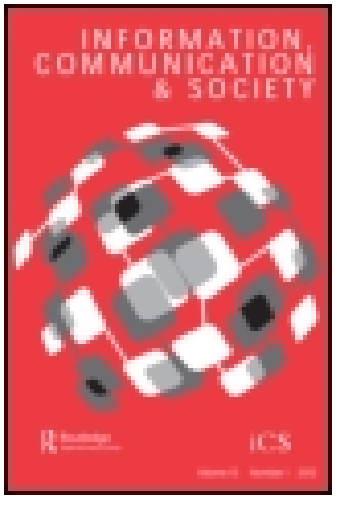

Information, Communication & Society
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/rics20

Power, knowledge, and the subjects of privacy: understanding privacy as the ally of surveillance

Sami Coll[a]
[a] Department of Sociology, University of Geneva, 40, Bd. du Pont-d'Arve, Geneva 1211, Switzerland
Published online: 22 May 2014.

To cite this article: Sami Coll (2014): Power, knowledge, and the subjects of privacy: understanding privacy as the ally of surveillance, Information, Communication & Society, DOI: 10.1080/1369118X.2014.918636

To link to this article: http://dx.doi.org/10.1080/1369118X.2014.918636

Information, Communication & Society, 2014
http://dx.doi.org/10.1080/1369118X.2014.918636

Power, knowledge, and the subjects of privacy: understanding privacy as the ally of surveillance

Sami Coll*

Department of Sociology, University of Geneva, 40, Bd. du Pont-d'Arve, Geneva 1211, Switzerland

(*Received 28 February 2013; accepted 15 April 2014*)

The aim of this article is to argue that privacy, rather than serving only as a countermeasure against surveillance, can also be seen as its 'partner-in-crime'. Normative statements made by governments and companies on privacy can be regarded as a tool of governance in service of informational capitalism. Initially defined as a fundamental freedom, privacy has become a precondition for a blossoming economy in the context of the information society. The notion of privacy, as a critique of information society, has been assimilated and reshaped by and in favour of informational capitalism, notably by being over-individualized through the self-determination principle. To develop this idea, this article builds on the results of a study on the loyalty programmes run by the four biggest retailers of Switzerland and on the Foucauldian concept of biopower. Indeed, sexual liberation and the development of scientific knowledge on sexuality, the democratization of privacy, and the emergence of scientific discourses about privacy are processes that show intriguing similarities. Like sexuality, privacy has become a 'power-knowledge' related to moral standards defining what privacy should be. It produces 'subjects of privacy' who are supposed to take care of it according to the official conception of privacy advocates and of the legislature. Finally, we suggest understanding the conception of privacy as a terrain of power struggle between the promoters of an informational capitalism based on surveillance of citizens and consumers, and those who would prefer to promote privacy as a common good leading society to more democracy and freedom.

Keywords: surveillance/privacy; sociology; biopower; Foucault; loyalty programmes; Big Data

Introduction

Although it does not explicitly mention privacy, the commentary of Bozovic (1995) in the introduction of Bentham's *Panopticon* indirectly suggests looking at privacy in a new way. The author reminds us of the existence of a line drawn on the floor of prison cells beyond which prisoners cannot be seen. However, as Bozovic argues:

> Invisibility is, no less than visibility, a reliable indicator of the prisoner's exact location at the time. Thus, if at a certain moment the prisoner cannot be seen, in the 'compact microcosm' of the panopticon, he can only be beyond the line. In the panopticon, it is impossible to escape the inspector's gaze even if the prisoners hide from his eyes and make themselves invisible – since once the prisoner has crossed the line and becomes invisible, 'his very invisibility is a mark to note him by', writes

*Email: sami@samicoll.com

> Bentham. In the all-transparent, light-flooded universe of the panopticon, invisibility itself has become a positive quality, a *visible sign* of the prisoner, as it were. Thus, the inspector is in fact all-seeing: his gaze extends *beyond the limits of the visible into the invisible*. (p. 18, emphasis in original)

The same idea can be found in George Orwell's novel *Nineteen eighty-four* (1949), wherein the main character, Winston Smith, thinks he has found a place where he cannot be seen. It turns out at the end of the novel that this was a staged illusion and that this private space was actually thought to exercise control on resistant citizens. The idea that can be built on these metaphors is that privacy, rather than being only a countermeasure against surveillance, can also be seen as a part of the whole mechanism of surveillance. The more clearly privacy is defined, the more it can be subject to control.

Without going as far as this, many privacy and surveillance scholars have been highly critical about the notion of privacy (Gilliom, 2011; Monahan, 2006; Stalder, 2002). The most radical ones suggest putting it aside in the analyses because, they argue, it tends to hide actual social and power issues (see, e.g. Gilliom, 2011, p. 500). Others, including Westin (2003), while still supporting the notion, consider privacy as an upper-class privilege:

> [P]rivacy is frequently determined by the individual's power and social status. The rich can withdraw from society when they wish; the lower classes cannot. The affluent do not need to obtain subsidizing support from the government by revealing sensitive information to authorities, while those in economic or social need must disclose or go without. (p. 432)

According to the results of Gilliom's (2001) study, which show how working classes hide their revenues from the social system in order to avoid having their social assistance removed and consequently becoming even poorer, Gilliom would not disagree with Westin. Steeves (2009) is also quite critical when she mentions that in her observations, the protection of data sometimes seems to contrast with the protection of privacy. For Regan, who has been defending since 1995 the idea that privacy should be reinforced as a collective value rather than being seen only as an individual resource, the idea of an 'invasion of privacy' has actually become too limited to account for what turned out to be a worrying and recurring issue of modern life (Regan, 2011).

