Chapter 2
The Role of Corporate Actors: The Dilemma of Privacy Monetization

The current transformations bring with them a wealth of potential informational gains from more intense use of detailed personal data, but also numerous uncertainties. Key areas where data on individuals are crucial to corporate success—and privacy concerns are bound to emerge—are the relationships of an organization with its stakeholders: in particular, customers and employees.

2.1 Privacy in the Relationship of an Organization with its Customers

Online advertising is an area in which personal data have become increasingly important over time. It has been one of the fastest-growing businesses in the last ten years, after a slower start in the mid-nineties: in the United States, Internet advertising revenues surpassed the cap of $10 billion in 2012; comparatively, they exceeded those of cable television in 2011, and narrowed their gap to broadcast television (traditionally the largest share in the market) in 2012 (Internet Advertising Bureau 2013). The success of Internet-based advertising is largely due to its promise to provide more efficient methods of matching advertisers and consumers, not least owing to growing use of detailed individual data. Generally speaking, matching can be achieved in two ways (Evans 2009): one is through content creation that facilitates the aggregation and sorting of potential buyers (say, people interested in mountaineering whom a vendor of suitable equipment may want to reach); the other, often referred to as 'behavioral targeting', is through observation of individuals' characteristics and behaviors (from gender, age and location to more specific features such as mountaineering experience, frequency of practice, or past purchases of equipment) to identify those most likely to buy. Personal data, especially but not exclusively from online social platforms, can improve the efficiency of both aspects: first, users themselves create content and self-aggregate into like-minded groups, so that an advertiser can much more easily identify and address them; second, users' profiles reveal information not only about their own

P. Tubaro et al., *Against the Hypothesis of the End of Privacy*,
SpringerBriefs in Digital Spaces, DOI: 10.1007/978-3-319-02456-1_2,

characteristics and behaviors but also their friends', for example by commenting on their purchases. Clearly, tapping into such data brings advantages to advertisers, and the social media companies that manage these platforms gain by selling them more valuable advertising opportunities. Although behavioral targeting is still in its infancy (as it had virtually no existence before the advent of social media), analytical techniques to extract relevant information from people's behavioral data are improving fast.

Another area in which individual-level information on users is an asset for companies is *customer relationship management*. More and more often, web-based communities and peer-to-peer collaboration tools (whether in the form of microblogging, forums, wikis or customer review services) are used as extensions of traditional solutions for customer relationship management. Examples include the French La Poste's Twitter service ('Lisa'), and Toyota's proprietary social network ('Toyota Friend'), aiming to connect its customers with their cars, their dealership, and the company (see Balagué and Fayon 2010, 2011 for details about these experiences). Some of these services have enabled companies to make substantial savings, a prominent example being Orange.[1] Consumers' engagement is paramount for these services to be effective: it is essential that consumers actively participate in content creation, and to do so, they must accept to disclose at least some personal information. Similar issues arise in the case of companies that crowdsource innovation through online social networking services, from Fiat's design of the 'Mio' car in Brazil to VitaminWater's Facebook group to create a new beverage: their initiatives can only be effective conditional on the willingness of users to reveal their tastes, interests, or expertise in specific areas. Disclosure of individual information has more far-reaching consequences when companies use generalist networks (La Poste's Twitter, VitaminWater's Facebook) or connect their private network to generalist ones (Toyota Friend allowing connection to Twitter and Facebook), as any personal information has greater potential to leak to a wider set of connections. At the same time, use of generalist online services has advantages both for companies (which can rely on existing technical solutions without designing their own) and for users (who often find it handier to maintain fewer accounts and profiles).

