Organizational Dynamics, Vol. 36, No. 2, pp. 217–229, 2007

www.organizational-dynamics.com
ISSN 0090-2616/$ – see frontmatter
doi:10.1016/j.orgdyn.2007.03.008

Radio Frequency Identification and the Ethics of Privacy

PHILIP L. COCHRAN MOHAN V. TATIKONDA
JULIE MANNING MAGID

Your bank account, your health record, your genetic code, your personal and shopping habits and sexual interests are your own business.

William Safire, editorial columnist, *New York Times* (see Safire (1999))

You have zero privacy anyway. . .get over it.

Scott McNealy, CEO, Sun Microsystems Inc. (see Sprenger (1999))

INTRODUCTION

The concept of personal privacy is deeply ingrained in the American psyche. In the early centuries after the first European colonization of North America, the density of settlement was exceptionally low. As a result, the United States grew a unique interest in privacy that often was achieved by the simple expedient of the frontier. If one could see smoke rising from a neighbor's chimney, then it was time to move further west. Although when the founders wrote the United States Constitution they included no specific language about privacy, in recent years the U.S. Supreme Court has found a ''penumbra of privacy'' in the U.S. Constitution. This assertion reflects the American concern about privacy protections.

At one time the average U.S. citizen believed that he or she understood the limits of personal privacy. Historically, most people (unless they were celebrities) could drive down any highway, shop in any store and go to any event with little concern of recognition and no concern that their movements might be tracked. In the last few years, this largely unexamined confidence in one's personal privacy has begun to be severely tested by a wave of new technological gadgets. As anyone who has ever watched the television show ''CSI'' knows—even someone who simply carries a cell phone today can be easily tracked by the authorities. Likewise someone who uses a credit card leaves an electronic trail that records the places, dates and times of all of his or her purchases. In a similar vein, U.S. citizens are beginning to accept the fact that their vehicular movements can be tracked by increasingly ubiquitous traffic cameras. In some states, it is now legal to use traffic camera evidence as the basis for traffic tickets.

These new technologies raise important questions regarding the ethics of privacy. When is it appropriate for the state or a company to track the movements and actions of an individual? If it is appropriate, what protections should be built into such data gathering? Such questions are new to U.S. business because the technologies to track an individual are themselves new.

THE ETHICS OF PRIVACY

Although ''privacy'' can evoke significant emotion, when you question different individuals you find that their definitions of

privacy vary tremendously. In practice, defining privacy is quite difficult and often unsatisfying, in part because of disagreements about its ethical boundaries. Even in the developed Western world, there are significant differences between the U.S. and European perspectives. For example, consider the U.S. idea of privacy ethics with respect to public nudity. In the United States, pubic nudity is almost universally considered to be unethical and is thereby banned almost everywhere. Contrast this to Europe, where it is not at all uncommon to see nude sunbathers or nudity on public television.

Because there is no commonly accepted definition of privacy, philosophers find it difficult to apply traditional philosophical theories. However, there are a few papers that have attempted to examine privacy based on deontological theory, Kantian theory, integrated social contract theory or stakeholder theory. None of these approaches are widely supported by subsequent writing. As a result, many philosophers simply suggest that privacy is little more than the ''right to be left alone.'' As a result, most of the work on the ethics of privacy approaches the topic by categorizing concerns about the ethics of privacy into a set of broad categories such as physical privacy, decisional privacy (an individual's independence in making important decisions), informational privacy (an individual's ability to avoid disclosure of personal matters) and communications privacy.

This paper will examine a new and rapidly emerging technology, radio frequency identification (RFID) tags, and will discuss some of the implications of this new technology for the ethics of privacy. Although we focus primarily on informational privacy, we also examine issues of physical, decisional and communications privacy.

RFID TAGS

RFID tags are very small radio transmitters that can be put into more and more products. It is very likely that within a few years RFID tags will be virtually everywhere. Today RFID tags show up in most consumer electronics, in many items of clothing, in pets, and occasionally even in people. Tomorrow they may be in almost all items sold in the developed world. For example, the Tokyo Ubiquitous Network Project plans to install over 10,000 RFID tags and readers in the Ginza region of Tokyo. This network of RFID tags will provide information and directions to tourists in the shopping district. One can imagine a day in which every shopping center in the world is blanketed in such tags.

