussion threads in forums or social media networks)
- Products or services provide effective channels to monitor the communications of individuals and reach them in a targeted fashion (e.g., mobile telephone providers)
- The firm has 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.

The security environment is particularly salient when:

- Consumer information has financial value for hackers (e.g., credit card and billing information)
- Consumer information reveals physical location or travel plans that could allow hackers to steal from customers (e.g., calendar information)
- Consumer information has reputational or intelligence value for hackers (e.g., allows them to shame the targets)
- 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)
- The firm has large market share or a market leadership position. Large firms provide access to larger stocks of personal information.

The market environment is particularly salient when:

- Consumer information facilitates demographic segmentation based on age, genre, income, zip code, etc.
- Consumer information identifies product purchases and product preferences (e.g., activity history on an online retailer)
- Consumer information identifies life events (e.g., moving homes, marriage, childbirth) or behaviors (e.g., frequent travel, fitness activities, gaming)
- Consumer information is of a sensitive nature (e.g., health history that could be exploited by advertisers to target particular illnesses)
- Product or service provides effective placement for advertisements or sponsored messages (e.g., sponsored recommendations in media center homepages)

The social environment is particularly salient when:

- Consumer information is of local scope or of a private nature within the peer 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 that would not be shared with the broader peer network)
- Peer network can be effectively exploited to promote product or service (e.g., experience goods, services with positive network effects)
- Product or service fosters peer interactions due its nature and design (e.g., media consumption, implementation of community features)
- Product or service attracts younger or more polarized audience (e.g., teenage content, fashion content)

Sidebar 3: Industry Examples

We present examples of a number of privacy landscapes to illustrate how the strength of each domain can vary broadly across industries. The implication is that the right strategy for seizing the landscape is industry-dependent: one size does *not* fit all.

Telecommunications: Vodafone

- Political: High. Telephone networks are subject to government monitoring and intervention.
- Security: Low. Telephone accounts are generally of limited value to hackers.
- Market: Medium. Telephone operators are expanding their services to profile and advertise to their subscribers.
- Social: Medium. The service contains a social component, but engagement of telephone operators in social activity is limited.

Banking: Barclays

- Political: High. Banking activity is monitored by the government.
- Security: High. Bank accounts and methods of payment are a prime target for hackers.
- Market: Low. Retail banking is subject to regulatory restrictions that limit the sharing of consumer information.
- Social: Low. Traditional retail banking lacks a social component.

Online Retail: Amazon

- Political: Low. Retail activity is generally of little interest to government.
- Security: Medium. Retail accounts contain billing information and could be used to place orders.
- Market: High. Retail accounts are a valuable source of consumer profiling and online retailers offer advertising channels to reach their customers.
- Social: Medium. Growing social component but of a limited sensitive or divisive nature.

Social Networking: Facebook

- Political: Medium. Social networking activity is a target of government monitoring.
- Security: Medium. Social networking accounts could be used by hackers to gain access to other services.
- Market: High. Social networking accounts are a valuable source of consumer profiling and social networks offer advertising channels to reach their customers.
- Social: High. The social component is essential to the service and carries associated risks.

Strategy Interdependencies

The four core strategies described above are effective and straightforward when there are no interdependencies among them. However, in a typical real-world situation, the firm must take the interdependencies present in its privacy landscape into account. These arise when the interactions between the strategies implemented by the firm across different domains generate negative consumer impact. This can happen because strategies designed to address one domain of the landscape simultaneously worsen the firm's performance in another domain.

The number of possible interdependencies is given by all combinations of the four domains. In general, the firm will not need to account for all possible interdependencies. When the weight of one or more domains is low, some interdependencies will not be relevant to the firm. Similarly, when the weight of some domains is very high, the firm will want to focus attention on the interdependencies that arise there. Sidebars 3 and 4 illustrate this by providing industry examples and depicting the privacy landscapes and relevant interdependencies.

Interdependencies that involve three and four domains can be broken into two-domain pairs. It is often easier to analyze interdependencies by evaluating these pairs separately, rather than by attempting to resolve all tensions simultaneously. Consider the case of Facebook in Sidebars 3 and 4. All four domains have medium to high weight, and therefore the firm faces a complex privacy landscape. This should not be surprising, given that consumer privacy on Facebook is often featured prominently in the media. In particular, third parties and peers exhibit a high weight in Facebook's privacy landscape. The interdependency between these two domains was precisely at play in Facebook's Beacon program, discussed in the introduction.

Facebook implemented an aggressive disclosure strategy with Beacon. The program tracked and reported a wide variety of user activities. This provided a rich stream of information for advertisers to exploit, and the program launched with forty-five partner companies including large players such as Blockbuster, Live Nation, the NBA, and TripAdvisor. But Beacon compromised Facebook's diffusion strategy, since it was rolled out without prior user opt-in and resulted in many users unexpectedly finding their activity published for their friends and contacts to view.