In all these cases, the key question for companies (as well as social media services and policy-makers) is how to balance benefits from more intense use of detailed individual data against the possible loss of privacy of their customers. If the end-of-privacy hypothesis were to be confirmed, there would be a straightforward way to achieve this balance: companies should simply not hesitate to increase their use of personal data because individuals are more and more willing to share information. Furthermore, if the alleged stronger tendency to transparency among younger generations or so-called 'digital natives' (Prensky 2001) were also proven correct, an even steadier growth of data release could be expected to occur

[1] See for a detailed case study of the Orange Forum: http://synthesio.com/corporate/wp-content/uploads/2010/11/Case-study-Orange-for-website-EN.pdf.

in the future. In a classical rational-choice optimization model, one may think that people trade off privacy against advantages offered by use of social media; so that if they are found to willingly renounce privacy, it must be because they receive sufficient compensation, for example in terms of free-of-charge use of social networking sites, or perhaps even in expectation of more relevant advertising. A more critical, Marxist-inspired view equates online interactions to 'digital labor' (Scholz 2012; Fuchs 2012) and stresses the generalized exploitation and commodification of connected audiences. If personal information is 'extracted' from them to produce value (in terms of contents, information, knowledge bases, or databases) then consensual loss of privacy can be seen as a form of alienation (Formenti 2011; Fisher 2012).

As a matter of fact, there are three major reasons why alleged willingness of users to disclose their private information on social media should be taken with a grain of salt. One is *imperfect information* (Evans 2009): consumers may not be aware that data are being collected about them. Even after numerous press scandals and awareness campaigns (cf. Sect. 3.1), conditions and modes of information gathering in social media often remain opaque. Further, it is known that inequalities in education and socio-economic status affect the degree of people's Internet skills, including the capacity to understand default privacy settings and to adjust and fine-tune them (boyd and Hargittai 2010; Hargittai 2010).

A second problem is that, even when consumers are willing to release some or all of their personal data to one service, they may fail to take into account the possibility that the data will be shared with other companies, or matched with other sources of information, in ways that potentially increase the cost of any disclosure (in terms of, for example, exposing them to negative judgment by others, loss of reputation, disputes with family or friends, and even forgone professional opportunities).

A third and often overlooked problem is the *network structure of data collected through social media*. Traditional data gathering approaches such as surveys used to protect subjects through anonymity. Data from an online platform can hardly be anonymous, though, because the network of who has ties with whom cannot be constructed without the names of the persons concerned. The other typical safeguard of classical surveys was consent: participants had to confirm in writing that they had been informed of the purposes of the data collection and of any risks. Instead in an online network structure, a person may appear in the data as a contact of another, often with their full identifiers (notably name and address), but without having ever opted in or signed a consent form. The social network analysis scholarly community had devised solutions to alleviate these problems in *face-to-face* networks, for example through *ex post* anonymization and precise network boundary definitions (Borgatti and Molina 2003); but challenges are more acute in computer-mediated communications where large amounts of data can be mined through automatic procedures and algorithms, much more prone to side-stepping users' awareness and consent. Neither is the distinction between 'data' and 'metadata' popularized in the wake of the Prism scandal of 2013, sufficient to protect users. Even in the absence of information about the contents of individuals'

online profiles and communications (the 'data'), sheer connections between individuals, directly and indirectly obtained (the 'metadata') are often enough to identify them and can do serious harm.

Concluding, the end-of-privacy hypothesis is insufficient to provide guidance here. Although individuals share more and more information, they may do so because of lack of understanding of all the possible consequences of their behaviors, not because of a considerate 'rational' choice. It is unclear, then, how to interpret observed behaviors and what predictions to make for the future; and concerns that individual data are being exploited by corporate actors without adequately compensating or even notifying social media users cannot be easily dismissed. Similar issues arise not only in regard to companies' external stakeholders such as customers, but also internally with their employees, as the following section discusses.