One way to think about RFID tags is as a replacement for bar codes. However, RFID tags pose both substantial advantages over bar codes and raise significant privacy issues that are not present with bar codes. One significant difference is that RFID tags can be read from a distance, whereas bar codes need to be very close to their readers. Another major difference is that bar codes need to be in the line of sight of the reader, whereas RFID tags just need to be in the vicinity. A third difference is that the amount of information stored on an RFID tag can be orders of magnitude larger than the information that can be stored in a bar code. A final difference is that the current RFID standard allows for the unique identification of every individual product. That is, a bar code may tell the retailer that a consumer bought a box of raisin bran cereal. An RFID tag could tell the retailer which unique box of raisin bran the consumer bought. The retailer or manufacturer then could determine where on the shelf that box was located, when it was manufactured, where the ingredients came from, etc. If the consumer who purchased the raisin bran used a store discount card, then the retailer and manufacturer could know who bought that particular box and link that to many personal details about the consumer.

RFID tags are the vanguard of what many are calling ''pervasive computing.'' Pervasive computing occurs where computers and computing power are ubiquitous. Some commentators suggest that we are entering an era of an ''Internet of things'' in which virtually everything in the world will be tagged and tracked. Even today, an

amazingly wide range of things – ranging from redwood trees to cats – are currently tagged with RFID tags.

From the perspective of business, RFID holds the promise of becoming one of the truly ''disruptive'' technologies of this new century. Earlier disruptive technologies included such devices as the automobile, the telephone, the microwave oven and the computer. Such new technologies ultimately reshape the way in which individuals work and live as well as the ways that organizations are designed and function. They also hold the promise of reshaping our notions of ethical behavior as well as the legal structure necessary for a society to function.

Retailers such as Wal-Mart Stores are currently saving hundreds of millions to billions of dollars through a more efficient inventory management process. Some estimate that Wal-Mart has reduced its out-of-stock situations by 30 percent since it began implementing RFID tracking. With RFID tags retailers can know in real-time the location of their entire inventory, as well as the speed that it is moving though their supply chain. RFID tags can reduce employee theft, make routings more efficient and significantly reduce costs. This allows firms to fine-tune inventory levels, order more economical quantities and better track consumer tastes.

Current RFID tags range in size from quite large tags that are the size of a brick to the size most often seen by consumer, about that of a grain of rice. Today's smallest RFID tags are about 0.3 mm in width—the size of a pencil tip. Future RFID tags hold the promise of being even smaller; some have suggested that RFID tags smaller than a grain of sand are likely in the near future.

RFID tags fall into two broad categories. Active tags tend to be large and include a battery. These can generally be read from a greater distance than can passive tags. Some active tags can be read at a distance of hundreds of meters. For example, active tags can be used to identify railroad cars passing a certain point, or automobiles going through an automated toll booth. Passive tags contain no battery. They can transmit data only when electromagnetically powered by a nearby reader. Passive tags are considerably smaller and less expensive than active tags. These are used for such uses as retail checkout.

The price of RFID tags continues to fall. The average price of a consumer level tag (that is, a tag that is used only once) is currently around 20 cents and likely to fall to five cents within the next few years. Such tags uniquely identify a specific item. Some industry observers are suggesting that the prices of such tags could eventually fall to less than one cent per tag. As the price of these tags fall, their potential uses grow exponentially. Today it generally makes little economic sense to tag objects worth only a few dollars. However, as the cost falls we can expect to see wider adoption of this technology. If the price of RFID tags falls to less than a penny a tag, it may be economically worthwhile to tag nearly every item in a retail store.

RFID tags can be placed into a wide variety of objects for a range of different reasons. One area that attracted some attention in the last year was the use of RFID tags in credit cards. Today there are over 11 million RFID enabled (''no swipe'') Mastercards in consumers' wallets and purses. In 2005, American Express Co. began adding RFID transponders to all their new ''Blue'' credit cards. Such cards allow the consumer to simply tap the reader with their card instead of swiping it through a reader. This has the advantage for the consumer of a slightly faster checkout.

RFID tags are increasingly being used in passports as part of the effort to increase border security. Today a few countries have RFID-tagged passports. Within a few years any country wishing to participate in the U.S. visa waiver program will have to include such tags in their passports. RFID tags have been embedded in some new passports issued by the United States beginning in August 2006. Due to privacy concerns, these new RFID-enabled U.S. passports now have a thin layer of foil embedded in the cover to prevent the tags from being read while closed. However, passports from other countries, such as Ireland, do not have such secur-

ity protection and are thus more vulnerable to being ''skimmed'' from a distance.