In retrospect, Facebook failed to anticipate the negative impact of Beacon on its users. The interdependency between third parties and peers implies that the firm should reconcile initiatives to raise disclosure revenues with social diffusion activity among peers. While Facebook probably evaluated the benefits of Beacon for its advertising partners, it failed to anticipate the negative impact of diffusing user activity. Initially, Facebook responded to user complaints moderating its diffusion strategy by delegating more control to users, but the backlash triggered by the service eventually forced Facebook to shut it down. If this interdependency had been evaluated more carefully in the design of the program, perhaps a balance that was acceptable to users could have been found prior to large scale deployment.

Google's AdWords program provides an example of how interdependencies can be resolved, in this case to reconcile government with third parties. The AdWords program allows advertisers to reach consumers on the Google Search Network, where ads are featured in connection with a particular set of search results. These search results might appear on specific Google sites like Maps, Shopping, and YouTube, as well as non-Google partner websites. For example, if a company ran a face-painting service for kids' parties, it could choose to target ads to people who searched for the term "children face painting," in which case the ad would appear in response to that search.

Google requires advertisers to comply with local laws around the world. For instance, political content including the promotion of political candidates or parties is prohibited in several countries including Japan, Brazil, and South Korea. In addition, Google imposes its own restrictions on advertisers across the globe. For instance, it forbids the advertisement of dangerous products or services, including recreational drugs, weapons, ammunition, explosives, and tobacco products. Advertisers are not allowed to target audiences based on sensitive information, such as health information or religious beliefs. In addition, advertisers are banned from promoting "any dangerous or derogatory content," including "content that incites hatred against, promotes discrimination of, or disparages an individual or group."

By imposing and policing these overarching rules, Google is excluding content from its advertising network and sacrificing advertising revenues. In doing so, however, Google also circumvents potential conflicts of interest with government and avoids profiling its users on sensitive topics to deliver advertising. Google is in effect moderating its disclosure strategy to reconcile it with its government cooperation strategy.

The Chinese app WeChat provides an example of how to resolve interdependencies between government and peers. WeChat was launched by Tencent in 2011 and is the dominant messaging app in China, with 889 million monthly average users in 2017. WeChat scans user messages and blocks those that relate to topics considered to be sensitive by the Chinese government. This includes content that might incite public protest or reflect poorly on Chinese political leadership.

WeChat messages are blocked based on a series of blacklisted keywords, or certain combinations of words. For instance, The Citizen Lab studied the censorship of keywords related to the death of Liu Xiaobo, a Chinese Nobel Peace Prize winner and political prisoner. The group found that messages containing Xiaobo's name in either English or Chinese, as well as popular images of him, were blocked by the service in one-to-one and group chats.[11] Initially, WeChat users were informed when their messages had been blocked, but by November 2016

[11] See Masashi Crete-Nishihata, Jeffrey Knockel, Blake Miller, Jason Q. Ng, Lotus Ruan, Lokman Tsui, and Ruohan Xiong, "Remembering Liu Xiaobo: Analyzing censorship of the death of Liu Xiaobo on WeChat and Weibo," The Citizen Lab, July 16, 2017.

they no longer received any notification when messages were not sent. Instead, the message simply failed to appear on the other end.[12]

By limiting the freedom of expression of its users and the scope of topics available, WeChat is reducing the functionality of its service. However, this is aligned with government policy and is consistent with social norms in China, and has the effect of reducing the threat of surveillance and negative impact for its users. WeChat therefore reconciles government cooperation with social diffusion by prioritizing the former and moderating the latter.

The general challenge when resolving interdependencies is to shape and implement core strategies in a way that resolves the underlying tensions. This implies that the firm must prioritize among the affected domains with the goal of minimizing the overall negative impact on consumers, frequently by strengthening one strategy over the others. In some domains this involves foregoing potential revenues (e.g., by limiting advertising or social media diffusion), and in other domains it involves incurring higher costs (e.g., to cooperate with government or strengthen cybersecurity).

The complexity of the privacy landscape stems from the fact that there are multiple potential interdependencies and no single solution; rather, firms adopt different solutions in the marketplace depending on the nature of their product or service and the industry and social norms under which they operate. In the preceding examples, we have illustrated the tensions by considering interdependencies between two domains. Resolving interdependencies that involve three or four domains can be very challenging. In the most complex cases, a redesign of the core product or service to reduce the weight of some domains may be the only way to alleviate negative privacy impact on consumers.[13]

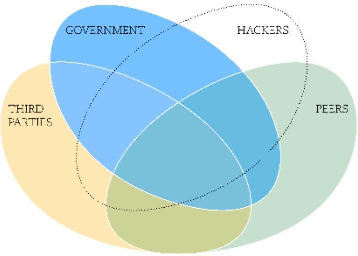
[12] See Lotus Ruan, Jeffrey Knockel, Jason Q. Ng, and Masashi Crete-Nishihata, "One App, Two Systems: How WeChat uses one censorship policy in China and another internationally," The Citizen Lab, Nov. 30, 2016.

