Radio Frequency Identification and Privacy Law: An Integrative Approach

Julie Manning Magid, Mohan V. Tatikonda,** and Philip L. Cochran****

I. INTRODUCTION

The indiscriminate nature of Radio Frequency Identification (RFID)[1] technology creates unique privacy issues.[2] Currently privacy standards for the type of information gathered through RFID and the use of that information do not exist.[3] With few exceptions, compatible readers may legally access from a remote location RFID devices and the information these devices contain. After gathering information, the legal uses of that information are innumerable in terms of aggregation and re-use.

*Associate Professor of Business Law, Indiana University, Kelley School of Business.

**Associate Professor of Operations Management, Indiana University, Kelley School of Business.

***Thomas W. Binford Chair of Corporate Citizenship and Professor of Management, Indiana University, Kelley School of Business.

The authors thank Candice L. Graham for her outstanding research assistance.

[1] Radio Frequency Identification refers to technology contained in a number of devices with the ability to transmit identifying information wirelessly, such as medical implants in a person, prescription drugs carried by that person, and the clothing the person is wearing. *See* Ari Juels, *RFID Privacy: A Technical Primer for the Non-Technical Reader*, *in* PRIVACY AND TECHNOLOGIES OF IDENTITY: A CROSS-DISCIPLINARY CONVERSATION 57, 60 (Katherine Strandburg & Daniela Stan Raicu, eds., 2006). For further discussion of RFID and its application, see generally Roy Want, *RFID: A Key to Automating Everything*, SCIENTIFIC AMERICAN MAGAZINE, Jan. 2004, at 56.

[2] Randal Jackson, *"Promiscuous" RFID a Data Threat, Warns Privacy Watchdog*, COMPUTERWORLD, Sept. 3, 2007, http://computerworld.co.nz/news.nsf/news/D83E8424E8F435F6CC2573470082076B.

[3] Catherine Rampell, *Google Calls for International Standards on Internet Privacy*, WASH. POST, Sept. 15, 2007, at D01 (noting that critic Marc Rotenberg of the Electronic Privacy Information Center equates Google's call for privacy standards to "someone being caught for speeding saying there should be a public policy to regulate speeding"). The National Institute of Standards and Technology, a nonregulatory agency of the U.S. Department of Commerce, published technical guidelines for deploying RFID in April 2007 including security standards but noted that, "[p]rivacy considerations are interrelated with security considerations." NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, NIST SPECIAL PUBLICATION 800-98, GUIDELINES FOR SECURING RADIO FREQUENCY IDENTIFICATION (RFID) SYSTEMS: RECOMMENDATIONS OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, at 6-14 (2007), *available at* http://csrc.nist.gov/publications/nistpubs/800-98/SP800-98_RFID-2007.pdf [hereinafter NIST RFID GUIDELINES].

RFID is a part of everyday life already. Everyone has had the experience of pushing a shopping cart around a grocery store.[4] Often one has a credit card on hand at the time.[5] By doing so, personal shopping patterns and preferences may now be associated with credit information and financial data and aggregated for marketing firms interested in targeting a certain demographic. A car could have a license plate with RFID technology to track personal movements.[6] A reader may track all this information from up to 12 miles away.[7] Many individuals do not care if others obtain an infinite amount of personally identifying data through their shopping, credit, and personal travel activities; however, they provide their data free of charge and without limits on its use despite that it is a valuable asset for which businesses are presumably willing to pay. Businesses make money from collecting personal information.[8]

The indiscriminate nature of RFID technology arises from ease of access of the information in that anyone with a compatible reader can connect to RFID devices[9] found

---

[4] (Meijer promotes its use of RFID as a way to improve its understanding of the amount of time customers spend in the store and to help staff crucial areas, such as check-out lines. *See RFID News: Will RFID Tracking of Shopping Carts In-Store Add Value – or Raise More Privacy Concerns?*, SUPPLYCHAINDIGEST, Nov. 9, 2006, http://www.scdigest.com/assets/newsViews/06-11-09-1.cfm?cid=759&ctype=content. Though that raises the question of whether employees really need technology to see when check-out lines need additional staffing. *Id.* ("We can't help but think Meijer is at least considering the possibility for additional intelligence as a potential benefit of the technology, available for the price of a few more readers.").

[5] Frequently, such credit cards are "no-swipe," enabled with an RFID microchip. This has raised serious privacy concerns for some. despite credit card companies' claims that information is encrypted, researchers ran tests on 20 different major credit cards using a device "cobbled together from readily available computer and radio components" and were able to obtain the cardholder's name, card number and expiration date. This information can be read through a wallet or item of clothing. *See* John Schwartz, *Researchers See Privacy Pitfalls in No-Swipe Credit Cards*, N.Y. TIMES, Oct. 23, 2006, at C1; *see also* Shane L. Smith, *Gone in a Blink: The Overlooked Privacy Problems Caused by Contactless Payment Systems*, 11 MARQ. INTELL. PROP. L. REV. 213, 259 (2007) ("[M]erely emblazoning a logo on contactless payment devices to allow users to get comfortable with an RFID-enabled microchip's presence does nothing to protect individuals' privacy.").

[6] *Tagged License Plates in the UK*, RFID NEWS, Aug. 9, 2005, http://www.rfidnews.org/weblog/2005/08/09/tagged-license-plates-in-the-uk. *See also* Benjamin Burnham, Comment, *Hitching a Ride: Every Time You Take a Drive, The Government is Riding With You*, 39 J. MARSHALL L. REV. 1499, 1500-02 (2006); Manoj Govindaiah, *Driver Licensing Under the REAL ID Act: Can Current Technology Balance Security and Privacy?*, 2006 U. ILL. J.L. TECH. & POL'Y 201, 206-09 (2006).

[7] Claire Swedberg, *Gentag to Commercialize Super RFID Technology*, RFID JOURNAL, Sept. 12, 2007, http://www.rfidjournal.com/article/articleview/3610.

[8] For example, start-up companies are building services that specialize in tracking people and their reputations using information found on MySpace, Amazon.com's Wishlists, and Facebook. They then sell the profiles to other companies for marketing and sales purposes. Heather Green, *It Isn't Just YourSpace Anymore*, BUSINESSWEEK, Sept. 24, 2007, a 13.

[9] Jackson, *supra* note 2.

in clothes, humans, animals, and an array of individual products,[10] including prescription medicine.[11] However, the proliferation of uses for RFID technology, with its vast informational capacity and no universal standard for privacy protection, contributes to the promiscuity.[12]

RFID holds great promise as a "disruptive" technology that will reshape the way individuals live.[13] The privacy concerns addressed here apply to data collected by RFID in particular, but also other indiscriminate technologies that are similarly disruptive. Already businesses successfully and conscientiously utilize disruptive technology in areas such as inventory control. As an early adopter of RFID, the United Kingdom retailer Marks & Spencer, received a great deal of public recognition for working with privacy advocates[14] and carefully considering principles of privacy protection while utilizing RFID for inventory and other operations efficiency gains.[15]

Prior to the introduction of RFID tags Marks & Spencer checked inventory the old fashioned way, by employing people to count and record all the unsold goods in its stores and warehouses and then checking counts against inventory records. With the advent of RFID, Marks & Spencer adopted real time inventory control. It began putting RFID tags

---

[10] Todd Lewan, *Microchip Implants Raise Privacy Concerns*, WASHINGTON POST, July 21, 2007, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2007/07/21/AR2007072100637.html.

[11] Bob Brewin, *FDA Backs RFID Tags for Tracking Prescription Drugs*, COMPUTERWORLD, Feb. 23, 2004, http://www.computerworld.com/industrytopics/healthcare/story/0,10801,90368,00.html. *See also* Bryan A. Liang, *Structurally Sophisticated or Lamentably Limited? Mechanisms to Ensure Safety of the Medicine Supply*, 16 ALB. L.J. SCI. & TECH. 483, 485 (2006); Suchira Ghosh, Note, *The R.F.I.D. Act of 2006 and E-Pedigrees: Tackling the Problem of Counterfeit Drugs in the United States Wholesale Industry*, 13 MICH. TELECOMM. TECH. L. REV. 577, 578 (2007).

[12] NIST RFID GUIDELINES, *supra* note 3, at 2-5 ("For most applications, the increased speed and operating range are considered advantages. One exception is applications for which security or privacy is a significant concern, such as those that involve financial transactions or personal data.").

[13] *See* Philip Cochran, Mohan Tatikonda & Julie Manning Magid, *Radio Frequency Identification and the Ethics of Privacy*, 36:2 ORG. DYNAMICS 217, 219 (2007) ("Such new technologies ultimately reshape the way in which individuals work and live as well as the ways that organizations are designed and function.").

[14] The two major privacy advocate organizations challenging business' adoption of RFID technology are Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN) and Privacy Rights Clearinghouse, although there are many other privacy advocacy groups and sponsors involved in the use of RFID and related technologies. *See, e.g.*, Privacy Rights Clearinghouse, *RFID Position Statement of Consumer Privacy and Civil Liberties Organizations* (Nov. 20, 2003), http://www.privacyrights.org/ar/RFIDposition.htm ("Radio Frequency Identification (RFID) is an item-tagging technology with profound societal implications. Used improperly, RFID has the potential to jeopardize consumer privacy, reduce or eliminate purchasing anonymity, and threaten civil liberties.").

[15] As a United Kingdom retailer, Marks & Spencer is subject to European Union privacy laws, including the Data Privacy Directive, Council Directive 95/46, 1995 O.J. (L 281) 31 (EU). We use the Marks & Spencer example only insofar as the retailer worked with privacy advocates championing the Fair Information Privacy Principles to protect personal privacy. For further discussion of the European Union privacy perspective, *see infra* notes 91-95 and text accompanying.

at the item-level; a trial that expanded to all its stores.[16] However, the retailer took many steps to ensure that the personal information of individuals was not at risk because of RFID in the stores.[17] It provided notice to store customers by distributing leaflets explaining RFID and marking each tag "Intelligent Label for stock control use."[18] The tags only provided information about the product (color, size, style, etc.) through a unique product number.[19] The RFID tags were passive so they emitted no signal and presented no health risks to the customers.[20]

To protect consumer privacy, Marks & Spencer took care to comply with the voluntary guidelines known generally as the Fair Information Practice Principles (FIPP).[21] Nonetheless, several practical issues arose. The first issue was that Marks & Spencer chose to curtail severely the use of RFID. Implementing RFID at the 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.[22] It is not reasonable to expect all firms to invest in this type of technology for very limited purposes.[23] Retailers employing inconsistent standards for their use of RFID may result

---

[16] *Marks & Spencer RFID Expansion Tackles Privacy Issue*, RFID UPDATE: THE RFID INDUSTRY DAILY, Feb. 28, 2005, http://www.rfidupdate.com/articles/index.php?id=789.

[17] *Id.*

[18] *Id.* ("But perhaps the most impressive component of the Marks & Spencer RFID trial expansion is the forthcoming approach it will take with customers: leaflets explaining RFID technology and Marks & Spencer's use thereof will be available at all 53 stores.").