Small passive RFID tags are increasingly being sewn into clothing. This has many advantages for the retailer. These advantages accrue in both the back-of-the-store operations that deal with inventory tracking and control and in the checkout phase. If the tags are not deactivated at the point of purchase, they can be used to help prevent fraudulent returns. In this case the database will ''know'' who purchased a particular item of clothing, when and at what retail outlet. Interestingly, such tags are also being marketed as a way of combating counterfeiting of various consumer goods such as expensive clothes. On the consumer side they are being marketed as a means of preventing in-home child abductions as well as to alert parents when children move about the house and to set off an alarm if they should leave the house at night.

There are persistent rumors that the European Union is considering weaving very thin threads containing inexpensive RFID tags into at least the larger-denomination Euro notes in order to curb counterfeiting and money laundering. At this time there has been no confirmation that the EU is seriously considering such a move, but given even the current direction of the evolution of RFID technology the possibility of doing so certainly exists.

ETHICAL CONCERNS ABOUT RFID TAGS

Because RFID tags can be read at a distance and because they can contain much more information than just the generic information on a barcode, privacy advocates have begun raising alarms. Firms that do not take appropriate measures today could inadvertently allow their customers to be tracked. If firms ignore such growing ethical concerns there could easily be a public backlash. Such a public backlash could lead to increased regulation and legislation that could literally cripple the industry – particularly by obviating the expensive technology already installed.

For example, although the new United States RFID passports were designed to be unreadable from distances greater than 4 inches, one recent test demonstrated that it is possible to read the data in these passports when they are opened from distances of at least 30 feet. This means that there is a possibility that the data could be ''skimmed'' by a determined criminal or terrorist nearby. Such skimming could also occur at anytime the passport is used for identification purposes, for example, in a retail establishment. Although this problem could be largely solved by encrypting the data, no decision to this effect has yet been made. This is a potentially serious flaw, since the new passport standard mandates that the information on such passports include biometric data.

The same potential problem exists with RFID-enabled credit cards. Unless one's wallet or purse has a foil lining, it is possible for a determined and knowledgeable hacker to read the full RFID tag on a credit card from as far as 30 feet. In either case, once the data has been read it is then possible to ''clone'' the passport or the credit card. Once cloned, the data could then be downloaded into a new passport or credit card, which would appear to an RFID reader to be identical to the original.

The ethical concerns about RFID tags in clothes are different in character, in that they raise a range of unsettling tracking possibilities. For example, if a consumer were wearing expensive shoes, suit, shirt, tie, etc. and each of these items held a live RFID tag, then this consumer could be profiled the moment he entered a store that has an RFID reader embedded in the doorframe. Hypothetically, the store computers could calculate the value of the consumer goods he was wearing and perhaps even the status level of his RFID credit cards (that is whether they were ''gold,'' ''platinum'' or even ''black'' credit cards). The store could then determine how to treat this consumer. One could extend this scenario even further. Since RFID tags are unique, it would be theoretically possible to

know where and when the consumer bought each item on his body. That information might then be combined with other databases to learn his name, phone number, home address, credit rating, debt, education level, marital status, criminal history, and so on.

This illustrates two key issues. First, it is not the tracking of an object itself, but rather a person's interaction with and use of the object, that raises the most concerns. When a person interacts with an RFID-tagged object, or when the person effectively becomes an RFID-tagged object, then that person's locations, actions and behaviors can be identified, tracked and compiled. Second, each firm may develop a database containing such information. The aggregation and integration of disparate databases across firms and organizations raises, to some, the greatest fears about the potential invasion of personal privacy.

In a geographic area awash with RFID readers, nearly every person passing through could be uniquely identified and tracked. His or her shopping patterns could be stored and analyzed. This would be similar to Amazon.com's ''recommendation service'' which looks at an individual's purchasing and even browsing habits and eerily suggests products that are often of interest. However, many of Amazon's shoppers find this recommendation service to be ''creepy.'' One wonders how they would react to an RFID-based system that would have the possibility of being many orders of magnitude more intrusive.