[13] The firm could reduce its own access to consumer information, for example, by adopting the role of a custodian. This can be achieved by storing consumer information in encrypted form only and delegating encryption keys to consumers. Many cloud computing providers have adopted this model. This solution compromises the firm's ability to exploit consumer information for the purpose of improving the product or service or tapping into disclosure and diffusion revenues, but also precludes most sources of negative privacy impact.

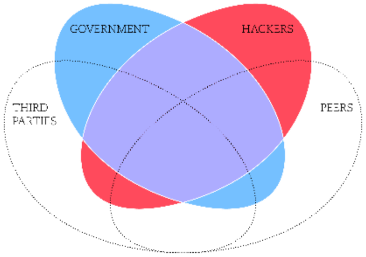
Sidebar 4: Privacy Landscape Representations

We provide examples of privacy landscape representations by revisiting Sidebar 3. Color intensity reflects the importance of the corresponding domain to the particular example, and domains with low weight are left blank. In the outer region of each representation, the weight of each domain can be assessed in isolation. Closer to the center, the intersections between the colored areas identify the strategy interdependencies that arise. These interdependencies are dissimilar across examples. The larger the number of intersections present, the higher the complexity of the privacy landscape. Because the landscapes differ across examples, the key strategies for seizing the landscape also differ. This implies that managers in different industries must consider and deal with different sets of strategy interdependencies.

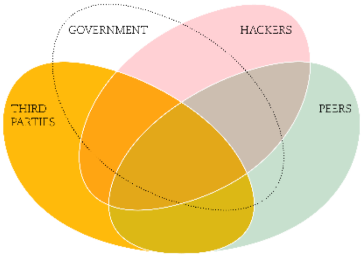
Vodafone Privacy Landscape



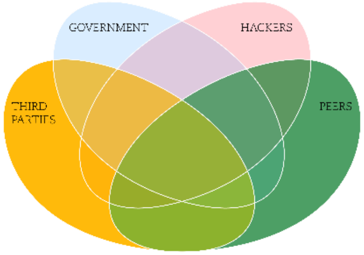
Barclays Privacy Landscape



Amazon Privacy Landscape



Facebook Privacy Landscape



Concluding Remarks

Consumer privacy presents a complex strategic problem. Firms accumulating and exploiting personal information need to manage privacy, and the framework presented in this paper provides a roadmap. The first step is to map your privacy landscape by evaluating the political, security, market, and social environments in which your firm operates. The second step is to adapt your public engagement initiatives, security practices, monetization channels, and social media policies accordingly. The third step is to identify and address the interdependencies that arise between these strategies in order to minimize negative consumer impact.

The privacy landscape is dynamic and will continue to evolve with technology, regulation, and social norms. For example, the advent of wearable devices and ubiquitous sensors (the Internet of Things) could soon configure a new domain within the landscape, leading to new information exploitation opportunities and consumer privacy concerns. If you seize your privacy landscape and react to these changes as they unfold – by identifying new interdependencies and mitigating sources of negative consumer impact – you will champion consumer privacy and profit from greater provision of personal information and increased customer willingness to pay for your products and services.

References

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

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 (2010), “Peer-to-Peer File Sharing and the Market for Digital Information Goods,” Journal of Economics and Management Strategy 19:2 333-373

Casadesus-Masanell, R. and A. Hervas-Drane (2015), “Competing with Privacy,” Management Science 61:1 229-246

Casadesus-Masanell, R., A. Hervas-Drane, and J. Mitchell (2006), “Peer-to-Peer File Sharing and the Market for Digital Information Goods,” Harvard Business School case 706-479, January 2006 (revised March 2010)

Casadesus-Masanell, R. and N. G. Karvounis (2011), “HUGE and Digital Strategy,” Harvard Business School Case 712-442, October 2011 (revised January 2012)

Casadesus-Masanell, R., I. Mackenzie, and D. Dadiomov (2015), “Uber and the Taxi Industry (A),” Harvard Business School Case 715-433, March 2015

Casadesus-Masanell, R., I. Mackenzie, and D. Dadiomov (2015), “UberX & Lyft (B),” Harvard Business School Supplement 715-434, March 2015 (revised October 2015)

Casadesus-Masanell, R. and A. Thaker (2013), “eBay, Inc. and Amazon.com (B),” Harvard

Business School Supplement 712-406, April 2012 (revised October 2013)

Hervas-Drane, A. (2015), “Recommended for you: The effect of word of mouth on sales concentration,” International Journal of Research in Marketing 32:2 207–218

Marthews A. and C. Tucker (2015), “Government Surveillance and Internet Search Behavior,” Working Paper

Shy, O. and R. Stenbacka (2015), “Customer Privacy and Competition,” Journal of Economics and Management Strategy, forthcoming

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

Tucker, C. (2016), “Social Advertising: How Advertising that Explicitly Promotes Social Influence Can Backfire,” Working Paper.

Upton, D. M. and S. Creese (2014), “The Danger from Within,” Harvard Business Review

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