[19] Andy McCue, *Marks & Spencer Tags Shirts with RFID*, SILICON.COM, Oct. 17, 2003, http://news.zdnet.co.uk/hardware/emergingtech/0,39020357,39117192,00.htm.

[20] Will Hadfield, *Marks & Spencer Expands RFID Trial as it Moves Closer to Decision Over Full Roll-out*, COMPUTERWEEKLY.COM, April 4, 2006, http://www.computerweekly.com/Articles/2006/04/04/215168/marks-spencer-expands-rfid-trial-as-it-moves-closer-to-decision-over-full.htm (noting that the passive tags require shop assistants to trigger reading device).

[21] Federal Trade Commission, *Fair Information Practice Principles*, http://www.ftc.gov/reports/privacy3/fairinfo.htm ("[The] five core principles of privacy protection [are]: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress."). See *infra* Part II.C.3 for additional discussion of FIPP.

[22] *But see Marks & Spencer RFID Expansion Tackles Privacy Issue*, RFID UPDATE: THE RFID INDUSTRY DAILY, Feb. 28, 2005, http://www.rfidupdate.com/articles/index.php?id=789 ("Folks, take note. This is how it should be done. Marks & Spencer has taken into account and balanced its own interests with those of consumer privacy groups, and it has crafted a program that respects the customer while reaping the benefits of item-level RFID tagging.").

[23] *See, e.g.*, Carol Sliwa, *Suppliers Eye RFID Data, Search for Potential Uses*, COMPUTERWORLD, March 7, 2005, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=100221 (discussing Wal-Mart's implementation of RFID).

in consumer backlash and tight government control that impact all potential users and uses of RFID.[24]

Even with a limited use of the technology, FIPP is an outdated view of privacy for advanced technology such as RFID. Apparently, the supposition made by Marks & Spencer is that, 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 must stop shopping at that retailer. Research does not support this supposition.[25]

The first two principles of FIPP, notice and consent, particularly rely on questionable assumptions. The parameters of notice and consent were devised about the same time that economic theory understood privacy as concealing information.[26] 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.[27] Economics now understands privacy more broadly as a class of interests.[28] Individuals are unlikely to act rationally when making decisions about privacy sensitive information.[29] Notice to an individual that a firm is collecting information that will be used for various transactions does not take into account privacy market failure.[30] Reasons that individuals do not act appropriately include incomplete information, bounded rationality, and psychological distortions (including the desire for immediate gratification).[31] Marks & Spencer avoided this problem by not connecting customer information with purchases.[32] Still, this came at the loss of greater application of, and benefits from, the technology.

---

[24] *See Customers to Retailers: Take Us Seriously*, CIO MAGAZINE, Dec 1, 2003, at 87 ("If retailers fail to consider these concerns, they may end up wasting money on pilots and deployments if legislation passes preventing item-level tagging. However, if retailers take these issues seriously, they'll reduce the risk of the government banning item-level RFID. . . .").

[25] *See infra* Part IV.

[26] *See* George J. Stigler, *An Introduction to Privacy in Economics and Politics*, 9 J. LEGAL STUD. 623, 624 (1980).

[27] *See* George J. Stigler, *The Economics of Information*, 69 J. POL. ECON. 213, 213-225 (1961) (the seminal article on information costs); *see also* Michael E. Staten & Fred H. Cate, *The Impact of Opt-In Privacy Rules on Retail Credit Markets: A Case Study of MBNA*, 52 DUKE L.J. 745, 746 (2003) ("Economists have long recognized that the costs of acquiring information and arranging transactions are like sand in the gears of commerce.").

[28] *See* Alessandro Acquisti, *Privacy in Electronic Commerce and the Economics of Immediate Gratification*, *in* PROCEEDINGS OF THE ACM ELECTRONIC COMMERCE CONFERENCE 21, 22 (2004).

[29] *Id.*

[30] *See* Paul Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2076 (2004) ("The emerging verdict of many privacy scholars is that existing markets for privacy do not function well.").

[31] *See* Acquisti, *supra* note 30, at 23-24.

[32] *See infra* notes 91-95 and text accompanying (noting stringent European Union regulations concerning personal information).

Notice and consent also assumes that individuals reveal personal information and do not intend to retain some level of control over it. Current behavioral theory suggests that recipients of personal information should not use the information freely.[33] Disclosing individuals expect the recipient to co-manage the information along with them.[34] The sociological theory of social networks contributes toward understanding the process of information dissemination.[35] It suggests an individual expects personal information to remain within a controlled group to which the individual has ties.[36] For instance, a customer of Marks & Spencer might not worry if the retailer has her credit card information, but does not want that information conveyed to unfamiliar firms.

Theories from different academic perspectives agree that the idea of 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.[37] Simply stated, these theories suggest that notice does not equal awareness, and that choice does not always mean informed consent.

Marks & Spencer took individuals' privacy into account when creating policies concerning its item-level RFID tags, but as a result it adopted policies that do not make full operational use of the technology. A future challenge is to develop privacy standards that go beyond the narrow understanding of privacy evidenced in FIPP, while allowing increased efficiency and effectiveness through the use of RFID. We address this challenge by integrating several theoretical lenses of privacy in this paper and applying an integrative approach to data collected using RFID.[38] The intent of this article is twofold. First we provide a baseline definition of privacy beyond the legal precedents and understanding, by incorporating other theoretical perspectives so as to frame broadly our discussion of RFID data collection. Second, we begin the discussion of potential

---

[33] *See generally* Sandra Petronio, BOUNDARIES OF PRIVACY: DIALECTICS OF DISCLOSURE 9 (2002).

[34] *Id.* at 10.

[35] *See generally* Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919, 946-47 (2005) ("The basic challenge of network theory is to understand how change occurs and is transmitted among adjacent units in any kind of network. Perhaps surprisingly, the same basic insights about network structure have been found applicable to a variety of disparate disciplines."); *see also* DUNCAN J. WATTS, SIX DEGREES: THE SCIENCE OF A CONNECTED AGE (2003).

[36] *See* Strahilevitz, *supra* note 35, at 954-55.

[37] *See infra* Part IV.

[38] We do not mean to suggest that we are the first to apply diverse academic perspectives to privacy law. *See, e.g.*, Ian Altman, *Privacy Regulation: Culturally Universal or Culturally Specific?*, 33 J. SOC. ISSUES 66 (1977) (discussing privacy in the context of cultural norms); Stephen T. Margulis, *Privacy as a Social Issue and Behavioral Concept*, 59 J. SOC. ISSUES 243 (2003) (offering a bridge between social psychology and social issues approaches to privacy and exploring behavioral aspects of privacy); Strahilevitz, *supra* note 35, at 919 (applying social network theory to the reasonable expectation of privacy standard of tort law). Nonetheless, our approach advances this interdisciplinary literature by incorporating diverse academic research into an integrative model.

solutions to managing private data obtained through RFID technology with an emphasis on data expiration policies as an important component of data retention practices.

In Part II of this paper, we provide the relevant background for our discussion, including the capabilities of RFID and related technologies that raise issues of privacy protection. The current regulation of technology and attempts to legislate RFID technology is highlighted.

In the first portion of Part III, we examine the law and economics underpinnings of privacy law as an important base for the specific concerns raised by RFID. The second portion of Part III outlines legal models for further expansion of individual privacy rights in light of expanding technological capabilities. We argue that current legal scholarship often fails in two crucial aspects when considering regulation of technology with privacy implications. The first, as seen in the Marks & Spencer example, demands limiting the operational use of the technology and discouraging developing the full potential of technological advances. The second is that the legal theory does not incorporate adequately a range of important understandings about privacy gleaned from economic, behavioral, and sociological research.

In Part IV we discuss three theoretical lenses concerning privacy: behavioral economics, communications privacy management, and social networks. Each lens offers relevant insight for evaluating privacy law and constructing privacy rights while permitting technological advancement.

We advocate in Part V for an integrative privacy approach utilizing the three crucial Integrative Considerations gleaned from our integrative theoretical research: 1) individuals expect to own, control, and share personal information even after disclosing it; 2) advancing technologies raise concerns about individuals' bounded rationality and ineffective analysis of the costs and benefits of disclosing personal information; and 3) the significant threat to personal privacy comes not from the initial disclosure of personal information but from the subsequent re-use, transfer to third parties, and aggregation of that information. This Part concludes by applying the Integrative Considerations to data collected by RFID. This integrative approach requires limits on information obtained through RFID, including the types of information gathered, the time frame in which the information is used and then expired, and the re-use and transfer of information.

In addition to our focus of offering self-regulation standards for RFID data collection, an additional benefit of recognizing the significant threats to personal privacy from RFID technology permits developing law to focus on these crucial aspects without unnecessarily impeding technological advancement.

II. BACKGROUND

The unique and pervasive capabilities of RFID provide context for our discussion of individual information privacy. Our focus is on the data generated through RFID technology while norms for governing this information are lacking.

A. Radio Frequency Identification Technology

An RFID tag often is described as the next generation of bar codes or as a "super" bar code.[39] Broadly speaking, RFID consists of a microchip attached to an antenna. The microchip of the tag can be as small as a grain of rice with an antenna spanning anywhere between 1/8 to 2 inches.[40] RFID systems are comprised of three main components: 1) the RFID tag, or transponder, which is located on the object to be identified and is the data carrier in the RFID system, 2) the RFID reader, or transceiver, which may be able to both read data from and write data to a transponder, and 3) the data processing subsystem which utilizes the data obtained from the transceiver in some useful manner.[41]

The RFID system grants the user the capabilities of tracking and obtaining very detailed information about the object to which the tag is attached.[42] RFID tags fall into two categories: active or passive. Active tags are equipped with an onboard power source whereas passive tags are activated by the electromagnetic signal sent by the RFID reader.[43]

RFID tracking capabilities can increase dramatically the power of logistic and supply chain management giving rise to many potential competitive advantages for businesses that choose to implement the technology. RFID technology has the potential to replace totally the traditional optically scanned barcodes due to the technology's numerous benefits.[44] For example, a stationary RIFD reader can instantaneously read entire boxes

---

[39] *See generally* NIST RFID GUIDELINES, *supra* note 3, at 2-1 ("Today, people typically perceive the label identifying a particular object of interest as static, but RFID technology can make this label dynamic or even 'smart' by enabling the label to acquire data about the object even when people are not present to handle it.").

[40] Sanjay E. Sarma et al., *RFID Systems, Security & Privacy Implications*, AUTO-ID CENTER-MASSACHUSETTS INSTITUTE OF TECHNOLOGY, WHITE PAPER 1, 16 (Nov. 1, 2002), www.autoidlabs.org/whitepapers/MIT-AUTOID-WH-014.pdf.

[41] *Id.*

[42] *See* Juels, *supra* note 1, at 59 ("In some ways RFID endows computer systems with the ability to 'see' everyday objects including visually obstructed objects and distinguish between objects that are physically identical.").

[43] *See* Sarma, *supra* note 40, at 16; *see also* Ephraim Schwartz, *The Case for Active RFID*, INFOWORLD, June 21, 2005, http://www.infoworld.com/article/05/06/21/26OPreality_1.html?BUSINESS%20INTELLIGENCE%20APPLICATIONS.