PUBLIC PERCEPTIONS OF PRIVACY

Public perceptions of whether or not a new technology poses an ethical threat to privacy can be very important to whether any new technology is eventually widely adopted. A recent analogous example is Monsanto's experience with genetically altered foods. Although there has been only minor resistance to genetically modified organisms (GMO) in the U.S., the backlash in Europe has been substantial. In Europe genetically modified food is often called ''Frankenfood.'' Most European countries now ban GMO. Monsanto has lost billions of dollars due to this largely unexpected backlash.

The ethical concerns about the impact of RFID tags on privacy could be similarly destructive to firms involved with this emerging technology. Unfortunately, in today's business world concerns about the ethics of privacy are not even on the radar screen of most senior managers. Indeed, most business people and RFID supporters argue that firms need to know more and more about their customers' characteristics, behaviors, preferences and needs. Given the value and ease of gathering and aggregating such information there will be a very strong temptation to do so once the technology is in place.

In general, firms prefer to gather more, rather than less, data about their customers. This is done to better understand the customers and to collect valuable consumer information that may be acted on by that firm and/or shared with other parties. Given the substantial value of gathering and aggregating such information, there will be a very strong temptation to do so once this technology is in place.

On the other hand, individuals generally prefer to provide less personal data. They do this in order to attempt to preserve anonymity or ''a sense of self,'' to avoid price or other forms of discrimination, and to maintain personal security and reduce potential future harm arising from the firm's use and transfer to third parties of the specific personal data. Fortunately, as we explain later in the paper, there is a range of mechanisms which firms may employ to better respect these customer concerns and to provide fair incentives for customer disclosure of personal information.

Managers need to be aware of the ethical concerns raised by such tracking technologies, because they would prefer to prevent a large-scale consumer backlash that could result in government regulation constraining the value of the technology. For example, in 2004, the California legislature considered a

bill that would have prevented any private entity from using RFID tags attached to consumer products that could be used to identify a specific individual, unless that entity met certain conditions. Although this bill passed overwhelmingly in the California State Senate, it failed to reach the floor of the State Assembly. Nonetheless, the extent to which it progressed is notable given the nascent nature of the technology. This example should give managers pause about the future of this technology. By not taking into account the public's ethical concerns about RFID and related technologies, there is always the potential that strict legislation will be passed that reduces the use of the technology and requires firms to revamp their technology infrastructures (causing a significant loss of installed technology and other organizational investments).

The serious ethical issues raised by the increasingly intrusive use of RFID technology are likely to become omnipresent as society evolves into the era of pervasive computing. We believe the time has come for managers to add concern about the ethics of privacy to the list of variables they consider as part of the adoption of new technologies. The focus on the ethics of privacy may be an effective strategic variable in the strategy portfolio. As a result, managers need a deeper conceptual understanding of the ethics of privacy.

PRIVACY MOTIVATIONS

It is necessary to differentiate the motivations for maintaining privacy from the actual practice of maintaining privacy. An individual may choose not to disclose certain personal information due to shyness, embarrassment or concern about potential resulting harms. Or the individual may choose not to disclose certain information because she knows that that information has economic value to some other party, and so waits until another party offers sufficient compensation for that information. In these examples, the mechanisms for maintaining privacy may well be the same, but the motivations are notably different. In the first example, the personal information has internal value to the individual, so much so that she might pay someone to leave that information alone. In the second example, the personal information (e.g., the individual's preference for automotive make and color) has external value, and she might let others compensate her to obtain that information.

Curiously, privacy is not always seen favorably. Some view privacy positively because it can protect individuals and allows the functioning of a free society. Others view privacy negatively because any privacy impedes the free flow of information, increases search costs in economic transactions, and makes markets less efficient. Some economists even equate ''privacy'' with ''secrecy'' and all its concomitant negative connotations. Some argue that maintaining privacy can allow negative outcomes, including personal misrepresentations, morally questionable behavior and illegal activities, while giving up privacy can allow positive outcomes, including richer customer-supplier relationships and improved service.

On the recipient side, the information acquisition can be overt (explicit and apparent to the individual, as occurs when filling out a registration form) or covert (e.g., surreptitious monitoring, where the individual is not notified in advance about the information collection activity). Intermediate forms exist as well. For example, whereas many individuals react very negatively to the possibility of surreptitious video monitoring (such as through a pinhole in a wall or ceiling) the same people are essentially indifferent to rapid proliferation of obvious cameras in public places such as street corners and in crime-troubled neighborhoods. In fact, it is altogether possible that a particular individual could be outraged by hidden cameras and lobby for overt cameras.