2.2 Privacy in the Relationship of an Organization with its Employees

Privacy concerns emerge at all stages of the employer-employee relationship, starting from *recruitment*. There is evidence that a growing number of employers scrutinize candidates' profiles on social media before making hiring decisions. In Spring 2012, the press reported cases of dismissal of job applicants based on their score as calculated by Klout.com, a service that purports to measure Twitter, Facebook and LinkedIn users' online influence on a scale from 1 to 100 (Stevenson 2012). Especially in the United States, controversies have surrounded more disturbing cases in which job applicants were allegedly asked to 'friend' a member of the selection panel or even to provide username and password to their Facebook account (Kravets 2013). Though seemingly infrequent, and disapproved by Facebook itself,[2] such practices raise major prospective concerns in terms of privacy. Access to the full profile of an individual could provide employers with sensitive personal information that anti-discrimination legislation would not authorize to ask in interviews: with some variation across countries, this may include ethnic background, age, religious beliefs, sexual orientation, marital status, intention to have children, or political views. Another worry is that if such requests become customary, they can spread beyond human resources departments, and be used to control employees more generally. Their potentially disruptive effects can be illustrated, on a smaller scale, by the already widespread practice of friending one's boss (or subordinate) on Facebook, which has been shown to induce discomfort in employees at all levels of the organizational ladder (Ollier-Malaterre et al. 2013). The problem here is the blurring of boundaries between personal and

[2] E. Egan (Facebook Chief Privacy Officer) 'Protecting Your Passwords and Your Privacy', Policy of March 23 2012, https://www.facebook.com/note.php?note_id=326598317390057.

professional lives, and the injunction for a growing number of workers, to bring their own personal lives into their professional activity.

Privacy concerns are also at the core of recent debates around the *bring-your-own-device* (BYOD) trend in company policies, which is changing the way smartphones, tablets and laptops are being used (Ovum 2012). Ten years ago, it was standard practice for companies to provide professional IT equipment to their employees (BlackBerry is a typical example), and keep use restricted to work purposes. But today, more and more devices are being conceived for consumption, entertainment and more generally, personal rather than professional use; their diffusion among the general population makes them suitable for performing communications and transactions of all types, both within and outside work. To accommodate employees' demand for greater usability and wider choice, a growing number of companies now let them buy their preferred devices, and just connect them to the corporate network when they are at work. However, BYOD practices are now producing unintended consequences, disrupting the existing work/life balance of employees and introducing new tensions between their private and public spheres (Broadbent 2011; Gregg 2011).

Thus employees' personal data are positively at risk of becoming part of their professional activity, and the boundaries between the two are blurred: once an employee's personal emails, list of online contacts, holiday videos and family photos enter the circuits of the corporate IT system, it becomes difficult preventing the employer from accessing them. These fundamental ambiguities open the door to myriad possible abuses, despite the effort of more and more companies to design responsible BYOD policies. As far as present-day legislations tend to favor employers against financial cybercrime, industrial espionage or instances of employee malpractice, any data circulating on a company's network (regardless of the device used to create or to transmit them) can be the object of unwanted and unnecessary scrutiny. Another major problem, stressed by companies themselves, is the growing difficulty for their IT departments to ensure the security of a wide range of different devices, keeping all of them up-to-date. Considering that the devices are ultimately under the control of private users rather than the organization, some companies have made users responsible for any unwanted disclosure of corporate information. But as a result, employees find themselves under a double, and contradictory, pressure to disclose their own personal information to the company, while at the same time acting as gatekeepers for company information. Such a task becomes ever more challenging in the increasingly frequent cases in which the boundaries of a company policy are themselves somewhat fuzzy—such as business partnerships, outsourcing, and more generally use of social media for parent-subsidiary coordination or business-to-business communication.

Once again, the end-of-privacy hypothesis, with its distinctively deterministic flavor, offers little guidance as to how to solve these problems and contradictions. There is a widespread perception that disclosure of employees' personal information to their employers via social media may have consequences that cannot be fully anticipated in the current state of things. In sharp contrast with the tenets of

theories of generalized 'publicness', some scholars are predicting that more users will opt for a more controlled approach to privacy as they realize that their online profiles are being scrutinized by potential or actual employers (Phillips et al. 2009); and career advisers are starting to warn people who are (or aspire to be) in top management positions, that caution in social media is preferable to exposure.