[44] The benefits of RFID in comparison to traditional optically scanned tags, according to Simson Garfinkel of MIT, are:

1. Optical barcodes need to be in plain view to be read; RFID tags can be read through fabric, paper, cardboard, and other materials that are transparent to the frequency of operation.
2. Traditional optical barcodes are limited to 13 digits of information, and two-dimensional barcodes are limited to several hundred; RFID tags can store hundreds or thousands of bytes of information.
3. Only a single optical barcode can be read at a time; dozens of RFID tags can be read at the same time with a single reader. For example, an RFID reader could be used to read all of the individually tagged items within a case of merchandise.

of inventory information for truckloads of goods in a matter of seconds, from feet or even miles away; whereas RFID's predecessor, the bar code, involves reading each individual item or pallet, one by one, with a scanner that demands close range and even unpacking or rearranging of boxes of goods.[45] Compared to the bar code, RFID chips can store exponentially more data at a cost per chip as low as 5 cents and falling.

At 200 tags per second, an incoming truckload could be scanned at a loading dock by a freestanding RFID reader in a matter of seconds depending on whether the shipment was tagged by pallet or by individual item. Assuming that each item is equipped with its own unique RFID tag, a grocery shopper could bag his or her groceries while shopping, pack them in the cart, and as he or she exited the store an RFID reader could scan all of the contents of cart in less than one second.[46] By incorporating readers into check-out lines, loading docks, and other points of data gathering, RFID technology provides benefits to business operations by reducing labor and time needed, and by increasing the accuracy of information about the location of inventory and other physical assets.[47]

The retail world is capitalizing already on the benefits of RFID. In fact, at the retailer's behest, more that 600 suppliers have started shipping RFID-tagged pallets and cases to Wal-Mart Stores, Inc.[48] However, the effectiveness of the technology is still relatively low as the infrastructure and data processing means have not yet been

---

4. Optical bar codes are read-only; advanced RFID tags can store information and perform limited processing.
5. Optical bar codes are promiscuous, in that any reader can read any compatible optical bar code that comes in range; RFID tags can be assigned a password, limiting who has the ability to read them.
6. The only way to deactivate an optical bar code is by obliterating or obscuring it; RFID tags can be electronically deactivated.

Simson L. Garfinkel, *Adopting Fair Information Practices to Low Cost RFID System*, MASSACHUSETTS INSTITUTE OF TECHNOLOGY-LABORATORY FOR COMPUTER SCIENCE, (2002), http://www.simson.net/clips/academic/2002.Ubicomp_RFID.pdf. *See also* NIST RFID GUIDELINES, *supra* note 3, at 2-1 ("RFID products often support other features that bar codes. . . do not have, such as rewritable memory, security features, and other environmental sensors that enable the RFID technology to record a history of events.").

[45] *See* NIST RFID GUIDELINES, *supra* note 3, at 2-1. Typically the information on an RFID tag is simply a tracking number with the personal data stored on a server. Theft of data through interception of the RFID signal, often the perceived danger, is not the main privacy threat. *Id.* at 4-5 (noting that with the accumulation of tagged items "the potential for more complex associations and inferences increases").

[46] *But see* Juels, *supra* note 1, at 62 (NCR conducted a pilot of auto-shopping cart inventory and found good scanning range can pose problems because customers sometimes paid for purchases of those behind them in line).

[47] *See* Will Sturgeon, *Las Vegas Casino Goes for RFID*, SILICON.COM, April 15.2005, http://software.silicon.com/security/0,39024655,39129583,00.htm (noting that a Las Vegas casino uses active tags to tag restaurant employees for the purpose of time and motion studies, but that many employees have complained).

[48] *See* Sliwa, *supra* note 23.

perfected.[49] Commentators agree that RFID's full impact is not imminent, but these commentators vary on predictions about the timing of RFID's proliferation.[50]

The serious privacy issues raised by RFID technology are becoming ubiquitous as society inevitably transitions into the era of pervasive computing, information, and identification technologies. Beyond RFID alone, other potentially privacy-invading technologies exist and include biometric identification, GPS-enabled devices, sensor networks and personal data chips.[51] When RFID systems connect to other privacy-invading technologies, the resulting information concerning individuals becomes quite revealing.[52] The focus of our discussion is on privacy issues associated with the collection and re-use of information obtained through RFID technology.

B. Privacy Definitions and Concepts

Our focus is on individual information privacy. We define privacy as the "control of personal information by the individual."[53] *Personal information* can be any data about the individual. *Control* is the individual's ability to regulate the flow of personal information to other parties; that is, to *retain* (keep secret, protect, keep confidential, secure, conceal, or restrict) or *disclose* (reveal, share, transfer, or inform) that personal information under the conditions and to the parties of the individual's choosing. In all, privacy is not so much the actual retention of information, but rather the ability to choose to retain or disclose personal information. Finally, our definition emphasizes that, although full retention and full disclosure represent endpoints on a spectrum, there also exist mixed and intermediate forms of information retention and disclosure.[54]

---

[49] RFID tags presently are unreliable because of signal interference caused by some metals and liquids. *See* Juels, *supra* note 1, at 63 ("[B]ecause human beings consist largely of water[, i]f you are worried about your RFID-tagged sweater being scanned, your best course of action may be to wear it.").

[50] *See RFID Market to Reach $7.26 Bn in 2008*, IDTECHEX, April 10, 2005, http://www.idtechex.com/research/articles/rfid_market_to_reach_7_26bn_in_2008_00000169.asp (predicting that the global RFID market will continue to grow and reach $24.50 billion by 2015). *But see* Juels, *supra* note 1, at 61 (predicting RFID impact between the years 2015 and 2020).

[51] *See generally* PRIVACY AND TECHNOLOGIES OF IDENTITY: A CROSS-DISCIPLINARY CONVERSATION (Katherine Strandburg & Daniela Stan Raicu, eds., 2006) (providing a collection of perspectives concerning emerging technologies and their impact on privacy).

[52] Jackson, *supra* note 2.

[53] *See* Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?*, 44 Fed. Comm. L. J. 195, 208 (1992) ("The American legal system does not contain a comprehensive set of privacy rights or principles that collectively address the acquisition, storage, transmission, use and disclosure of personal information within the business community.").

[54] *See* ALLAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967) (describing informational privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."); Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 562-563 (2006) ("Protecting privacy requires careful balancing, as neither privacy nor its countervailing interests are absolute values. Unfortunately, due to conceptual confusion, courts and legislatures often fail to recognize privacy problems, and thus no balancing ever takes place."); Strahilevitz,

Significantly, giving up (disclosing) personal information is different from giving up control over personal information.

Although the United States Supreme Court recognizes some limited areas of privacy, there are many other conceptualizations of privacy.[55] Extant research aims to cut through this definitional clutter by categorizing individual privacy.[56] For example, one commentator identifies four "factual principles" of individual privacy: physical privacy, decisional privacy (an individual's independence in making important decisions), informational privacy[57] (an individual's ability to avoid disclosure of personal matters) and communications privacy.[58] In contrast, others identify broad areas of individual privacy based on activity context: medical privacy,[59] workplace privacy[60] and consumer privacy.[61]

It is also necessary to differentiate the motivations for maintaining privacy from the actual practice of maintaining privacy.[62] An individual may choose not to disclose certain personal information due to shyness, embarrassment, or concern about potential resulting harms.[63] Or the individual may choose not to disclose certain information because she knows that information has economic value to some other party. So she

---

supra note 35, at 921 ("[T]he law should focus on the more objective and satisfying question of what extent of dissemination the plaintiff should have expected to follow his disclosure of that information to others.").

[55] *See* Solove, *supra* note 54, at 479 ("Privacy seems to be about everything, and therefore it appears to be nothing.").

[56] *But see* Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1130 (2002) (concluding there is no singular essence or core characteristics found in all privacy law).

[57] *But see* Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as the Object*, 52 STAN. L. REV. 1373, 1427-28 (2000) ("[I]nformational privacy, in short, is a constitutive element of civil society in the broadest sense of the term."); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1613 (1999) ("Informational privacy is best conceived of as a constitutive element of civil society.").

[58] Lisa S. Nelson, *Constructing Policy: The Unsettled Question of Biometric Technology and Privacy*, *in* PRIVACY AND TECHNOLOGIES OF IDENTITY: A CROSS-DISCIPLINARY CONVERSATION 151, 153 (Katherine Strandburg & Daniela Stan Raicu, eds., 2006).

[59] Robert Gellman, *Personal, Legislative, and Technical Privacy Choices: The Case of Health Privacy Reform in the United States*, VISIONS OF PRIVACY: POLICY CHOICES FOR THE DIGITAL AGE, 129, 134 (Colin J. Bennett & Rebecca Grant, eds., 1999).

[60] *See, e.g.*, Eugene F. Stone & Diane L. Stone, *Privacy in Organizations: Theoretical Issues, Research Findings, and Protection Mechanisms*, 8 RESEARCH IN PERSONNEL AND HUMAN RESOURCE MANAGEMENT 349, 350 (1990).

[61] *See, e.g.*, Curtis R. Taylor, *Consumer Privacy and the Market for Customer Information*, 35 RAND J. ECON. 631, 635 (2004).

[62] *But see* Fred H. Cate, *Principles for Protecting Privacy*, 22 CATO J. 33, 36 (2002) ("[P]rivacy tends to be a one-sided issue. Who is against it?").

[63] *See* Petronio, *supra* note 33, at 49-50.

waits until another party offers sufficient compensation for that information.[64] 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.[65] 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.[66]

Privacy is not always perceived favorably. Some view privacy positively because it can protect individuals and allows the functioning of a free society.[67] Others view privacy quite negatively because any privacy at all impedes the free flow of information, increases search costs in economic transactions, and makes markets less efficient.[68] Some economists even equate "privacy" with "secrecy" and all its concomitant negative connotations.[69] And yet others view privacy more neutrally and in a situational light, because 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, information acquisition can be *overt* (explicit and apparent to the individual, as occurs when filling out a registration form) or *covert* (without advance notice of the information collection activity to the individual, as with surreptitious monitoring such as the use of Internet "cookies"). Intermediate forms exist as well.[70]

Finally, we note that privacy is very contextual, personal, cultural, and dynamic.[71] 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.[72] And how

---

[64] *See* Taylor, *supra* note 61, at 633 (noting that consumers who anticipate the sale of their information "misrepresent their preferences by strategically refusing to buy [from the firm] if it sets a high price").

[65] *Id.* at 635.

[66] *See* Staten & Cate, *supra* note 27, at 786 (noting the efficiencies and benefits of target marketing).

[67] *See, e.g.*, Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L. J. 421, 455 (1980) ("Privacy is also essential to democratic government because it fosters and encourages the moral autonomy of the citizen, a central requirement of democracy.").

[68] *See, e.g.*, Cate, *supra* note 62, at 37 (noting that privacy laws emphasizing control of information create significant costs without yielding net benefits).

[69] *See* Richard A. Posner, *The Economics of Privacy*, 71 AM. ECON. REV. 405, 405-09 (1981).

[70] Anna E. Shimanek, *Do You Want Milk with Those Cookies? Complying with the Safe Harbor Privacy Principles*, 26 J. CORP. L. 455, 459-61 (2001).