It is important to recognize that not all information is equally private, nor do different individuals treat similar information as

having the same level of privacy. An individual might care more, or less, about privacy in different settings and at different times in life and society. And how people treat their own personal information can be quite different from how they treat and place importance on someone else's personal information.

COMMUNICATIONS PRIVACY MANAGEMENT

One way to approach the ethics of privacy is to use a rule-based theory for coordinating disclosure of personal information. In her recent book, Dr. Sandra Petronio offers an important framework for understanding privacy and how it applies to individuals' decisions to disclose personal information. Her evidenced-based theory, Communications Privacy Management (CPM) focuses on privacy and disclosure as coordinated efforts rather than opposing conditions. Individuals may choose to share personal information, but may also expect that the information shared will remain private among those to whom it is disclosed. When information is disclosed, the recipient does not acquire full control over the information. Reporting personal information is not an all-or-nothing proposition, but instead is an effort to co-manage information with various individuals and groups.

Disclosure of personal information is necessary for any number of reasons – to build a relationship, learn more information, or function within a group dynamic – but the disclosure does not end the individuals' right to manage their personal information. Instead, those receiving the information now are linked to the discloser and must manage the information appropriately. We know this intuitively. When someone shares personal information (such as when confiding to a colleague that she plans to resign from her job in two weeks), the recipient of this information is not free to share this announcement, but must use discretion in guarding the information until the discloser makes a general announcement.

According to Petronio, the ownership lines of personal information can be seen as a boundary. Each person operates by keeping personal information within their boundaries. These boundaries may be permeable or impermeable. One individual's privacy boundaries may overlap with other individuals' privacy boundaries. These interpenetrating regimes represent disclosure. Disclosure of personal information does not remove it from the discloser's boundary, but instead creates an overlap with those to whom it is disclosed. Boundary overlaps are multiple in nature because each person manages a multitude of information over which a degree of control is necessary so that it remains within privacy boundaries and does not move to public information.

CPM is a rule-based system that explains the management of boundaries. Individuals use rules to manage access to their personal information. The rules allow differing degrees of access to personal information. How the recipient and discloser coordinate the boundaries depends on a number of rules. Rules are developed based on five decisional criteria: cultural norms into which people are socialized, gendered differences (similar to cultural socialization but gender related), motivations for disclosure (encompasses a variety of factors), context of the disclosure (both in terms of social environment and physical setting), and risk-benefit analysis. Although these criteria form the basis for establishing rules to balance disclosure and privacy, they are not static.

Rules are formulated based on these five decisional criteria. However, after these rules are formulated, they have two additional dimensions. The first dimension is the way individuals acquire rules. Learning the rules for managing personal information typically involves socialization (such as a family rule not to discuss finances or a firm's rules for training employees) or negotiations (including the explicit ''don't tell anyone I told you,'' and the implicit ''should we tell the boss about the error?''). Rules develop different properties over time to help an individual manage the multitude of personal informa-

tion disclosures. Thus, some rules are very stable and become a routine (e.g., keeping a firm's trade secrets) or represent an overall privacy orientation, as might be the case for an individual socialized in a family where financial information was not openly discussed. New situations or events, such as a fire in a factory or traveling to conduct business in another country, may trigger new rules or a change in existing rules. As co-owners of information negotiate their shared boundaries, positive or negative sanctions reinforce the group privacy management rules.

Individuals constantly coordinate privacy boundaries that include concealed information, co-owned information (whether such information was obtained accidentally or formally) and shared information within a number of groups such as family relationships, professional associations and community. Permeability of boundaries refers to the degree of access individuals have to the information. Thick walls of a boundary mean that the information is controlled tightly. That does not mean it is kept a secret. For instance, a personal health issue that an individual generally wants to conceal is often freely discussed with selected extended-family members. These family members become confidants and now have a responsibility to keep the information private and must also engage in boundary coordination. CPM posits that groups or individuals that solicit disclosure of personal information are brought inside a boundary of co-ownership with specific obligations related to managing the information.