The intention of this article is to further develop this critical perspective by arguing that normative statements on privacy made by governments and companies can be regarded as a tool of power and governance in service of informational capitalism. Initially defined as a fundamental freedom, privacy seems to have become a precondition for a blossoming economy in the context of the information society (Kessous, 2012, p. 79). This is precisely the idea that will be developed herein, with the argument based on the Foucauldian concept of biopower and on the results of a study on the loyalty programmes run by the four biggest retailers of Switzerland (Coll, 2014).

Governing with privacy

Because the notion of privacy, despite more than 30 years of scholarly work, is still a very complex, multidimensional, and confusing notion (Bennett, 2008; Solove, 2008), there is no univocal definition of it that could unify scholars and lawyers. In the information society context, since the 1960s and 1970s when 'society was moving from paper records to large computerized databases' (Regan, 2011, p. 497), laws generated to protect citizens' privacy have been increasingly focusing on privacy's informational dimension. Protection of privacy now inevitably involves protection of data, so specific data protection laws have been adopted by many governments. Their purpose is to ensure the protection and the ownership of personal data, and the

specific area of privacy that consists of all private data concerning an individual is most often defined as *informational privacy*.[1]

Despite this attempt to define the issue of privacy in the information society, it is not always clear in the debates and in the literature whether one is talking about privacy in its entirety or about a specifically informational privacy – that is to say, a set of information considered private in a given context. Moreover, even if one focuses on studying the informational dimension of privacy, it is unclear whether one is interested in information in general or in computer data. Notwithstanding these difficulties, when speaking about the possible abuse of surveillance practices, the notion of privacy remains the weapon of choice and is not reduced solely to its informational dimension. In the 1960s, pioneering thinkers consolidated the idea of self-determination of privacy (Jourard, 1966; Ruebhausen & Brim, 1965; Westin, 1967), which has become the cornerstone of current privacy policies. Concretely, in the legal context, such debates aim to address the problem of data protection by granting every individual the right – but also the responsibility – to control his or her own data through the right to access the data and correct it if needed.[2] This became the so-called 'informational self-determination principle' promoted by most European policies on data protection, particularly in Germany and Switzerland (Bennett, 2008, pp. 6–7).

Today, legislators continue the difficult task of developing an operational approach to privacy and a set of rules that can address the problems emerging with the massive production of data. While recognizing the importance of this work, many authors lament the tendency of data protection laws to shut privacy up within an individualistic and static conception (see, e.g. Gilliom, 2011, p. 501; Stalder, 2002, p. 121). Most often, privacy is seen as an informational bubble surrounding individuals that must be protected against external and undesired intrusions from the state, private companies, or even other persons motivated by their curiosity.

No one would blame the legislature for this tendency, as these laws are primarily intended to thwart the damage that could be produced by the increasing digitization of personal data, not to feed an endless discussion about an academic definition of privacy. Nevertheless, this positivist view of privacy, which we propose to call herein *objective privacy*, has a normative and prescriptive scope that produces power effects that we wish to analyse.

Power, knowledge, and the subjects of privacy

Before becoming a value protected by the legislature, privacy has been the subject of a historical development originating, according to historians, around the early eighteenth century. They observe the emergence at this time of specific activities that have become increasingly autonomous from public ones and that can gradually be qualified as private activities (Ariès, 1987, p. 18). The gradual increase in the autonomy of these activities shows the emergence of the value of the right to own 'privacy'. A new window of space and time became available for specific activities that would today be labelled as private, allowing the possibility of privacy to emerge. Such privacy remained an exclusively upper-class privilege until the early 1960s (Holvast, 2007; Prost, 1999). Before, for example, popular classes had no designated places such as the conjugal bedroom, a boudoir, or an alcove, as the bourgeoisie did, as a place for private sexuality (Prost, 1999, p. 60). This democratization of privacy as a value probably encouraged middle classes to claim a so-called sexual liberation during the 1960s and 1970s. The very same liberation has been described by Foucault (1978) as a subtle operation of power aiming to encourage popular classes to speak about their sexuality to the social institutions, such as medicine or government, aiming to regulate sexual practices through birth control politics. Foucault further generalized the concept of biopower, first theoretically developed around sexuality, for any type of power that directly targets the body and intends to take control of it (Foucault, 1979, 2008).

Sexual liberation and the development of scientific knowledge on sexuality, the democratization of privacy, and the emergence of scientific discourses about privacy are processes that show intriguing similarities. Like sexuality, privacy involves the acquisition of rights, the diffusion of values, and the development of statements that regulate its implementation. In this sense, privacy, like sexuality, is a 'power-knowledge' (Foucault, 2003, p. 252) related to moral standards defining what privacy should be.