[71] *See* Petronio, *supra* note 33, at 38-83.

[72] *See* Strahilevitz, *supra* note 35, at 959-66 (discussing cultural and strategic considerations in sharing information based on three empirical studies involving topics as diverse as HIV status, academic discipline, and bakery closings).

one treats his or her personal information can be quite different from how one treats and places importance on someone else's personal information.[73]

C. The Reach of Privacy Legislation and Regulations

Privacy law at both the federal and state level has developed inconsistently over time and typically in response to a specific threat. That trend continues with legislation aimed at regulating the use of RFID.

1. Federal Law

Two broad themes are apparent in federal law pertaining to individual privacy.[74] The first theme is preventing intrusion on individuals by the government.[75] This is addressed in the U. S. Constitution. The second theme is preventing the use of information by the private sector that (unfairly) harms consumers.[76] This is addressed in various federal acts comprising the federal statutes.[77]

Although the U. S. Constitution does not overtly address the privacy of individuals, aspects of privacy are referenced throughout the Bill of Rights Amendments to the Constitution. These appear most notably in: the First Amendment,[78] guaranteeing the right to free speech, freedom of religion, and the right to association; the Fourth Amendment,[79] protecting against unlawful search and seizure;[80] the Fifth Amendment,[81]

---

[73] *Id. See generally* Andrew Askland, *What, Me Worry? The Multi-Front Assault on Privacy*, 25 ST. LOUIS U. PUB. L. REV. 33, 33 (2006).

[74] Cate, *supra* note 62, at 36.

[75] *Id.*

[76] *Id. See generally* Grayson Barber, *Personal Information in Government Records: Protecting the Public Interest in Privacy*, 25 ST. LOUIS U. PUB. L. REV. 63 (2006); Lars S. Smith, *RFID and Other Embedded Technologies: Who Owns the Data?*, 22 SANTA CLARA COMPUTER & HIGH TECH L.J. 695 (2006) (describing the development of law to protect consumers' information).

[77] The Fair Credit Reporting Act, for example. 15 U.S.C. § 1681 (2000). A full discussion of the federal laws with important privacy implications, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (Aug. 21, 1996) (codified as amended in scattered sections of 26 and 42 U.S.C), is outside the scope of this RFID discussion. However, for a discussion of privacy policies in recent federal legislation, see Corey A. Ciocchetti, *E-Commerce and Information Privacy: Privacy Policies as Personal Information Protectors*, 44 AM. BUS. L.J. 55, 72-88 (2007) (proposing an E-Commerce Privacy Protection Awareness Act (EPPAA) based on the FIPP principles).

[78] U.S. CONST. amend. I.

[79] U.S. CONST. amend. IV. *See* Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J.L. & POL'Y, 211, 237-245 (2006); Reepal S. Dalal, Note, *Chipping Away at the Constitution: The Increasing Use of RFID Chips Could Lead to an Erosion of Privacy Rights*, 86 B.U.L. REV. 485, 486 (2006).

[80] *Compare* Smith v. Maryland, 442 U.S. 735, 743-44 (1979) ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.") *with* Kyllo v. United States, 533 U.S. 27, 34 (2001) (addressing whether the use of a thermal imaging

guaranteeing freedom from self-incrimination;[82] and the Ninth Amendment,[83] addressing general liberties.

However, there are limits to the constitutional privacy protections.[84] Constitutional privacy protections do not extend to the private sector's interaction with consumers.[85] The Constitution does not prohibit the collection and use of personal information by private firms unless Congress enacts specific legislation.[86] Congress is generally reticent to do so, but has on occasion passed such legislation, typically in response to significant consumer concerns. Some examples include Cable Privacy Protection Act of 1984[87] (a user's cable watching history is private); Video Privacy Protection Act of 1988[88] (a video rental consumer's rental history is private); Fair Credit Reporting Act[89] (consumers may correct inaccuracies in credit profiles maintained by reporting agencies); Gramm-Leach-

---

device to detect heat from a private home, to determine whether marijuana was being grown within, constituted a search under Fourth Amendment). In *Kyllo*, the government contended the device was non-intrusive and revealed no intimate details because device merely interpreted radiation that emanated from the home into public space. However, the Court stated, "It would be foolish to contend that the degree of privacy secured to citizens under the Fourth Amendment has been entirely unaffected by the advance of technology . . . . The question we confront today is what limits are placed upon this technology to limit encroachment on the realm of guaranteed privacy." *Kyllo*, 533 U.S. at 33-34.

[81] U.S. CONST. amend. V.

[82] The Fifth and Fourteenth Amendments' Due Process clauses affect only government actors. *See* Colorado v. Connelly, 479 U.S. 157 (1986) (holding that coerced confession violates due process only if coercion is from a state actor); s*ee also* Shimanek, *supra* note 70, at 469 (noting that Commerce Clause protections likely are applicable to the dissemination of information collected).

[83] U.S. CONST. amend. IX.

[84] *See* Shimanek, *supra* note 70, at 466 ("Many individuals erroneously assume that these privacy rights extend to almost all aspects of daily life, including commercial activities. . . [but these rights] are only applicable when government agents invade an individual's privacy."); Cate, *supra* note 62, at 56 ("The government may not unreasonably search and seize and the government may not compel disclosure of personal matters in certain circumstances. The private sector, by contrast, is free to do so, at least from a constitutional perspective.").

[85] *But see* Anita L. Allen, *Coercing Privacy*, 40 WM. & MARY L. REV. 723, 755-57 (1999) (arguing that certain individual liberties must be sacrificed in the name of maintaining societal expectations of privacy).

[86] *See* Cate, *supra* note 62, at 36. *But see* Whalen v. Roe, 429 U.S. 589, 605 (1977) (upholding New York statute requiring physicians to submit prescriptions for abused drugs to a state centralized computer system, but recognizing dangers of computer databases to an individual's right to privacy of personal information); *see* Nelson, *supra* note 58, at 161 (stating that *Whalen* highlighted two important points: "facilitation of information gathering by technology might necessitate greater Constitutional protections of information privacy" and "despite compelling political objectives, personal information must be afforded protections").

[87] Pub. L. No. 98-549, 98 Stat. 2779 (1984) (codified as amended in various sections of 47 U.S.C.).

[88] 18 U.S.C. §§ 2710-2711 (2000).

[89] 15 U.S.C. § 1681 (2000).

Bliley Financial Services Act of 1999[90] (financial services customers must be given notification of the financial service firm's privacy policy).

Interestingly, the United States' piecemeal approach to federal privacy law contrasts the stringent personal data protection adopted by the European Union (EU).[91] EU member countries' citizens have a fundamental right to privacy that is more encompassing than that of United States' citizens.[92] Since 1998 the EU has regulated consumer privacy in its member countries through the European Union's Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data.[93] This directive mandates both statement of the purpose of data collection and receipt of consent from the individual, before personally identifiable information can be transferred to another party.[94] Personally identifiable data is any information that can reveal an individual's identity (including phone number, name, address, physical characteristics, email address, Internet cookies, or personal identification numbers).[95]

2. State Law

Common law tort claims for privacy protection are traced to the seminal 1890 law review article by Samuel Warren and Louis D. Brandeis.[96] Warren and Brandeis

---

[90] Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified in various sections of 12, 15, 16, 18 U.S.C. (2000)).

[91] *See* Nelson, *supra* note 58, at 158 ("The international trend is to shift responsibility for privacy protection to governmental and private entities. This is different from Constitutional doctrines that are based on an expectation of privacy either formed by the individual or defined within the realm of intimate or informational decision making.").

[92] *See* Francesca Bignami, *Privacy and Law Enforcement in the European Union: The Data Retention Directive* , 8. CHI. J. INT'L L. 233, 233 (2007) ("Data privacy is one of the oldest human rights policies in the European Union."); Scott Rempell, *Privacy, Personal Data and Subject Access Rights in the European Data Directive and Implementing UK Statute:* Durant v. Financial Services Authority *as a Paradigm of Data Protection Nuances and Emerging Dilemmas*, 18 FLA. J. INT'L L. 807 (2006); Morey Elizabeth Barnes, Comment, *Falling Short of the Mark: The United States Response to the European Union's Data Privacy Directive*, 27 NW. J. INT'L L. & BUS. 171 (2007); *see also* David Lindsay, *An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law*, 29 MELB. U. L. REV. 131, 134 (2005) ("This article contends that there is a fundamental divergence between the two main approaches to privacy within the Western legal tradition, which can be conveniently labeled the European approach and the American approach.").

[93] Council Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data, 1995 O.J. (L281) 31. European Union member states are: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and United Kingdom. Europa, European Countries, http://europa.eu/abc/european_countries/index_en.htm (last visited October 6, 2008).

[94] Council Directive 95/46/EC, *supra* note 93.

[95] *Id.* For a discussion of the Directive, see David Church, *Recent Developments Regarding U.S. and European Union Regulation of Electronic Commerce*, 33 INT'L LAW 347 (1999).

[96] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

introduced the possibility that individuals would have a common law action in state courts to protect personal information, particularly about "the private life, habits, acts, and relations of an individual."[97] Further developed and defined,[98] the four basic kinds of privacy rights[99] that every individual has against other individuals and entities that are not government actors in common law are: 1) unreasonable intrusion upon the seclusion of another;[100] 2) appropriation of a person's name or likeness;[101] 3) publication of private facts;[102] and 4) publication that places a person in a false light.[103] Other claims, including negligence claims from the use of privacy-invading technology, are possible under state law.[104]

State legislatures actively have pursued privacy legislation related to RFID.[105] Initially, model RFID legislation developed by Katherine Albrecht mandated users of RFID to declare the presence of the tracking device on the product to which it was attached.[106] Her bill proposal, The Right to Know Act of 2003[107] was a benchmark for legislation proposals in California on February 20, 2004,[108] in Utah on January 27,

---

[97] *Id.* at 216.

[98] William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960). *See also* Solove, *supra* note 54, at 483 ("Prosser's great contribution was to synthesize the cases that emerged from Samuel Warren and Louis Brandeis's famous article. . . . However, Prosser focused only on tort law.").

[99] For those categorizing privacy beyond the tort law categories, see for example, Ken Gormley, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335 (1992) (categorizing privacy as tort privacy, Fourth Amendment privacy, First Amendment privacy, fundamental-decision privacy, and state constitutional privacy); Solove, *supra* note 54, at 482 ("I aim to develop a taxonomy that focuses more specifically on the different kinds of activities that pose privacy problems."); Westin, *supra* note 54, at 31-32 (identifying "four basic states of individual privacy").

[100] RESTATEMENT (SECOND) OF TORTS § 652B (1977).

[101] RESTATEMENT (SECOND) OF TORTS § 652C (1977).

[102] RESTATEMENT (SECOND) OF TORTS § 652D (1977).

[103] RESTATEMENT (SECOND) OF TORTS § 652E (1977).