CLASHES OVER PRIVACY

Not surprisingly, then, throughout the boundary coordination process, there are clashes about privacy management. According to Petronio, these clashes can be seen as a form of boundary turbulence. Turbulence occurs for a variety of reasons, both intentional and through mistakes or errors. Fuzzy boundaries result when ownership of personal information is unclear. Such ownership confusion is becoming more problematic, because personal information is increasingly available through technologies, including RFID and other pervasive computing technologies. The problem of availability of information is magnified by two factors. First, there is an incorrect presumption that access to personal information equals the right to control the information. CPM maintains that ownership of personal information is not wholly transferred through disclosure. Second, there is an incongruity of access. Individuals' sense of privacy is disturbed when others are able to obtain information about them with ease, despite an individual controlling the information tightly, and use the information without regard for the established rules, such as when social security numbers are stolen by computer hackers and used for consumer credit transactions.

The coordination process breaks down when there is disagreement over information ownership. Further advancements in technology offer opportunities to undermine privacy boundaries or gain in privacy protection. It becomes increasingly important to understand where these boundaries are drawn, how to protect and solve ownership issues and to learn how people manage personal information.

CPM offers interesting insights concerning the ethics of privacy. In particular, it presents disclosure as something other than the antithesis of privacy. Instead, disclosure requires the recipient to join the discloser in co-ownership of the information. The recipient cannot take the information and freely use it however the recipient might like. Personal information remains associated with the discloser and is meant to remain private on some level. In addition to casting disclosure in a new light, CPM explains why new technology like RFID tags contribute to fuzzy boundaries and, hence, boundary turbulence. Technology increasingly presents ownership issues. Finally, CPM offers insight into individuals' expectations about privacy management based on established rules.

IMPLICATIONS FOR BUSINESS

The Fair Information Practice Principles (FIPP), in conjunction with the notions of CPM, can be applied to potentially privacy-invading technology such as RFID (see Table 1 for a list of the FIPP principles). We relate the experiences of the retail operations of Marks & Spencer PLC, and suggest how firms might adapt these principles to better reduce the public's concerns about the ethics of privacy.

The prevailing thought about protecting individuals from privacy intrusions is organized around the five tenets of the Fair Information Privacy Principles: notice, consent, access, security and enforcement. In seeking to limit any consumer concerns about the ethics of privacy brought on through the use of technologies such as RFID, some firms have sought to adjust their operating practices based on the FIPP tenets. An early adopter of RFID technology, the United Kingdom retailer Marks & Spencer, received a great deal of public recognition for working with privacy advocates and carefully considering principles of privacy protection while utilizing RFID for inventory and other operations efficiency gains.

Marks & Spencer wanted greater inventory accuracy and better product availability for its customers. The company began putting RFID tags at the item-level, a trial that has now expanded to all its stores. Before the trial, the retailer took many steps to ensure that the personal information of individuals was not at risk because of RFID in the stores. ''Notice'' to store customers, a crucial element of FIPP, was achieved through leaflets at all its stores explaining RFID. In addition each tag was clearly marked: ''Intelligent Label for stock control use.'' The tags only provided information about the product (color, size, style) through a unique product number. These tags are passive. After adequate notice, the customers ''consent'' to the use of RFID by remaining in the store and choosing to purchase products. If customers object to RFID, they would need to stop shopping at that retailer.

The retailer greatly limited the full use of this technology to protect its customers from unwanted privacy intrusions. The RFID application could have been far more extensive. For example, the tags are not scanned at the time of purchase; therefore no customer information is associated with the product information. No tag is hidden, and each tag is easily removed and disposed of; customers are encouraged to do so. Customers are not required to have the tag when returning a purchase. In addition, the mobile tag scan-

TABLE 1 THE FTC FAIR INFORMATION PRACTICE PRINCIPLES (FIPP)

Notice/awareness. ''Consumers should be given notice of an entity's information practices before any information is collected from them.'' The consumer must be informed of the information tracking capabilities of RFID before they are subjected to what could be considered an invasion of privacy. An example of proper notice would be signage in front of the store or labeling of products that are tagged with RFID.

Choice/consent. ''At its simplest, choice means giving consumers options as to how any personal information collected from them may be used.'' Consumers should be given the right to choose to ''opt-in,'' ''opt-out,'' or ''tailor the nature of the information they reveal and the used to which it will be put.''

Access/participation. ''[Access] refers to an individual's ability both to access data about himself or herself – i.e., to view the data in an entity's files – and to contest that data's accuracy and completeness.''

Integrity/security. ''To assure data integrity, collectors must take reasonable steps, such as using only reputable sources of data and cross-referencing data against multiple sources, providing consumer access to data, and destroying untimely data or converting it to anonymous form.''