In the second volume of Foucault's work on sexuality, *The use of pleasure* (1985), sexuality is theoretically formalized as a social control to regulate sexual behaviour, a *dispositive of power* with the objective of taking control of bodies. This dispositive organizes power around three axes (Foucault, 1985):

> To speak of sexuality as a historically singular experience also presupposed the availability of tools capable of analyzing the peculiar characteristics and interrelations of the three axes that constitute it: (1) the formation of sciences (*savoirs*) that refer to it, (2) the systems of power that regulate its practice, (3) the forms within which individuals are able, are obliged, to recognize themselves as subjects of this sexuality. (p. 4)

According to Foucault, around the middle of the nineteenth century, sexuality was being redefined as a list of particular practices that creates scientific knowledge – mainly medical and psychoanalytic – and the church no longer monopolized societal understanding of it. This new type of knowledge has produced discourses distinguishing normal and pathological practices based on rational argumentation. This alludes to the theoretical suggestion of this article: that privacy can also be modelled through the very same axes used to describe biopower on sexuality. First, privacy is also an object of *science*. Efforts are made by many experts – some call them the 'privacy scholars' (Bennett, 2011a) – to provide the best definition of it. In the information age, scientific literature on privacy is growing. Second, data protection laws and policies, public or private, and 'privacy advocates' (Bennett, 2008; Regan, 1995) constitute 'the systems of power that regulate its practice' (Foucault, 1985, p. 4). They have the power to define what privacy is or is not and to suggest measures to protect it. Lawyers, for example, have the power to determine when an invasion of privacy is legitimate or not, in the name of security, public health, or economic growth. Third, by promoting in the first place the self-determination principle, the main project and discourse of data protection laws is to educate users to protect their own privacy, at least in the informational context. In other words, biopower is producing subjects owning a privacy, feeling concerned about it and willing to protect it. Discourses produced by most privacy advocates and activists about our freedom are *de facto* prescriptive when addressing citizens, consumers, or users of technologies of information. Their statements might sound something like, 'You have privacy, you must protect it, and we will tell you how to do it.'

From here emerges the theoretical idea that the notion of privacy and the surveillance of data act as the 'partners-in-crime' of the current growing digital economy. The aim of the second part of this article is to use the results of a case study on loyalty cards to empirically illustrate some of the aspects of this dynamic. Although it is limited to the context of consumption in Switzerland, this case study can nevertheless modestly present an argument in favour of such a thesis.

Loyalty cards in Switzerland

For more than a decade, many retail companies have been collecting massive amounts of data on a daily basis through loyalty card programmes that gather, at point-of-purchase, the identity of the consumer, date and time of the transaction, and the list of products purchased. As an incentive, these programmes usually enable customers to collect points for each purchase, which can be

converted to rewards or give them access to rebates only available to card owners. The large amount of data gathered in this way can be used for several purposes, mainly to maximize benefits or minimize costs. By maintaining this information, private companies generally aim to enhance their relationships with their customers, increase sales and, more specifically, suggest to their customers relevant products that carry a larger profit (Coll, 2012a). Because they collect data in large amounts and process them with elaborate data-mining algorithms that are able to produce new sets of data carrying more information than raw data, such as psychological profiles (Millar, 2009; Pridmore, 2008), the question of privacy protection inevitably arises in the literature (Gilliom & Monahan, 2012; Lyon, 2007; Tavani, 1999).

We draw on an ethnographical study that we conducted on the loyalty programmes of the four biggest retail stores in Switzerland, focusing on data protection and privacy issues. First, field observations (more than 167 hours) were made behind checkout lines (in three stores), at customer service desks (in four stores), in call centres (of two of the four companies), around point of purchase (in one store), and in a training centre for employees (of one company). Standing behind the cashiers, we observed the way employees asked customers to show their loyalty card and how they tried to convince them to get one if they did not have one already. At the customer service desks and at the points of purchases, we focused on the type of access employees had to the database and how they could use it to provide personalized services to the customers. In the call centres, we were allowed to listen in real time to claims customers made about their loyalty cards when they called in. In the training centre, one day was spent observing how future sales managers were trained to include the loyalty card of the company in their marketing strategies. Second, semi-structured interviews were conducted with managers in charge of supervising the loyalty programme, the store, the marketing branding, or the training of employees (14 interviews); and with employees (9 in-depth interviews and 57 short interviews made during the field observations, primarily focusing on interactions that had just occurred). Finally, a total of 108 customers (71 women and 37 men) of the four retail companies, recruited at the exit of the stores, were interviewed, whether they owned loyalty cards or not. All data were fully transcribed and added to a heuristic data base on ATLAS.ti, and analysed using grounded theory (Charmaz, 2011).

Subjective privacy and privacy as lived experience

One of the main findings of this study is the inadequacy between the legal perspective of privacy – in particular, informational privacy as articulated in data protection policies – and the subjective perspective of consumers. The consumer's *subjective privacy*, as expressed by consumers when they were asked to define privacy in their own terms, appears to be richer and more diverse than that of privacy advocates. However, the myriad of different points of view expressed can be summarized in five ways, as expressed below, which are not exclusive and in most cases overlapped in the interviews. They account for a highly subjective approach to privacy and go beyond the idea of a control of data, even if some of them are closer than others to the juridical definition.