The above considerations put forward several reasons why companies may want to enhance their capacity to use detailed individual information, but at the same time, face numerous challenges if they push their data analytics agenda too far. It becomes important at this point, to look closer at the threats and opportunities that privacy raises for social media services, and their specific incentives as key intermediaries between businesses and end users.

2.3 Privacy Dilemmas for Social Media Services

Internet and more specifically, social media companies face particularly complex challenges in their role of intermediaries in what economists call 'two-sided' markets. This expression designates markets in which: (1) two different sets of agents interact through an intermediary or platform, and (2) the decisions of each set of agents affect the outcomes of the other set of agents, typically through an externality (Rysman 2009). Media companies operating between advertisers and consumers are a typical example, along with the payment card industry (between merchants and customers). Typically, pricing is asymmetric, and depends on the price sensitivity—technically, the elasticity of demand—of each side; it often turns out that one side does not pay, or is even rewarded for using a service (with cash-back for credit card use for example), while the other, more price-inelastic side faces a high mark-up (Rochet and Tyrole 2003, 2006). Indeed use of several of the most popular generalist social media has traditionally been free of charge, while advertisers pay fees. The zero price on the users' side attracts huge numbers of people who may otherwise be unwilling to use the service, thereby increasing the value of advertising space and leading to higher prices for participation on the advertisers' side; in turn, the value extracted from advertising fees enables the social media platform to improve the service and attract ever more users.

Relative to newspapers and traditional media, Internet platforms are of particular interest to advertisers for their capacity to leverage detailed personal information on a much larger scale than ever before, achieving high efficiency in matching advertisers and consumers as discussed above. Most of their operations consist in gathering, sorting and repackaging information on one side of the market, users, in ways that are relevant to the other side, advertisers. Therefore Thépot (2013) proposes a definition of the relevant market as being in the area of *monetization of users' information to advertisers*, and as encompassing not only social media companies but other Internet service providers too, notably search engine businesses.

Despite this common core, there are differences between the business models of social media and other Internet firms. Most of online advertising is search-based, essentially consisting in matching user searches and advertiser-generated keywords, with high effectiveness because it reaches consumers precisely when they are looking for something specific. For example, Google's model is based on this scheme, and achieves precise targeting using data on searches (including sometimes search history) and other personal information such as location. Advertising on Facebook has long been seen as less effective, partly because users mostly log onto the service to socialize rather than search or buy things, so they perceive ads more as a nuisance than as useful information. Google's ads have always commanded higher rates than Facebook's (Evans 2009); Google has also had a consistently higher share of the worldwide online ads market, of 33.24 % in 2013, against 5.04 % for Facebook (eMarketer 2013). Yet online social networking services offer newer and promising opportunities. They enable marketers to exploit word-of-mouth mechanisms—which were already known to be highly effective, but were very hard to implement or even just measure before the digital age. For example, Facebook has devised various ways to target consumers based on the choices and behaviors of their friends. Since its early days, Facebook has aspired to become a one-stop shop to access other websites, and an ever-increasing number of external services have been using Facebook identifiers for logging in.

In sum, it has been relatively difficult for social web companies to monetize their gains from personal data so far, despite the unprecedented amount and scope of the information available, the social connectedness in which it is embedded and its assumedly voluntary release by users.

In what follows, we will see that the main dilemma and the crucial difficulty for understanding digital interactions reside precisely in this last aspect—the extent to which private data are released *willingly*. This is also the main bottleneck for the future development of the social web and the business opportunities that it provides to corporate actors. *The specter of privacy haunts today's Internet*: it is only to the extent that users continue to willingly provide information, and do not entirely resist its re-use for commercial purposes as well as its release to affiliated companies and services—put differently, if the end-of-privacy hypothesis is confirmed—that their business model can hope to grow and prosper. If concerns over online privacy grew significantly worldwide, translating into a wave of restrictive legislation in multiple countries, web giants could find it very hard to prosper any further along the same lines.