Enforcement/redress. ''It is generally agreed that the core principles of privacy protection can only be effective if there is a mechanism in place to enforce them. Absent an enforcement and redress mechanism, a fair information practice code is merely suggestive rather than prescriptive, and does not ensure compliance with core fair information practice principles. Among the alternative enforcement approaches are industry self-regulation; legislation that would create private remedies for consumers; and/or regulatory schemes enforceable through civil and criminal sanctions.''

ners used in the stores have a much lower frequency level than those typically used in the United States, consistent with standards in Europe. The lower frequency and power limits the range for an accurate read, reducing the potential for surreptitious reading.

The Marks & Spencer RFID implementation is an excellent example of steps taken to comply with FIPP. However, we know from the discussion of CPM that simply complying with FIPP does not address the most current understanding of customer privacy. The first issue is that Marks & Spencer chose to severely curtail the use of RFID. Implementing RFID at an item-level, and then only using it for inventory control, means the retailer is not making full use of the technology in other areas such as marketing and customer service. It is not reasonable to expect all firms to invest in technology for such very limited purposes. The potential danger is that customers will assume their personal information is not impacted by this technology, and a firm that uses RFID in more applications than Marks & Spencer could experience a consumer backlash that might result in tight government control.

Even with a limited use of the technology, FIPP would still not reflect some of the most important issues associated with privacy. Recent research makes the first two principles of FIPP, notice and consent, particularly troublesome. The parameters of notice and consent were devised about the same time that economic scholars understood privacy as the concealment of information. Individuals could choose to conceal their personal information, but economists believed the best result was achieved through revealing the information so that it could flow freely. Some scholars now argue that privacy is not a unitary concept but instead needs to be viewed as a class of interests. Individuals may not be able to act rationally when making decisions about personal information. Notice to an individual that a firm is collecting information that will be used for various transactions does not take into account what some call the ''privacy market failure.'' Reasons that individuals do not act appropriately include incomplete information, bounded rationality and psychological distortions (including the desire for immediate gratification). One example is the willingness of some consumers to disclose personal information to a radio station, credit card issuer, magazine subscription company or other private entity simply in order to obtain a t-shirt or other low-value reward. Marks & Spencer avoided problems by not connecting customer information with purchases. Still, this came at the loss of greater application of, and benefits from, the technology.

Notice and consent also assumes that individuals reveal personal information and do not intend to retain some level of control over it. The CPM theory explains that recipients of personal information are not completely free to use the information. Individuals expect the recipient to co-manage information that they disclose. Simply giving consumers notice about the use of their personal information, and obtaining their consent to the immediate use as well as any future use, does not adequately address the privacy expectations held by individuals. Simply stated, notice does not equal awareness, and that choice does not equal informed consent.

The three other FIPP tenets of ''access,'' ''security'' and ''enforcement'' are addressed in CPM theory as well. CPM recognizes that advancing technology impinges on individuals' privacy. The limitations of FIPP, and even the current relative under-utilization of FIPP tenets by firms, increase the likelihood of government regulation that could increase technology costs and diminish its practical benefits.

Industry self-regulation that considers both the ongoing interest of individuals and their personal information, and the needs of industry to operate efficiently and effectively, is clearly preferable to government regulation. Marks & Spencer took individuals' privacy into account when creating policies concerning its item-level RFID tags, but as a result, the retailer adopted policies that do not make full operational use of the

technology. A future challenge is to develop models of technology use that go beyond the narrow understanding of privacy evidenced in FIPP, while allowing increased efficiency and effectiveness through the technology applications.

CONCLUSIONS

The ethics of privacy is an important but largely unexplored topic for managers. The topic is particularly pressing given RFID and other emerging technologies that have the potential to challenge society's ethical beliefs. It is time for managers to purposefully incorporate discussion of the ethics of privacy into their portfolio of strategy dimensions, and to more carefully include privacy in planning analyses. Accordingly, this paper aims to initiate a discussion of privacy and set a basis for managerial decision making. Our conclusions are:

1. Privacy is a sweeping concept. There is no one commonly accepted or understood definition of privacy. One useful way to define privacy is as ''control of personal information by the individual.''

2. Current United States federal law provides almost no restrictions on the collection and usage of consumer personal information by private firms.

3. There is no widespread legal constraint on RFID usage by United States firms at this time.

4. Multi-national firms must abide by information privacy regulations that vary considerably by country. This necessitates decisions regarding common information privacy policy and technology infrastructures.