First, privacy was frequently defined in relational terms, which involve friends, partners, or a family member. It contains feelings and sexuality, as well as the content of personal secrets or discussions on private subjects:

> Because my privacy is more something like the relationships I have with people, my friends, what I think. It is more than what I like to buy. (Female employee, 31 years old)

> My privacy is, I would say, my family, my son, yes, my everyday life, my professional life. (Female employee, 55 years old)

Second, privacy was often seen in terms of freedom – notably the freedom of choice. Any attempt to limit it, whether by governments, companies, or a person, is seen as an invasion of privacy:

> My privacy is all that is determined by my will of action. Anything that doesn't come from an external will, such as the state's for instance. That is my freedom, my own decisions. (Female student, 25 years old)

> I think it is a sphere where no one has to right to break in, the government, but also companies, in general. (Female student, 20 years old)

Third, relations to the body, the mind, and the feelings were frequently mentioned. Not only was the body seen as private, but also any information concerning it, such as health matters. Privacy was also seen as concerning opinions or feelings of a personal nature:

> Knowing if I drink coffee or not, if I drink milk or not, well … all of this is not really important. I don't mind that others know about it. I feel more concerned about data regarding my health. This would be a problem. (Female student, 23 years old)

> Aside from personal data, for me, privacy is situated at another level. It is more about what is intimate, what I feel. (Female student, 35 years old)

Fourth, a definition in terms of space and time was given. In that case, privacy is not only delimited by space – generally, the home – but also by time boundaries such as lunch, dinner, leisure time, and evenings:

> The most annoying is the ad calls, above all the time when they call. It is always when it is the most inappropriate … either noon or 7 pm, when you are going to cook. (Housewife, 40 years old)

Finally, a few persons, in fact a very small minority, link the notion of privacy with *information*. When they do, such information includes age, religion, and sexual preference as well as less-sensitive information. Nevertheless, 'information' is seen in a larger, more abstract and blurred way, and above all, not necessarily as computerized data:

> I remember my dad, when I was a kid; he used to answer the phone, that's something that drove him crazy: 'Hey, would you also like to know my pant size?' Because they ask for so much details! (Housewife, 40 years old)

> Privacy, for me, is where I draw a line at what I am going to disclose or not. That is to say, what is under my control, when I can make the decision of if I want to share something or not. (Female student, 20 years old)

These perspectives differ from the normative definition of privacy given by the legislature and privacy advocates, even if a few similarities exist (for example, in the last quotation above, the student mentions the idea of control of her personal information). This difference of perception of one's own privacy poses an initial problem for the application of the principle of informational self-determination. It becomes even more complicated when consumers face systems collecting and conserving their personal data in their everyday lives, and experience privacy in their everyday lives – what we have called, for the sake of the argument, *privacy as lived experience*. This perspective not only moves away from the juridical definition, but also from the subjective definition that comes from consumers themselves. This observation agrees with the results of

researchers who have shown, beyond the sole case study of loyalty cards, a significant difference between people's expressed concerns about privacy and their actual practices of disclosure (Chellappa & Sin, 2005; Malhotra, Kim, & Agarwal, 2004; Metzger, 2006).

Indeed, what would be seen as an invasion of privacy by data protection laws or by the interviewees themselves, when asked, does not actually seem to cause problems in their everyday interactions with companies. During field observations in a call centre, a customer who called on behalf on his partner did not seem annoyed when the operator asked him if they lived together (see below). However, asking this question precisely clashes with the subjective definition given by some of the interviewees themselves when they described privacy in relational terms. Moreover, it is paradoxically the data protection policy of the company that required the operator to ask this 'indiscreet' question (in her own terms) in order to prevent frauds:

A male customer to the operator:	I am calling on behalf of Ms. X.
The operator:	Well, but there is the protection of data policy … do you live together?
The customer:	Yes, we see each other every day.
The operator commenting after the call:	Sometimes we have to be indiscreet. I had to ask if they live together. It is a bit indiscreet!

No feeling of invasion was observed either when a female employee of a consumer service desk asked customers requesting a new card if they were single or married, even though the question is about an intimate relationship. The same absence of a feeling of invasion of privacy was observed when an elderly woman asked a male employee at the same customer service desk to find in the loyalty system the name of a tonic breast cream she bought a few months ago, although this interaction involves the intimacy of the body:

A male employee at the customer service:	I can see two purchases of Yves St-Laurent products in February.
The elderly woman:	It can't be. The last purchase was in January.
The employee:	Would you like to know which article it was?
The woman:	Yes, please.
The employee:	So, there were some mascara, some nail varnish and a cosmetic which price was 79 francs and 90 cents.
The woman:	That's a tonic breast cream, for 79 francs 90, yes!

Actually, it is rather the employees that show discomfort when customers, for example, put condom boxes on the conveyor belt of the cashier that will be registered in their customer account:

> Recently I had a couple of times condom boxes or similar kind of stuff I was feeling uncomfortable about. I was about to go red because, I thought, I don't want him to see that I saw what it was, condoms, I was afraid it would make him uneasy, and I was feeling uneasy. Well, a bit difficult experience to go through, you know, because, I don't know, it's a bit embarrassing, it's true, to see this displayed in everyone's sight. (Cashier, 22 years old)

On the contrary, other situations that would not be defined either by privacy advocates or customers as invasions of privacy sometimes produce such a feeling. During observations, feelings that privacy had been breached were expressed in concrete ways that did not necessarily involve

collecting data. Worries were clearly expressed when, for example, a young man in a customer service department was asking middle-aged women for their date of birth in order to register a new loyalty card. These women felt discomfort because the employee was younger rather than because the company could possibly use their date of birth for marketing purposes. As Regan (1995) argues, 'The privacy people express concern about is not abstract but derived from real circumstances with immediate consequences' (p. 224). In this example, the immediate consequence here, for a middle-age woman, is for a young man to discover how old she is. It is in fact situations related to very concrete concerns of consumers – like hiding their age – that trigger feelings of invasion of privacy, instead of the knowledge that companies are collecting and analysing data. For consumers, these corporate practices are easy to forget, if ever known, compared to their everyday and concrete concerns.