[104] *See* Remsburg v. Docusearch, Inc., 816 A.2d 1001, 1009 (N.H. 2003) (holding that information brokers owe a duty of reasonable care); Thyroff v. Nationwide Mut. Ins. Co., 8 N.Y.3d 283, 285 (N.Y. 2007) (finding insurance company liable for conversion of computer data by denying an insurance agent access to "his customer information and other personal information that was stored on the [company's] computers."); *see also* Jennifer E. Smith, Recent Development, *You Can Run, But You Can't Hide: Protecting Privacy from Radio Frequency Identification Technology*, 8 N.C. J.L. & TECH. 249, 271 (2007) ("In the absence of legislation, consumers may yet find recourse via federal or state unfair and deceptive trade practices law.").

[105] *But see* Jerry Brito, *Relax Don't Do It: Why RFID Privacy Concerns are Exaggerated and Legislation is Premature*, 2004 UCLA J.L. & TECH. 5, 6 (2004) ("Technologies reliably rouse old privacy concerns.").

[106] *See* Mark Baard, *Lawmakers Alarmed by RFID Spying*, WIRED NEWS, http://www.wired.com/politics/security/news/2004/02/62433 (Feb. 26, 2004).

[107] CASPIAN, *RFID Right to Know Act of 2003*, http://www.nocards.org/rfid/rfidbill.shtml.

2004,[109] in Missouri on December 1, 2003,[110] and in Maryland on January 14, 2004.[111] None of these bill proposals became law; however, state legislative efforts concerning RFID continue each year.[112]

In 2006, a least 17 states considered RFID legislation.[113] The major characteristics of the bills concerning the use of RFID were: requiring disclosure of such use, requiring removal or deactivation of the RFID device, and prohibiting linking RFID data to personal information.[114] Other legislation proscribed the use of RFID in certain circumstances, such as remotely reading identification documents without the owner's consent;[115] including RFID devices in government-issued or mandated identity documents;[116] and using RFID devices for tracking employees, students, or clients as a condition for obtaining benefits or services.[117] Of the 17 state legislatures considering

---

[108] S.B. 1834, 2003-2004 Reg. Sess. (Cal. 2004).

[109] H.B. 314, 56th Leg., 2004 Gen. Sess. (Utah 2004).

[110] S.B. 867, 92nd Gen. Assem., 2d Reg. Sess. (Mo. 2004).

[111] H.B. 354, 56th Leg., 2004 Gen. Sess. (Maryland 2004).

[112] National Conference of State Legislatures, *2007 Privacy Legislation Related to Radio Frequency Identification (RFID),* http://www.ncsl.org/programs/lis/privacy/rfid07.htm (13 states in 2007 considered RFID legislation, compared to 17 states in 2006 (*2006 Privacy Legislation Related to Radio Frequency Identification (RFID),* http://www.ncsl.org/programs/lis/privacy/rfid06.htm) and 12 states in 2005 (*2005 Privacy Legislation Related to Radio Frequency Identification (RFID),* http://www.ncsl.org/programs/lis/privacy/rfid05.htm)). *But see* Kristina M. Willingham, Note, *Scanning Legislative Efforts: Current RFID Legislation Suffers From Misguided Fears*, 11 N.C. BANKING INST. 313, 313 (2007) ("Since much of the legislation reflects exaggerated fears about RFID, increased awareness and education about the technology is necessary in order to allay these fears and allow financial institutions the opportunity to implement this cost-saving technology.").

[113] National Conference of State Legislatures, *2006 Privacy Legislation Related to Radio Frequency Identification (RFID),* http://www.ncsl.org/programs/lis/privacy/rfid06.htm. *See* Laura Hildner, *Diffusing the Threat of RFID: Protecting Consumer Privacy Through Technology-Specific Legislation at the State Level*, 41 HARV. C.R.-C.L. L. REV. 133, 164 (2006) ("A significant benefit of RFID-specific legislation would be its consumer education effects."). *But see* Serena G. Stein, *Where Will Consumers Find Privacy Protection from RFID? A Case for Federal Legislation*, 2007 DUKE L. & TECH. REV. 3, 22 (2007) ("Since RFID technology is used to track inventory nationally and manufacturers supply products to various states, regulating at state levels interferes with efficient commerce. This is not an effective way to protect the privacy of our nation's citizens or promote economy.").

[114] *Id.*

[115] S.B. 682, 2005-2006 Reg. Sess. (Cal. 2006). California leads other states in privacy protection legislation. *See, e.g.*, California Office of Information Security & Privacy Protection, Consumer Privacy, http://www.privacy.ca.gov/ (last visited October 1, 2008).

[116] S.B. 2558, 94th Gen. Assem. 2005-2006 Reg. Sess. (Ill. 2006) (with an exception for the I-pass system). Note that the language of this legislation refers to "contactless integrated circuits" as opposed to RFID specifically.

[117] H.B. 7432, 2006 Jan. Sess. (R.I. 2006) (vetoed by Governor June 23, 2006).

RFID in 2006, three states adopted RFID provisions: Georgia, New Hampshire and Wisconsin. Georgia and New Hampshire both established study groups to focus on RFID technology.[118] New Hampshire further enacted a law that prohibited the use of RFID to identify occupants of a vehicle or the ownership of a vehicle.[119] Wisconsin law prohibited requiring an individual to have a microchip implanted.[120] North Dakota[121] and California[122] passed bills prohibiting mandatory human microchip implants in 2007. These laws would permit voluntary RFID implants.

Privacy advocates and consumers are expressing concern successfully about privacy issues raised by RFID.[123] The trend of state laws poses difficulty for businesses wishing to implement RFID widely. A patchwork of varying legal requirements[124] significantly increases the cost of technological improvement.[125]

3. Fair Information Practice Principles

The Federal Trade Commission (FTC) advocates voluntary guidelines regarding information privacy.[126] The FIPP guidelines[127] are modifications of earlier guidelines promulgated by the U. S. Dept. of Health, Education and Welfare in 1973,[128] the

---

[118] H.R. 1558, 2005-2006 Leg. Sess. (Ga. 2006); H.B. 203, 2006 Sess. (N.H. 2006).

[119] H.B. 1738, 2006 Sess. (N.H. 2006).

[120] A.B. 290, 2005 Leg. Sess. (Wis. 2006).

[121] S.B. 2415, 60th Leg. Sess. (N.D. 2007)

[122] S.B. 362, 2007-2008 Reg. Sess. (Cal. 2007) (not yet signed by the Governor).

[123] *See, e.g.*, Katherine Albrecht**,** *Supermarket Cards: The Tip of the Retail Surveillance Iceberg*, 79 DENV. U. L. REV. 534, 562 (2002).

[124] State constitutions may address privacy along with the common law privacy protections. *See generally* Ken Gormley & Rhonda G. Hartman, *Privacy and the States*, 65 TEMPLE L. REV. 1279 (1992) (discussing state privacy laws).

[125] *See, e.g.*, Cate, *supra* note 62, at 37 (noting that privacy laws emphasizing control of information create significant costs without yielding net benefits).

[126] FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICE IN THE ELECTRONIC MARKETPLACE 2 (2000), http://www.ftc.gov/reports/privacy2000/privacy2000.pdf. *See* Shimanek, *supra* note 70, at 467 ("Widespread industry resistance to regulatory measures had, until recently, persuaded the FTC to adopt a passive approach to ensuring privacy for Internet customers. The FTC has endorsed industry self-regulation as the sole regulatory measure.").

[127] *See* Federal Trade Commission, *supra* note 21.

[128] Incorporated into US law in the Privacy Act of 1974, 5 U.S.C. § 552a (2000).

Organization for Economic Cooperation and Development in 1980,[129] the Canadian Standards Association in 1996,[130] and others.[131] Private corporations are not bound by FIPP.[132]

Although FIPP is the prevailing emphasis for privacy protection, the privacy law on which it is based is littered with exemptions and other weaknesses.[133] The crux of its protection comes from the notion of an "expectation of privacy"[134] and assumes that individuals have an adequate understanding of privacy threats when given legal notice of the risks (including information collected and how it may be used and disclosed to other entities) and the opportunity to consent.[135] Legal theories focus on the notice and consent issue and attempt to develop and refine the privacy protection achieved through this system.[136] Just one of the challenges of this system is that the privacy policies can

---

[129] OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA, O.E.C.D. Doc. C58 (final)(Oct. 1, 1980), *reprinted in* 20 I.L.M. 422 (1981), *available at* http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

[130] MODEL CODE FOR THE PROTECTION OF PERSONAL INFORMATION: A NATIONAL STANDARD OF CANADA, (1996), http://www.ftc.gov/reports/privacy3/endnotes.htm#N 27.

[131] *See* William J. Kambas, *A Safety Net in the Marketplace: The Safe Harbor Principles Offer Comprehensive Privacy Protection Without Stopping Data Flow*, 9 ILSA J. INT'L & COMP. L. 149, 155 n.27 (2002).

[132] *See* John M. Eden, *When Big Brother Privatizes: Commercial Surveillance, the Privacy Act of 1974, and the Future of RFID*, 2005 DUKE L. & TECH. REV. 20, 24 (2005) ("[P]rivate corporations are not bound by the fair information practices, open-access rules, and data-ownership principles embodied by the [Privacy Act of 1974].").

[133] "Specific exemptions exist for disclosure to agency employees, the Bureau of the Census, the National Archives and Records Administration, Congress or its committees, the Comptroller General, and the consumer protection agencies. Also exempted is disclosure required under the Freedom of Information Act, for statistical research or law enforcement purposes, in response to emergency circumstances, or pursuant to court order. Finally, the broadest exemption is for disclosure pursuant to a 'routine use.'" Nelson, supra note 58, at 164 (discussing the Privacy Act of 1974, 5 U.S.C. § 552a (2000)) (footnotes omitted). Nelson continues by noting that , even apart from stated exemptions, "requirements of notice and consent are often circumvented." *Id.*

[134] *See* Katz v. United States, 389 U.S. 347, 361 (1967) (discussing objective expectation of privacy in a Fourth Amendment claim); Oleg Kobelev, Recent Development, *Big Brother on a Tiny Chip: Ushering in the Age of Global Surveillance Through the Use of Radio Frequency Identification Technology and the Need for a Legislative Response*, 6 N.C. J.L. & TECH. 325, 333 (2005) ("[T]he Court's decision has been largely limited to the contents of the conversation, rather than giving any meaningful protection from the government tracking the physical location of the individual. . . ."). *But see* Strahilevitz, *supra* note 35, at 933 n.35 ("As a practical matter, however, defendants virtually always claim to have a subjective expectation of privacy, and the courts rarely second-guess those representations about the defendant's state of mind.").

[135] *But see* Strahilevitz, *supra* note 35, at 929 n.25 (noting negative externalities associated with voluntary disclosure where consent is not obvious).

[136] *See, e.g.*, Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 409-21 (1978) (economic analysis); Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a*

change at any time if new notice is given. RFID presents unique information privacy issues that current laws do not address adequately.[137]

III. LEGAL PRIVACY THEORIES

The specific concerns raised by privacy-invading technologies like RFID are not reflected in current legal theories of privacy. Economic theory is emphasized in current privacy law, but a legal property right in personal information is another theory garnering attention.