Having outlined the main incentives, opportunities and challenges for the industry, it becomes now important to detail how the different stakeholders have reacted to them.

References

Balagué, C., Fayon, D.: Facebook, Twitter et les autres. Pearsons Education, Paris (2010)

Balagué, C., Fayon, D.: Réseaux sociaux et entreprise: les bonnes pratiques. Pearson, Paris (2011)

boyd, d., Hargittai, E.: Facebook privacy settings: Who cares? First Monday **15**(8), http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3086/2589 (2010)

Broadbent, S.: L'intimité au travail: La vie privée et les communications personnelles dans l'entreprise. FYP éditions, Limoges (2011)

Borgatti, S.P., Molina, J.L.: Ethical and strategic issues in organizational social network analysis. J. Appl. Behav. Sci. **39**(3), 337–349 (2003)

eMarketer: Worldwide mobile Internet ad revenues, June 13, http://www.emarketer.com/Article/Google-Takes-Home-Half-of-Worldwide-Mobile-Internet-Ad-Revenues/1009966 (2013). Accessed 1 Aug 2013

Evans, D.S.: The online advertising industry: Economics, evolution, and privacy. J. Econ. Perspect. **23**(3), 37–60 (2009)

Fisher, E.: How less alienation creates more exploitation? Audience labour on social network sites. TripleC-Cogn. Commun. Co-oper. **10**(2), 171–183 (2012)

Formenti, C.: Felici e sfruttati: Capitalismo digitale ed eclissi del lavoro. Egea, Milan (2011)

Fuchs, C.: Dallas Smythe today—The audience commodity, the digital labour debate, Marxist political economy and critical theory. Prolegomena to a digital labour theory of value. TripleC-Cogn. Commun. Co-oper. **10**(2), 692–740 (2012)

Gregg, M.: Work's Intimacy. Polity Press, London (2011)

Hargittai, E.: Digital na(t)ives? Variation in Internet skills and uses among members of the 'net generation'. Sociol. Inquiry **80**(1), 92–113 (2010)

Internet Advertising Bureau, IAB: Global internet advertising revenue report for Full-year 2012, conducted by PricewaterhouseCoopers on behalf of IAB. http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-060313 (2013)

Kravets, D.: 6 states bar employers from demanding Facebook passwords. Wired, January 2, http://www.wired.com/threatlevel/2013/01/password-protected-states/ (2013)

Ollier-Malaterre, A., Rothbard, N., Berg, J.: When worlds collide in cyberspace: How boundary work on online social networks impacts professional relationships. Acad. Manage. Rev. **38**(4), 645–659 (2013)

Ovum: Ovum's multi-market Q4 2012 BYOD survey, multi-market BYOD Survey Results: employee behaviour and attitudes toward mobile device usage at work. http://www.logicalis.com/news-and-events/news/logicalis-white-paper-byod.aspx#.UNYb67bvxJO (2012)

Phillips, K.W., Rothbard, N.P., Dumas, T.L.: To disclose or not to disclose? Status distance and self-disclosure in diverse environments. Acad. Manag. Rev. **34**(4), 710–732 (2009)

Prensky, M.: Digital natives, digital immigrants. Horiz. **9**(5), 1–6 (2001)

Rochet, J.C., Tirole, J.: Platform competition in two-sided markets. J. Eur. Econ. Assoc. **1**(4), 990–1029 (2003)

Rochet, J.C., Tirole, J.: Two-sided markets: A progress report. Rand J. Econ. **35**(3), 645–667 (2006)

Rysman, M.: The economics of two-sided markets. J. Econ. Perspect. **23**(3), 125–143 (2009)

Scholz, T.: Digital labor: Introduction, in Id. Digital Labor: The Internet as Playground and Factory. Routledge, New York (2012)

Stevenson, S.: What your Klout score really means. Wired, April 24, http://www.wired.com/business/2012/04/ff_klout/ (2012)

Thépot, F.: Market power in online search and social-networking: a matter of two-sided markets. World Compet. **36**(2), 195–221 (2013)