In other words, concrete situations producing a feeling of invasion of privacy often do not square with what is considered a risk by data and privacy protection laws. Ironically, measures meant to protect customers' privacy are the very ones that produce this feeling. The observations in one call centre repeatedly revealed this paradox. Notably, in order to protect customers' data against fraud, operators were required to identify callers by following a precise protocol. Customers had to give their card number, their home address, and their telephone number, as well as to answer two additional 'control questions':[3] how many points they thought they had on their account, the last store they visited, or some information about the last reward they ordered. Although they are meant to protect their data, it is precisely these questions that produced a feeling of invasion of privacy, as shown below in two observation extracts and followed by the operator's comments from a short interview:

The operator:	What was the last reward you ordered?
A female customer:	Uh … is this an investigation or what?
A male customer:	Why are you asking me all of this? You're not a bank!
Operator's comment:	Some customers get angry and ask 'do you also want my size, my date of birth?' or they hang up directly.

To avoid negative reactions, some operators had developed personal strategies to hide 'control questions' behind questions that can be understood as necessary to provide the service the customer are asking for. In the example below, the operator asks two such questions: how a reward has been ordered and when:

A female customer:	Good morning, I would like to cancel a reward I just ordered please.
The operator, after basic identification questions:	How did you order the reward, with our Website or by mail?
The customer:	Through Internet I think.
The operator:	Do you remember when?
The customer:	That was ten days ago.

The fact that customers potentially react badly to questions meant to protect their privacy – to the point where some operators use strategies to hide these questions – show that companies, in a sense, seem willing to protect customers' privacy even when customers do not seem worried about it. Paradoxically, private companies and governments seem to be actually defending privacy values much more than the majority of consumers (Holvast, 2007, p. 766), although they are the very ones that represent a threat to privacy. This is an additional paradox to the one often described as the 'privacy paradox' by scholars who underline the distance between

the discourse of people who express concern about their privacy, via interviews and surveys, and their actual behaviour in disclosing their personal data quite easily (Metzger, 2006; Nissenbaum, 2009; Regan, 2003).

These apparent paradoxes can possibly be explained by the diversity of ways in which the people observed in our study understand and adopt the notion of privacy. The normative definition of privacy given by most privacy advocates – *objective privacy* – does not always fit the subjective perspective of consumers we interviewed – *subjective privacy* – and even less the way it is experienced in consumers' everyday lives – *privacy as lived experience* – as shown briefly in the empirical extracts above. The lack of concern observed when customers showed their loyalty card to the card reader should not be interpreted as indifference towards privacy, although it could be seen as such in regards to *objective privacy*. Customers do value privacy, as they duly elaborated during interviews – in terms of *subjective privacy* – but this does not often square with the *objective privacy* that the legislature advocates. What is more, in the context of market interactions, as we could see during our field observations, *privacy as lived experience* is sensitive to very concrete human interactions (such as face-to-face requests for information like date of birth or requests to show a card) and does not necessarily echo subjective and objective definitions of privacy. On the contrary, situations that could have been felt by consumers as posing a threat to privacy according to their discourse do not seem to be problematic in the context of direct interactions. These observations not only show how the perception of privacy and intimacy relates to the context of the interaction (Coll, 2012b; Nissenbaum, 2009); they also actually unveil that the definition of privacy is a terrain of power struggle. The empirical dissociation between subjective privacy, objective privacy, and privacy as lived experience show how one of these conceptions, the objective (and normative) perception of privacy, seeks to dominate the other conceptions through a *dispositive of power* (Foucault, 1985) in order to make them compatible with surveillance devices that feed informational capitalism.

Challenging the informational self-determination principle

Through the results of this research, the *informational self-determination principle* guiding privacy and data protection laws – which holds that every person should serve as a proactive actor of his or her own privacy (using the right of access to the data, its modification, or its destruction) – is seriously challenged. Is it reasonable to expect that individuals would learn how to 'manage' their own privacy, as suggested, for example, by data protection laws? This would mean the three perspectives on privacy we observed in our research must converge. We must ask, though, is such a thing really desirable? Is not the divergence of perspectives on privacy, in a way, a guarantee of freedom because it provides individuals with some leeway to approach privacy as they wish? Indeed, if individuals had a perception strictly similar to the prescriptive definition of authorities, their privacy would definitively become the target of a generalized surveillance. In other words, the sharper the definition, the easier its control. In Foucault's terms, any scientific discourse about the subject reinforces its subjection (Foucault, 1972). This is how privacy, we think, might tend to become the best 'partner-in-crime' of surveillance rather than its antidote (Stalder, 2002).