A. Law and Economics

The traditional legal understanding of privacy focuses on an individual's expectation of privacy, or "the right to be let alone."[138] Economists started applying economic theory to the concept of privacy when privacy was defined narrowly as concealing information.[139] For example, if an individual attempts to conceal personal information (e.g., HIV status is not revealed during a job interview), then that concealment retards the efficient flow of information. Early emphasis in economics was that a free flow of information achieves the best results in terms of efficient processing and optimal benefits.[140]

As firms increasingly seek access to personal information, the concept of information as a commodity that firms can buy and sell has led legal theorists to rethink the way law understands privacy.[141] Currently, the emphasis of privacy law for non-governmental

---

Right to Stop People from Speaking About You, 52 STAN. L. REV. 1049, 1122 (2000) (constitutional analysis).

[137] *See, e.g.*, Lars S. Smith, *RFID and Other Embedded Technologies: Who Owns the Technology?*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 695 (2006); D. Zachary Hostetter, *When Small Technology is a Big Deal: Legal Issues Arising From Business Use of RFID*, 2 SHIDLER J.L. COM. & TECH. 10 (2005).

[138] Warren & Brandeis, *supra* note 96, at 193.

[139] *See* Stigler, *supra* note 26, at 624; *see also* Posner, *supra* note 136, at 411-12.

[140] *See* Staten & Cate, *supra* note 27, at 746 (maintaining that this free flow still is vital to economic efficiency for the "New Economy"). *But see* James P. Nehf, *Incomparability and the Passive Virtues of Ad Hoc Privacy Policy*, 76 U. COLO. L. REV. 1, 32 (2005) ("We should openly acknowledge that non-economic values are legitimate in privacy debates, just as they have been recognized in other areas of fundamental importance.").

[141] *See, e.g.*, Lawrence Lessig, CODE AND OTHER LAWS OF CYBERSPACE 142-63 (1999); Simon G. Davies, *Re-Engineering the Right to Privacy: How Technology Has Been Transformed from a Right to a Commodity*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 143, 160-61 (Philip E. Agre & Marc Rotenberg eds. 1997); Symposium, *Cyberpersons, Propertization, and Contract in the Information Culture: Propertization, Contract, Competition and Communication*, 54 CLEV. ST. L. REV. 1 (2006). For a sampling of those who resist this notion of commodification, see Allen, *supra* note 85, at 750-57; Cohen, *supra* note 57, at 1423-28; Mark A. Lemley, *Private Property: A Comment on Professor Samuelson's Contribution*, 52 STAN. L. REV. 1545, 1551 (2000).

transactions is the concept of notice of intent to collect personal information, along with receiving some measure of consent. Anyone who has signed a privacy notice in a doctor's office recently has experienced this.[142] The doctor's office must prove its patients received notice of privacy rights, which it accomplishes by requiring the patient's signature on a form stating the patient has read the notice and agreed to it.[143]

Giving consumers greater control over personal information is the focus of the debate concerning opt-in versus opt-out rules associated with various consumer protection laws.[144] Advocates of opt-in rules argue that requiring specific consumer consent for the use of personal information encourages informed consent better than requiring specific steps to opt-out of the use of personal information.[145] Those advocating an opt-out system advocate for a free flow of information and a presumption that consumers prefer the benefits associated with a free flow of information.[146] Those who argue for economic efficiency see a requirement for explicit consent as a "drag" on the information flows that result in lower costs and benefits specifically targeted to consumers.[147]

B. Owning Personal Information

A growing number of legal scholars believe a better legal system for protecting an individual's personal information is to treat that information as property.[148] Legal property rights in personal information such as social security number, consumer preferences, and medical history would give individuals control over how that information is used.[149] Currently, firms that collect personal information (e.g., through a shopper loyalty card) have control over the personal information after the individual discloses it.[150] Therefore, the firm can treat that information, either by itself or in the

---

[142] *See* Cate, *supra* note 62, at 38 ("In this situation, a privacy law based on notice and consent imposes costs but does little to enhance privacy protection.").

[143] *Id.* at 46-53 (evaluating HIPAA legislation).

[144] Federal statutes adopting the opt-out approach include the Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified in various sections of 12, 15, 16, 18 U.S.C. (2000)) and the Fair Credit Reporting Act, 15 U.S.C. § 1681b(e) (2000). *See also* Staten & Cate, *supra* note 27, at 749 n.9 (citing examples of federal opt-in legislation introduced in the 107th Congress).

[145] *See, e.g.*, Albrecht, *supra* note 123, at 560-562.

[146] *See* Cate, *supra* note 62, at 34 ("These rules ignore much of the evidence about the cost and burden to consumers of providing notices and securing consent. . . .").

[147] *See* Staten & Cate, *supra* note 27, at 751- 767 (using specific examples from MBNA information to illustrate how opt-in laws "neutralize many of the productivity gains by advances in information technology").

[148] *See supra* note 141 (listing such scholarship).

[149] *See* Schwartz, *supra* note 30, at 2077-78 (discussing privacy preferences).

[150] *Id.* at 2059. *See generally id.* (focusing on four case studies involving the commodification of personal data: the VeriChip, an implantable ID chip; the wOzNet, a wearable ID chip; network computing, such as spyware; and compensated telemarketing).

aggregate with other shopper loyalty card holders' information, as an asset to sell to interested third parties (e.g., a retail marketing consultant).[151] For some card holders, that arrangement is acceptable if they receive discounts by using the card.[152] Other card holders might be less comfortable with such use of their personal information. Under the notice and consent system, individuals' privacy preferences are not given consideration.[153] Receiving discounts by using the card requires the individual to give full control of their information to the retail firm.

If an individual owns property, such as manufacturing equipment, then no one else can claim an interest or a "right" to that equipment. All rights associated with that property are a part of the property itself. It is possible to contract with others to use the equipment, but that right applies only to those with whom the contract was made and only according to the terms of the contract. The rights to the property are not just about control over the property.[154] The focus here is more on the concept of property as a bundle of sticks.[155] Using a single stick in the bundle (such as leasing the equipment to another manufacturer) does not eliminate the ability to enjoy other ownership rights associated with the equipment (such as valuing it as a firm asset or selling it outright). The flexibility of rights in property is important for addressing transactions involving personal information. Information privacy in this context refers to any means (be they legal, social norms, or other conditions) that concern transactions of personal information.[156]

The propertized legal regulation of personal information devised by Professor Schwartz contains five elements: inalienabilities, defaults, right of exit, damages, and institutions.[157] Per Schwartz, the hybrid inalienability regime arises out of the first element of inalienabilities.[158] Inalienability concerns restrictions on the transfer, ownership, or use of personal information.[159] If individuals have a legal property right to

---

[151] A firm's privacy statement may limit its ability to transfer individual's information but, typically, these privacy statements reserve the right to change the terms. For the consumer, it is a take-it-or-leave-it system. *See* Ciocchetti, *supra* note 77, at 89.

[152] *See* Schwartz, *supra* note 30, at 2077-78 ("Privacy price discrimination therefore requires an increased flexibility on the part of those who collect personal information to meet [customers] privacy preferences.").

[153] *Id. But see* Nehf, *supra* note 140, at 35 ("Preferences on privacy matters are generally muddled, incoherent, and ill-informed. If privacy preferences are real but not sufficiently coherent to form a sound basis for valuation, any attempt to place a monetary value on them loses meaning.").

[154] *See* Schwartz, *supra* note 30, at 2094 (rejecting "an unadorned Blackstonian conception in which individual control over personal property is an all-or-nothing proposition").

[155] *Id.*

[156] *Id.* at 2058.

[157] *Id.* at 2095-2113.

[158] *See* Susan Rose-Ackerman, *Inalienability and the Theory of Property Rights*, 85 COLUM. L. REV. 931, 931 (1985).

[159] *See* Schwartz, *supra* note 30, at 2098.

personal information, such as their consumer preference information, the law may restrict both the use of the information by a firm that collects such information and the firm's ability to transfer the information to a third party (such as a marketing consultant).

1. Limiting Firms' Use of Personal Information

Property rights would restriction the free use of personal information, such as for those individuals who are happy with the arrangement of receiving discounts in return for the personal information collected through the shopper loyalty card. However, free alienability of personal information is not optimal because it does not address the problems of market failure in transactions concerning personal information.[160] The current privacy market includes pervasive failures such that individuals, including those who sign up for shopper loyalty cards just to receive discounts, are unaware that "negotiating" is taking place in collecting data.[161] Most individuals are unaware that their consumer patterns are processed by collecting data from each individual use of the shopper loyalty card and these data, on its own and combined with other loyalty card holders' data, are sold to third parties. This asymmetry of information available to all the people involved, as well as the systematic disadvantage and relative vulnerability of consumers, in the market for personal information requires restrictions on alienability of personal information.[162] Professor Schwartz notes that one consequence of the market failure is that data processing companies that exploit personal information then over-invest in reaching consumers who do not want to be contacted.[163] There is no incentive for these companies to invest adequately in technology or services that enhance a consumer's expression of privacy preferences.[164]

Similarly, free alienability of personal information does not promote privacy commons.[165] Many scholars believe that deliberative democracy requires a free exchange of personal information through spaces (physical, technological, or otherwise) where legal rules and regulation encourage individuals to anonymously and semi-anonymously

---

[160] *Id.* at 2076-77. *But see* Cohen, *supra* note 57, at 1391 ("Recognizing property rights in personally-identified data risks enabling more, not less, trade and producing less, not more, rights.").

[161] *See* Schwartz, *supra* note 30, at 2078; *see also* Jeff Sovern, *Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information*, 74 Wash. L. Rev. 1033, 1074 (1999) ("[S]ellers can be expected to exploit consumer ignorance.").

[162] *See* Schwartz, *supra* note 30, at 2078.

[163] *Id.* at 2079.

[164] *Id.* ("Acquisition of personal information at below-market costs also leads companies to underinvest in technology or services that can enhance the expression of privacy preferences.").

[165] *See generally* Lawrence Lessig, THE FATE OF THE COMMONS IN A CONNECTED WORLD (2001) (discussing the ownership of information that results in less opportunity for innovation). Paul M. Schwartz describes the "privacy commons" concept as: "[I]nformational privacy can be seen as a commons that requires some degree of social and legal control to construct and then maintain. The privacy commons is a place created through rules for information exchange." Schwartz, *supra* note 30, at 2088.

share information with no fear of surveillance or unauthorized use of the information.[166] In this view, maintaining individuals' sense of security in how and where personal information is exchanged not only benefits the individual, but has societal benefits of promoting open discourse.[167]

The hybrid restriction on both the use of personal information, and transfer of the information, allows a consumer to transfer personal information only for an initial category of use.[168] The consumer is required to have the opportunity to block any further uses of the information or transfers of the information to unaffiliated firms.[169] This restriction limits the transfer of personal information because it eliminates the right of a consumer to grant permission to a data collector, such as the retailer that provides a shopper loyalty card, for all use or transfer of their information in a one-stop information consent transaction.[170] The advantage to the consumer is that if the data collector wants the data for further use or transfer, the collector must seek permission from the consumer, thus giving the consumer an opportunity to bargain for the use and transfer of data (possibly receiving additional discounts).[171]

The use-transferability restriction is designed to limit the negative impact of one-stop permission for personal information trade. The hybrid inalienability regime, however, also relies on the use of defaults that safeguard individual choice.[172] The regime emphasizes the value of an opt-in default[173] because it is information-forcing in that the data collector, as the most informed participant in the personal information market, is forced to inform the individual how the information will be used and to ask permission to

---

[166] *See, e.g.*, Solove, *supra* note 56, at 1087.