5. The current social responsibility standard for operational practice regarding RFID and other potentially privacy-invading technology is embodied in the Fair Information Practice Principles. Although it has limitations, this is an accepted baseline policy that managers should seriously consider.

6. Individuals expect ownership or control of personal information, even after disclosing it. Firms should consider that disclosed information is still owned, controlled or shared by the individual who disclosed it.

7. Advancing technologies significantly challenge individuals' comprehension of the use of their personal information. This raises concerns about human bounded rationality and their ineffective analysis of the costs and benefits of disclosing personal information.

8. It is not the initial disclosure of personal information that is most threatening, but rather the subsequent re-use, transfer to third parties, and aggregation of that information. Firms must be very vigilant about re-using, transferring or aggregating personal information about consumers.

9. Given concerns about information transfer, bounded rationality and changing technology, there is increasing demand from a variety of parties for greater regulation of consumer information privacy. Responsible use of potentially privacy-invading technologies may prevent some regulatory actions.

SELECTED BIBLIOGRAPHY

For more information on Communications Privacy Management, see S. Petronio, *Boundaries of Privacy: Dialectics of Disclosure* (Albany: State University of New York Press, 2002). For more information on the ethics of privacy see L. D. Introna and A. Pouloudi, ''Privacy in the Information Age: Stakeholders, Interests and Values,'' *Journal of Business Ethics*, 1999, 22(1), 27–38; and K. Jackson, ''Systematizing Norms: Toward a Moral Jurisprudence Theory of Business Ethics,'' *Business Ethics Quarterly*, 2000, 10(2), 451–481.

The classic legal article on privacy is S. D. Warren and L. D. Brandeis, ''The Right to Privacy,'' *Harvard Law Review*, 1890, 4, 193–200. For an excellent look at how ethical and legal visions of privacy differ between cultures refer to J. Q. Whitman, ''The Two Western Cultures of Privacy: Dignity Versus Liberty,'' *The Yale Law Journal*, 2004, 113(6), 1151–1221. For an excellent legal perspective on privacy see P. M. Schwartz, ''Property, Privacy, and Personal Data,'' *Harvard Law Review*, 2004, 117, 2055–2128.

For information on Fair Information Practice Principle (FIPP) see: http://www.ftc.gov/reports/privacy3/fairinfo.htm.

The popular press articles on the ethics of privacy are extensive and include: S. G. Davies, ''Re-Engineering the Right to Privacy: How Privacy Has Been Transformed From a Right to a Commodity,'' in: Agre and Rotenberg (Ed.), *Technology and Privacy: The New Landscape* (MIT Press, 1997, 143–166); R. A. Fusaro, ''None of Our Business?'' *Harvard Business Review*, December 2004, 33–44; R. Want, ''RFID: A Key to Automating Everything,'' *Scientific American*, January 2004, 56–65; P. Sprenger, ''Sun on Privacy: 'Get Over It','' *Wired News*, January 26, 1999 (www.wired.com).

Philip L. Cochran is a professor of management in the Kelley School of Business at Indiana University, Indianapolis, IN 46202, U.S.A. He is also a professor of philanthropic studies at the Center on Philanthropy at Indiana University. He holds the Thomas W. Binford Chair in Corporate Citizenship and is director of the Randall L. Tobias Center for Leadership Excellence. He is past chair of the Social Issues in Management Division of the Academy of Management and was the first president of the International Association for Business and Society. He has taught and lectured extensively in North America, Europe and Asia (Tel.: +1 317 274 4179; e-mail: plcochra@iu.edu).

Mohan V. Tatikonda is an associate professor of operations and technology management in the Kelley School of Business at Indiana University, Indianapolis, IN 46202, U.S.A. His research focuses on product and service innovation, advanced technology, six-sigma processes and supply chain management. He has consulted for The World Bank, SAP and other organizations, and served on the faculty at the University of North Carolina and Boston University (Tel.: +1 317 274 2751; e-mail: tatikond@iu.edu).

Julie Manning Magid is an associate professor of business law in the Kelley School of Business at Indiana University, Indianapolis, IN 46202, U.S.A. Her primary areas of research include legal empiricism, employment law and emerging technology with a particular interest in interdisciplinary approaches to these issues (Tel.: +1 317 274 2275; e-mail: jmagid@iu.edu).