In 1987, Simitis already spoke of the right to control one's own data as being 'chimerical' (p. 736). Since then, it has become even more difficult to exercise the right of access to one's own data, claiming a so-called transparency that is actually a fiction. In the specific case of loyalty cards, but also in any other commercial relationship established through information technologies (Kessous, 2012), data gathered can be used to produce a new kind of data set, such as psychological or sociological profiles (Millar, 2009; Pridmore, 2008). Although raw data collected can appear trivial to those disclosing them, data-mining techniques allow companies to

infer sensitive information such as sexual orientation, political opinions, or medical condition (Coll, 2013) without the knowledge of concerned people. Real transparency would not only allow subjects access to raw data, but also to the sociological or psychological profiles that are built on them. Although the vast majority of interviewees did know that by using cards they disclose details about their purchases that companies could retain, they did not know that such details can reveal sensitive data, as demonstrated in the extracts shown below:

> Is there anybody able to do something with these data? I don't think so. Oh yeah, there were the 'best customer' promotion with coupons, special products, so they know who bought what. (Female employee, 29 years old)

> I don't know if they monitor, but I guess they do an assessment; well, I really don't know. They calculate how many points we have, that's all. (Retired woman, 78 years old)

> Honestly, I don't care if they keep all these data about what I buy. I don't even understand what they can do with it. (Female student, 21 years old)

> I don't care; it's only about carrots and potatoes. If it was that I slept with a twenty-five-years-old boy, no way! (Retired woman, 64 years old)

An imbalance of power is created by this transparency asymmetry, which relies on the lack of knowledge consumers have about how data are collected, analysed, and used. Although some companies have addressed some consumers' concerns about how data are collected – some of them provide direct, secured access to personal data on the Web (as in the case of two of the four studied companies) – they still keep how they analyse and make use of these personal data strictly secret. Consequently, not only does the legislature's *objective* approach of privacy tend implicitly to shape privacy as a tool of governance, but its informational self-determination principle, given the transparency asymmetry, seems doomed to failure. Consequently, no privacy policy should assume that the only way to counter surveillance is to educate people – that is to say, by making them aware that disclosing personal data can be risky.

Conclusion

In following the adaptation of Foucault's model of the *dispositive of power* to privacy, companies and governments should be considered the main actors of the regulation of a 'practice of privacy', as medical institutions have been regulating a 'practice of sexuality'. In a way, data protection policies (created by companies or governments) make people feel at ease with the spread of the information society now at the core of modern capitalism, without blocking the economic market (Kessous & Rey, 2007). For Regan, it 'can in fact be alibi on the part of public power wishing to avoid the new problems brought about by the development of enormous data files' (Regan, 1995, p. 219). For example, in the 'Montreux Declaration (2005)', a reference document produced and used by privacy commissioners and privacy advocates from all over the world, there is no fundamental critique of the information society. While expressing concerns about surveillance practices, the report mentions that the development of the information society must not be hindered in any way. Even though privacy commissioners have shown an increasing concern about surveillance practices (Madrid Privacy Declaration, 2009), the global direction is still set to embed privacy within modern informational capitalism. Like the artistic critique during the 1960s and 1970s (Boltanski & Chiapello, 2005), privacy as a critique of information society has been assimilated and reshaped by and in favour of capitalist structures, notably by being over-individualized. First a political and literary critique, then defended by non-profit organizations, it is now

included in each company's policy – especially Internet giants (Bennett, 2008) – to the extent that privacy seems to have become, somehow, a consumer good (Rey, 2012, p. 158). As Kessous (2012, p. 79) suggests, the current 'sanctuarisation of privacy' (our translation) has become conditional to the well-being of the economy. Indeed, although it could be approached as a common, public, and collective value (see Regan, 1995), privacy is continuously the subject of a drive towards individualization, occurring notably through the so-called individual empowerment that lies at the very centre of the self-determination principle.

With the growth of the information society and its economical 'partner-in-crime', relationship marketing, companies will continue collecting massive amounts of data. Data mining has become more sophisticated and now allows marketers to infer significant knowledge and sensitive data about consumers from 'innocuous' raw data. This is why the debate on data protection is considered highly relevant and as the main way to protect an individual's privacy. Even the majority of most critical privacy scholars (see, e.g. Gilliom, 2011; Regan, 2011) agree that facing the lack of solutions to abuses of personal data use, the 'regime of privacy' (Bennett, 2011a) and its resources already in place must certainly still be defended. As Stalder (2011, p. 508) argues, while being very critical of the concept of privacy, 'it would be foolish to give up such resources in exchange for, well, what?'. Indeed, the history of privacy policies shows many successes in preventing the worst surveillance practices from being used (Bennett, 2011b).

However, as was also made clear in our study on loyalty programmes, privacy advocates, reflexive consumers, and consumers experiencing privacy as an everyday life experience do not share the same perspective. Aside from this empirical study, many authors have already focused on different theoretical aspects of privacy (Holvast, 2007, p. 738), which leads to different perspectives. The perception of privacy is controversial, and any attempt to provide a univocal definition of it must be considered an act of power. Because we depicted *privacy* as a tool of governance in the sole context of Swiss loyalty cards and because almost two-thirds of the interviews were conducted with women,[4] some precautions should be taken about the generalizability of our study. However, we think that our argument demonstrates at the very least that surveillance issues cannot be simplified any longer into a duality between one's privacy and surveillance systems. Broaching surveillance only in terms of privacy threat is potentially detrimental and can paradoxically reinforce it, since privacy and surveillance are not antagonistic (Stalder, 2002); rather, they seem to work together in the deployment of the surveillance society. The more that is said about privacy, the more consumers focus on their individuality, reinforcing the *care of the self*, described by Foucault (1986), which shapes them as the subjects of control.