[167] *Id.*

[168] *See* Schwartz, *supra* note 30, at 2098.

[169] *Id.* ("The use-transferability restriction runs with the asset; it follows the personal information downstream.").

[170] Certain large data collectors are positioned to utilize data in significant ways. For example, in September 2000, Amazon.com experimented with dynamic-pricing, selling DVD movies to some customers for up to 40% less than what they sold the same movie to others based on customer buying histories. David Streitfeld, *On the Web Price Tags Blur: What You Pay Could Depend on Who You Are*, THE WASHINGTON POST, Sept. 27, 2000, at A1 ("With its detailed records on the buying habits of 23 millions customers, Amazon.com is perfectly suited to employ dynamic pricing on a massive scale."). When privacy groups learned of the price discrimination and brought media attention to it, Amazon.com issued a public apology and made refunds to over 6,500 customers. Lori Enos, *Amazon Apologizes for Pricing Blunder*, E-COMMERCE NEWS, Sept. 9, 2000, http://www.ecommercetimes.com/story/4411.html.

[171] *See* Schwartz, *supra* note 30, at 2098.

[172] *Id.* at 2100-06.

[173] *Compare* Staten & Cate, *supra*, note 27, at 776 (noting that opt-in requirements restricted MBNA ability to function efficiently) *with* Sovern, *supra* note 161, at 1074 (expressing concern for consumers in opt-out regimes). *See also* Kristen E. Edmundson, *Global Positioning System Implants: Must Consumer Privacy Be Lost in Order for People to Be Found?*, 38 Ind. L. Rev. 207, 234 (2005) ("Thus, any legislation aimed at the privacy of consumers with GPS implants should have an opt-in mechanism.").

do so.[174] Hidden information about data processing practices are forced out by the opt-in default. To promote the disclosure of information, participation in the system is mandatory, and is enforced by a law barring individuals from bargaining out of the system.[175] This means that individuals who do not care how their personal information is used cannot turn over their right completely; the collector still must contact them for every new use of the information or transfer to a third party.[176]

2. System for Protecting Individuals

Schwartz conceptualizes the hybrid inalienability regime as promoting bargaining for personal information. However, individuals nonetheless may enter bad bargains despite the use-transfer restriction and opt-in default. In the instance of a bad bargain, individuals have a right to exit – and to re-enter – transactions involving their personal information.[177] This would legally minimize long-term consequences of data transactions.[178]

Professor Schwartz suggests that laws supporting a property right in personal information should include penalties for violations that are not limited to the actual damages an individual can prove.[179] Damages associated with unauthorized data transactions should include a minimal fine because of the recognized impact of privacy intrusions on society as a whole.[180]

The role of institutions in Professor Schwartz's system would arise out of three functional needs.[181] The first is a market-making function that focuses on trading mechanisms. The private sector would address this function adequately.[182] The second

---

[174] *See* Schwartz, *supra* note 30, at 2103 ("An opt-in rule forces the data processor to obtain consent to acquire, use, and transfer personal information. It creates an entitlement in personal information and places pressure on the data collector to induce the individual to surrender it.").

[175] *Id.* (observing that the opt-in regime "also promotes social investment in privacy.").

[176] *Id.*

[177] *Id.* at 2106.

[178] *Id.* at 2107. Schwartz recognizes problems with this system. *Id.* ("The possible danger of a right to exit, however, is that it might actually encourage, rather than discourage, deceptive claims from data collectors. The risk is that deceptive information collectors will encourage defections from existing arrangements that are privacy-friendly.").

[179] *Id.* at 2108-10.

[180] *Id.* at 2109 (stating that a state determination of damages through legislation is preferable to the "Calabresi-Melamed approach" of injunctions).

[181] *Id.* at 2110 (relating this to the privacy commons discussion)

[182] *Id. But see* Kenneth C. Laudon, *Markets and Privacy*, COMMUNICATIONS OF THE ACM, Sept. 1996, at 99-104 (advocating the establishment of a National Information Market where individuals would establish "information accounts").

function of institutions in this system is that of verification.[183] One recommendation is that decentralized data markets coordinate verification through a separate association.[184] The government would oversee the market of private data transactions also through a decentralized system.[185] Oversight might include the right for citizens to file lawsuits concerning transactions of personal information, as well as privacy laws requiring multiple agency oversight.[186] One suggestion is for the federal government to create a Data Protection Commission to fill a more general oversight role.[187] This includes helping private entities, advocacy groups, and legislatures to understand the boundaries of existing information territories.[188]

C. Evaluating Legal Theories

The property right in personal information theory provides crucial lessons that supplement our understanding of personal privacy and data collection.[189] First, the perception is that the law does not adequately protect individuals' personal information and that changes are necessary to address this.[190] Second, a property right in personal information allows individuals to disclose their information and still retain control over it.[191] Each transaction by the data collector would require negotiating with individuals.[192]

---

[183] *See* Henry Hansmann & Reinier Kraakman, *Property, Contract, and Verification: The Numerous Clauses Problem and the Divisibility of Rights*, 31 J. Legal Stud. 373, 384 (2002) ("A verification rule sets out the conditions under which a given right in a given asset will run with the asset.").

[184] *See* Schwartz, *supra* note 30, at 2115.

[185] *Id.* at 2113 (calling for a mix of public and private action to enforce legal norms).

[186] *Id.* at 2112.

[187] *Id.* at 2115 ("In contrast to existing agencies that carry out enforcement actions, such as the FTC, a United States Data Protection Commission is needed to fill a more general oversight function."); *see generally* Benjamin R. Barber, STRONG DEMOCRACY: PARTICIPATORY POLITICS FOR A NEW AGE 310 (1984) (arguing for expanding the role of ombudsmen in society).

[188] *See* Schwartz, *supra* note 30, at 2115.

[189] Schwartz has applied this property system to specific technology elsewhere. *See, e.g.*, Paul M. Schwartz, *Privacy Inalienability and Personal Data Chips*, *in* PRIVACY AND TECHNOLOGIES OF IDENTITY: A CROSS-DISCIPLINARY CONVERSATION 93, 95 (Katherine Strandburg & Daniela Stan Raicu, eds., 2006); Paul M. Schwartz, *Privacy Inalienability and the Regulation of Spyware*, 20 BERKELEY TECH. L.J. 1269 (2005). *See also supra* note 141.

[190] *See, e.g.*, Nelson, *supra* note 58, at 169 ("Thus, an expectation of privacy cannot serve as a bulwark of protection. When an expectation of privacy cannot be adequately formed or is mistaken as to its power of protection, then it does little to afford safeguard privacy."); Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1313 (2000); Robert C. Post, Book Review, Jeffrey Rosen, *Three Concepts of Privacy*, 89 GEO. L.J. 2087, 2090 (2001).

[191] *See generally* Lessig, *supra* note 141, at 142-60.

[192] *See* Schwartz, *supra* note 30, at 2078.

This control aspect of the property right is in stark contrast to the free flow of information advocated by those who approach the question from a law and economics perspective.[193] Although there is value to the control sought by private property theorists, there are significant costs associated too.[194] These costs impede the development of technology as well as the operational efficiency the technology can achieve. Similar to how Marks & Spencer's implementation limited full operational use of the technology, the property system discourages the use and development of technological advances.

However, the current market system for transactions involving personal information lacks mechanisms for verification of the information, regulation of its use and security, and government oversight.[195] Benefits achieved through the free flow of information are not significant enough to ignore the risks and costs associated with the lack of privacy rights achieved by individuals in this system.

We argue that current legal theories do not adequately represent the privacy research in other academic disciplines.[196] The legal discussion must not exist in a vacuum but incorporate important insights from economic, behavioral, and sociological research. Understanding fully the issue of individual privacy advances the opportunity to develop a sustainable legal model of privacy.

IV. THEORETICAL LENSES

We introduce three theories to expand and advance the discussion of legal privacy rights.[197] We sampled quite diverse fields within the social sciences, as well as multiple theories within each discipline, before settling on these three. It is beyond the scope and intent of this paper to summarize all the privacy-related literature in any given discipline; rather, we chose one theoretical approach from each discipline. We also settled on this particular set of theories for specific reasons. Each theory provides meaningful lessons about privacy that arise because of the distinctive focus of the given discipline. Collectively the theories span a wide range of social science disciplines, providing different perspectives and contrasts. Finally, these theories, although from quite different disciplines, have relevant synergies and salient commonalties.[198] In all we believe these theories have great potential for developing a new understanding of privacy law.

---

[193] S*ee* Cate, *supra* note 62, at 37; Posner, *supra* note 136, at 394-96.

[194] *See* Staten & Cate, *supra* note 27, at 776.

[195] *See* Schwartz, *supra* note 30, at 2128 ("[O]ngoing scrutiny of regulation of personal data is needed because failure on the privacy market can harm both individual self-determination and democratic deliberation.").

[196] Some notable exceptions are highlighted in note 38 *supra*.

[197] *See infra* Part IV.A. (behavioral economics); Part IV.B. (Communication Privacy Management); Part IV.C. (social network theory).

[198] *See infra* Part V. (An Integrative Privacy Approach).

A. Behavioral Economics

As technology has progressed rapidly to impact how personal information is collected, processed, and stored, economic analysis also has developed to reach a broader understanding of privacy and its implications.[199] Then economic theory began to incorporate considerations of technologies that allow allowing greater protection of personal information (such as encryption technology).[200] Economic theory also began to consider the role of third party purchasers who create secondary markets in personal information.[201] Most recently, some economists have applied behavioral economics to better explain and understand how individuals make decisions about their personal information in the context of technology.[202] This lens offers a framework for understanding why the actions of individuals – even those with complete information – are affected by the economics of immediate gratification.[203]

Behavioral economists now posit that individuals may not be able to act economically rational when considering their personal privacy options.[204] Traditional economics maintained that individuals are forward-looking and when making decisions about their own personal information, they can take into account their future preferences.[205] In other words, individuals can value their personal information in the long-term and make decisions based on the value they associate with the information.[206] They will reveal the information to those willing to exchange it for something of equal or greater value, including discounts on products or faster service. Recent experiments, however, indicate that individuals do not value their personal information adequately.[207] In one case, those

---

[199] *See generally* Christine Jolls, Cass R. Sunstein &Richard Thaler, *A Behavioral Approach to Law and Economics*, 50 Stan. L. Rev. 1471, 1471 (1998).

[200] Eli M. Noam, *Privacy and Self-Regulation: Markets for Electronic Privacy*, *in* U.S. DEPT. OF COMMERCE, PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE (1997), *available at* http://www.ntia.doc.gov/reports/privacy/selfreg1.htm#1B..

[201] Hal R. Varian, *Economic Aspects of Personal Privacy*, *in* U.S. DEPT. OF COMMERCE, PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE (1997).