One way to counter this tendency and to make privacy less easy to grab and control would be to pursue the work of scholars who have been trying to approach it as a common good, rather than considering it only as an individual resource to be protected against potential invasions (Regan, 1995; Westin, 2003). That might address Tocqueville's early concern expressed in the second volume of *Democracy in America* (2004). According to him, liberal societies place too much importance on intimacy and individuality, which weakens the public action that maintains common goods like freedom and democracy. Indeed, if the notion of privacy remains trapped within an individualistic perspective, it might be related to an inappropriate and over-individualized conception of freedom. Concretely, compared to the interests of a national economy or to the security of the state, privacy, as a private value, is likely to be neglected – because, as argued by Westin (2003), 'when society does not accept certain personal conduct, it is saying this is not a matter of private choice and does not allow a claim of privacy' (p. 433).[5] Privacy as an individual resource, which every individual should 'learn' to protect thanks to the self-determination principle, cannot compete with political concerns such as the wealth and security of the state. Only a conception of privacy oriented in terms of a collective good can possibly balance measures meant to serve these overwhelming interests. In other words, as argued by Regan (1995,

p. 221), privacy should not only aim to protect the individual, but also the society and its democratic values. This study aimed to demonstrate that when privacy policies are reduced to the self-determination principle, a risk is taken to shape it as a tool of power and governance. Privacy and its definition must urgently be understood as a struggle of power between the promoters of a model of informational capitalism based on surveillance of citizens and consumers, and those who would prefer to promote privacy as a common good that could lead society to more democracy and freedom. Since *Big Data* is going to be a revolution in the way we produce knowledge, make decisions, and govern people through massive data collection and analysis (Mayer-Schönberger & Cukier, 2013), the normativity of privacy we wanted to discuss in this article must be more than ever at the centre of the debates.

Notes

1. See, e.g. the Electronic Privacy Information Center & Privacy International report (2002) that distinguishes four main types of privacy: territorial, bodily, communicational, and informational.
2. See, e.g. Switzerland, article 8 of the Federal Act on Data Protection (2011).
3. This is the term used in the call centre protocol that employees follow.
4. Also, due to the fact that women were more forthcoming about privacy and because we wanted to show the most eloquent quotations in this article, almost all of them are extracted from interviews with women.
5. The Swiss data protection law, for example, states precise exceptions that allow breaches of the right to privacy.

Notes on contributor

Dr Sami Coll first got a degree in 1991 in computers and telecommunication sciences. After several years working as an engineer, he started studying sociology and finally got a Ph.D. in 2010. Then, he spent a couple of year working as a visiting research fellow at the City University of New York and at the Surveillance Studies Centre of the Queen's University in Kingston, Canada. He is currently working as a lecturer at the Department of Sociology of the University of Geneva. His main field of research is on information technologies, especially the production of massive personal data and the risks that involves for privacy and freedom.

References

Ariès, P. (1987). Pour une histoire de la vie privée. In P. Ariès & G. Duby (Eds.), *Histoire de la vie privée. De la renaissance aux lumières* (pp. 7–19). Paris: Seuil.

Bennett, C. J. (2008). *The privacy advocates: Resisting the spread of surveillance*. Cambridge, MA: MIT Press.

Bennett, C. J. (2011a). In defence of privacy: The concept and the regime. *Surveillance & Society*, *8*(4), 485–496.

Bennett, C. J. (2011b). In further defence of privacy.... *Surveillance & Society*, *8*(4), 513–516.

Boltanski, L., & Chiapello, E. (2005). *The new spirit of capitalism*. London: Verso Books.

Bozovic, M. (1995). Introduction: An utterly dark spot. In J. Bentham (Ed.), *The panopticon writings* (pp. 1–27). London: Verso.

Charmaz, K. (2011). *Constructing grounded theory: A practical guide through qualitative analysis (Repr.)*. London: Sage.

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

Coll, S. (2012a). Le marketing relationnel et le lien marchand : Le cas des cartes de fidélité suisses. In F. Cochoy (Ed.), *Du lien marchand: comment le marché fait société* (pp. 197–218). Toulouse: Presses Universitaires du Mirail.

Coll, S. (2012b). The social dynamics of secrecy: Rethinking information and privacy through Georg Simmel. *International Review of Information Ethics*, *17*, 15–20.

Coll, S. (2013). Consumption as biopower: Governing bodies with loyalty cards. *Journal of Consumer Culture*, *13*(3), 201–220.
Coll, S. (2014). *Surveiller et récompenser: Les cartes de fidélité qui nous gouvernent*. Zürich: Seismo.
Electronic Privacy Information Center & Privacy International. (2002). *Privacy and human rights 2002: An international survey of privacy laws and developments*. Washington, DC: Author.
Federal Act on Data Protection. (2011). Retrieved February 14, 2013, from http://www.admin.ch/ch/e/rs/2/235.1.en.pdf
Foucault, M. (1972). *The archaeology of knowledge*. New York, NY: Pantheon.
Foucault, M. (1978). *The history of sexuality vol. 1: An introduction*. New York, NY: Pantheon.
Foucault, M. (1979). Naissance de la biopolitique. *Annuaire du Collège de France*, *79*, 367–372.
Foucault, M. (1985). *The history of sexuality vol. 2: The use of pleasure*. New York, NY: Vintage.
Foucault, M. (1986). *The history of sexuality vol. 3: The care of the self*. New York, NY: Pantheon.
Foucault, M. (2003). *Society must be defended : Lectures at the Collège de France, 1975–76*. (D. Macey, Trans.). New York: Picador.
Foucault, M. (2008). *The birth of biopolitics: Lectures at the College de France, 1978–1979* (1st ed.). Basingstoke, NY: Palgrave Macmillan.
Gilliom, J. (2001). *Overseers of the poor: Surveillance, resistance, and the limits of privacy*. Chicago, IL: University of Chicago Press.
Gilliom, J. (2011). A response to Bennett's 'in defence of privacy.' *Surveillance & Society*, *8*(4), 500–504.
Gilliom, J., & Monahan, T. (2012). *SuperVision: An introduction to the surveillance society*. Chicago, IL: University of Chicago Press.
Holvast, J. (2007). History of privacy. In K. M. M. de Leeuw & J. Bergstra (Eds.), *The history of information security: A comprehensive handbook* (pp. 737–770). Amsterdam: Elsevier.
Jourard, S. (1966). Some psychological aspects of privacy. *Law and Contemporary Problems*, *31*(2), 307–318.
Kessous, E. (2012). *L'attention au monde: Sociologie des données personnelles à l'ère numérique*. Paris: Armand Colin.
Kessous, E., & Rey, B. (2007, September). *Les traces d'attention entre captation et opportunité. La production conjointe du marché, des services et de la vie privée*. In Actes de la conférence RESER, Tampere, Finland.
Lyon, D. (2007). *Surveillance studies: An overview*. Cambridge: Polity Press.
Madrid Privacy Declaration. (2009). Retrieved February 14, 2013 from http://thepublicvoice.org/madrid-declaration
Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, *15*(4), 336–355.
Mayer-Schönberger, V., & Cukier, K. (2013). *Big data: A revolution that will transform how we live, work, and think*. Boston, MA: Houghton Mifflin Harcourt.
Metzger, M. J. (2006). Effects of site, vendor, and consumer characteristics on web site trust and disclosure. *Communication Research*, *33*(3), 155–179.
Millar, J. (2009). Core privacy: A problem for predictive data mining. In I. Kerr, C. Lucock, & V. Steeves (Eds.), *Lessons from the identity trail: Anonymity, privacy and identity in a networked society* (pp. 103–119). New York, NY: Oxford University Press.
Monahan, T. (Ed.). (2006). *Surveillance and security: Technological politics and power in everyday life*. New York, NY: Routledge.
Montreux Declaration. (2005). *The protection of personal data and privacy in a globalised world: A universal right respecting diversities*. Retrieved November 15, 2013, from http://www.privacyconference2005.org/fileadmin/PDF/montreux_declaration_e.pdf
Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford, CA: Stanford University Press.
Orwell, G. (1949). *Nineteen eighty-four*. London: Secker & Warburg.
Pridmore, J. H. (2008). *Loyal subjects?: Consumer surveillance in the personal information economy*. Kingston: Department of Sociology, Queens University.
Prost, A. (1999). Frontières et espaces du privé. In P. Ariès & G. Duby (Eds.), *Histoire de la vie privée. De la première Guerre mondiale à nos jours* (pp. 13–132). Paris: Le Seuil.
Regan, P. M. (1995). *Legislating privacy*. Chapel Hill: The University of North Carolina Press.
Regan, P. M. (2003). Privacy and commercial use of personal data: Policy developments in the United States. *Journal of Contingencies and Crisis Management*, *11*(1), 12–18.
Regan, P. M. (2011). Response to Bennett: Also in defence of privacy. *Surveillance & Society*, *8*(4), 497–499.
Rey, B. (2012). *La vie privée à l'ère du numérique*. Cachan: Lavoisier.

Ruebhausen, O. M., & Brim, O. G. (1965). Privacy and behavioral research. *Columbia Law Review*, *65*(7), 1184–1211.
Simitis, S. (1987). Reviewing privacy in the information society. *University of Pennsylvania Law Review*, *135*(3), 707–746.
Solove, D. J. (2008). *Understanding privacy.* Cambridge, MA: Harvard University Press.
Stalder, F. (2002). Opinion. Privacy is not the antidote to surveillance. *Surveillance & Society*, *1*(1), 120–124.
Stalder, F. (2011). Autonomy beyond privacy? A rejoinder to Bennett. *Surveillance & Society*, *8*(4), 508–512.
Steeves, V. (2009). Data protection versus privacy: Lessons from Facebook's Beacon. In D. Matheson (Ed.), *The contours of privacy* (pp. 183–196). Newcastle upon Tyne: Cambridge Scholars Press.
Tavani, H. T. (1999). KDD, data mining, and the challenge for normative privacy. *Ethics and Information Technology*, *1*(4), 265–273.
Tocqueville, A. de. (2004). *Democracy in America*. New York, NY: Library of America.
Westin, A. F. (1967). *Privacy and freedom*. New York, NY: Atheneum.
Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of Social Issues*, *59*(2), 431–453.