[202] *See, e.g.*, Alessandro Acquisti & Jens Grossklags, *Privacy Attitudes and Privacy Behavior: Losses, Gains, and Hyperbolic Discounting*, *in* THE ECONOMICS OF INFORMATION SECURITY, 165-78 (Jean Camp & Stephen Lewis eds., 2004); Sarah Spiekermann, Jens Grossklags & Bettina Berendt, *E-privacy in 2nd Generation E-commerce: Privacy Preferences Versus Actual Behavior*, *in* PROCEEDINGS OF THE ACM CONFERENCE ON ELECTRONIC COMMERCE 38-47 (2001).

[203] *See* Acquisti, *supra* note 28, at 22-27.

[204] *See* Alessandro Acquisti & Jens Grossklags, *Privacy and Rationality: Theory and Evidence*, *in* PRIVACY AND TECHNOLOGIES OF IDENTITY: A CROSS-DISCIPLINARY CONVERSATION 15-29 (Katherine Strandburg & Daniela Stan Raicu, eds., 2006).

[205] *See* Acquisti, *supra* note 28, at 22.

[206] *Id.* at 23 (showing this as an equation).

[207] *Id.*

individuals who identified themselves as valuing privacy highly nonetheless exchanged information for small rewards.[208]

Part of the explanation for why individuals do not value their personal information consistent with their own privacy preferences is that privacy itself is an ever-growing concept. It is better considered as a class of interests rather than a single monolith.[209] Information advances have blurred the lines between public and personal information and technology has changed the way individuals interact with personal information.[210] Consider the increasing popularity of on-line dating services. A process that in the recent past was considered private and personal now engages individuals willing to disclose their personal information for others to read in a very public way.[211]

1. Impeding Rational Privacy Decisions

One of the issues individuals face when they attempt to manage the trade-offs between protecting personal information (e.g., using encryption technology or an anonymous email service) and declining such protection is *incomplete information*.[212] Asymmetric information is a factor in many economic transactions.[213] In particular, incomplete information affects individuals' ability to measure the costs and benefits of these transactions. Costs include both monetary as well as nonmonetary costs. Everything from the cost of identity theft to the cost of employing technology to protect data involves specific monetary outlays.[214] Nonmonetary costs might include the effort

---

[208] *See* Spiekermann et. al., *supra* note 202, at 40.

[209] *See* Acquisti, *supra* note 28, at 23; *see also supra* Part II.B. (discussing privacy definitions and concepts).

[210] *See* Katherine J. Strandburg, *Social Norms, Self Control, and Privacy in the Online World*, *in* PRIVACY AND TECHNOLOGIES OF IDENTITY: A CROSS-DISCIPLINARY CONVERSATION 36 (Katherine Strandburg & Daniela Stan Raicu, eds., 2006) ("[T]he study may provide evidence that the inconsistency between individuals' stated attitudes about disclosing personal information and their behavior is a result of struggles pitting long term desires for privacy against short term temptations to disclose information in exchange for relatively minor, but immediately attractive, savings or conveniences.").

[211] *Id.* ("'Taste from disclosure' may result in less inhibition and looking out for one's own good."). Another example is the explosion of popularity of the web site www.myspace.com where younger people share personal information that an older generation would never dream of disclosing, *see, e.g., Teachers Warned About MySpace Profiles*, ESCHOOL NEWS, Nov. 19, 2007, http://www.eschoolnews.com/news/top-news/index.cfm?i=50557 (noting an investigation of public school teachers' postings on MySpace that included messages about drug use and sexual exploits while sometimes listing students as MySpace friends).

[212] *See* Acquisti, *supra* note 28, at 24.

[213] *See* Schwartz, *supra* note 30, at 2080 (discussing the problem of information asymmetries as a motivation for his information as property regime); *see generally* H. Jeff Smith, MANAGING PRIVACY: INFORMATION TECHNOLOGY AND CORPORATE AMERICA 95-138 (1994) (studying the inconsistent enforcement of corporate privacy policies).

[214] *See* Acquisti, *supra* note 28, at 24.

to identify the best technologies to protect data, anxiety over loss of control over private information, or the inability to interact fully in an on-line community because of a personal privacy preference. The identified benefits likewise are monetary (discounts to consumers willing to share personal information) or intangible (satisfaction with using encryption technology). Although important, it is very difficult to quantify the value of these costs or benefits until after a privacy intrusion such as identity theft.[215]

In a dynamic environment of changing technologies and new uses for personal information, individuals must deal with incomplete information about the probability distribution of future events.[216] If an individual knew with any certainty that entering a credit card number in a database today would result in identity theft in the next four to six years then that individual could perform a rational cost-benefit analysis, which would include considerations of completing a transaction quickly without waiting on hold for a customer service representative, canceling the credit card in the next year and switching to a new credit card company, and any future discounts from the store for revealing this personal information. However, knowing these future events with any certainty is impossible.[217]

Thus, individuals must make decisions about revealing personal information while limited by bounded rationality.[218] Individuals cannot make rational economic trade-off calculations because, once personal information is revealed, the individual has lost all control over it.[219] The personal information may be forwarded to third parties, aggregated with other individuals' personal information, and otherwise processed, manipulated, and exchanged in unpredictable ways (because some uses of this information are not even discovered yet) and without limit in time.[220] Not knowing key pieces of information, such as which firms are interested in purchasing personal information and to what ends, disadvantages an individual so that rational evaluation of personal information-revealing strategies is impossible. RFID technology and its ability to gather vast amounts of personal data contribute to an individual's inability to make rational privacy decisions.[221]

---

[215] *Id.* ("It is difficult for an individual to estimate all these values. Through information technology, privacy invasions can be ubiquitous and invisible. Many of the payoffs associated with privacy protections or intrusions may be discovered or ascertained only *ex post* through actual experience.")

[216] *See* Acquisti & Grossklags, *supra* note 204, at 29. *See generally* Susan Powell Mantel, Mohan V. Tatikonda & Ying Liao, *A Behavioral Study of Supply Manager Decision-Making*, 24 J. OPERATIONS MGMT. 822, 822-838(2006) (examining the process of decision-making).

[217] *See* Acquisti, *supra* note 28, at 24.

[218] *See* Schwartz, *supra* note 30, at 2081 ("Behavioral economics scholarship has demonstrated that consumers' general inertia toward default terms is a strong and pervasive limitation on free choice.").

[219] *See* Acquisti, *supra* note 28, at 24-25. For a discussion of privacy disclosure, see *infra* Part IV. B.

[220] *See* Strandburg, *supra* note 210, at 44 ("Data aggregation exacerbates the self-control issues that affect decisions to disclose personal information. Disclosure of each piece of information is particularly tempting because each disclosure forms an insignificant part of the picture.").

[221] *See supra* Part II.A.

2. Human Tendencies Impact Privacy

Lack of information and the ability to evaluate it fully are not the only factors hampering an individual in devising a rational strategy for personal information disclosure. Psychological distortions impact individual strategy, including hyperbolic discounting, under insurance, self-control problems, and immediate gratification.[222] Hyperbolic discounting refers to the tendency of individuals to apply a different discount rate to events that will happen soon than to events in the future.[223] Even if a high risk exists in the future of a loss of personal information through a security breach, individuals may not factor that risk into their strategy the same as they would a loss of personal information next week.[224] Compounding individuals' tendency not to discount future risks consistent with short term risks is their tendency to underinsure against risks.[225]

The nature of revealing personal information creates other psychological problems for the individual. It is rare that an individual is willing to turn over every piece of personal information all at once. Instead, the nature of requests for various small pieces of information (e.g., grocery shopping practices) seems innocuous and a small price to pay in return for discounts on grocery items. Each small piece of information remains available for long periods of time.[226] Therefore, even if an individual is only willing to reveal small innocuous pieces of information, these pieces released to various sources accumulate and congregate in the personal information market.[227] The time inconsistency involved in revealing information makes it difficult for individuals to judge the potential costs.[228]

An individual's inclination toward immediate gratification is exacerbated when the issue is privacy.[229] Loss of privacy usually is not felt immediately after revealing

---

[222] *See* Acquisti, *supra* note 28, at 25.

[223] Matthew Rabin & Ted O'Donoghue, *The Economics of Immediate Gratification*, 13 J. BEHAV. DECISION MAKING 233, 240 (2000).

[224] *Id.*

[225] *See* Acquisti, *supra* note 28, at 25.

[226] *See* Strandburg, *supra* note 210, at 44 ("This widespread and rapid dissemination makes it difficult, if not impossible, for individuals to make rational predictions of the costs and benefits of each disclosure.").

[227] *See* Acquisti, *supra* note 28, at 27 ("This dynamic captures the essence of privacy and the so-called anonymity sets, where each bit of information we reveal can be linked to others, so that the whole is more than the sum of the parts."); Cohen, *supra* note 57, at 1425 (data collection poses risks to autonomy because the "picture" that develops of an individual – over time – is in many respects more detailed than a visual observation of the individual, because patterns and preferences may be discerned).

[228] *See* Acquisti, *supra* note 28, at 27.

[229] *Id.* ("Individuals may tend to downplay the fact that single actions present low risks, but their repetition forms a huge liability: it is a deceiving aspect of privacy that its value is truly appreciated only after privacy itself is lost.").

information but the benefits from revealing small pieces of information may be received immediately, such as when you are asked to complete a survey to receive a coupon for a useful product or service. It is only when a future risk is realized, and the full effect of the loss of privacy is felt, that individuals can value privacy appropriately. For instance, when a routine search of a credit report reveals identity theft that requires canceling credit cards and re-establishing credit over a long period of time, the individual can appreciate the value of privacy. Until then, immediate gratification tendencies focus on short term results.[230]

Those individuals sophisticated enough to understand the self-control problems associated with immediate benefits could take steps to incorporate their awareness of these risks into their decision making process about revealing personal information.[231] An individual might think to himself, "Although I want to receive a discount for services at my favorite car detailer, to do so would require releasing my preferences, along with my credit card number and my home and email addresses. This information, if made available widely, will expose me to junk mail, spam email, and potential identity theft. The discount is not worth the risk." Studies suggest, however, that even the sophisticated individual does not engage in this type of analysis. In a counter-intuitive twist, knowing the risks may actually decrease an individual's incentive to reveal less information.[232] With the knowledge that complete protection from all future privacy intrusions is not possible, sophisticated individuals choose to reveal information now in order to obtain the greatest benefit immediately.[233] It is as if they think to themselves, "I will not get the discount unless I reveal the information, and it is inevitable there is personal information about me available to others."

This analysis in economic theory concludes that simply giving individuals as much knowledge as possible to help them analyze the cost and benefit trade-offs in privacy may not promote rational economic behavior.[234] Instead, rational privacy behavior is impossible, given individuals' incomplete information, the problem of bounded rationality, and a variety of psychological distortions. Improved individual awareness of the problem and adopting self-protection through better technologies will not resolve all the psychological issues that are factored into privacy decisions. Policies to regulate the collection and use of personal information may be necessary to increase privacy-related welfare.[235] Self-regulation by data collectors using RFID technology necessarily would include policies that regulate the collection and use of personal information.

---

[230] *See* Rabin & O'Donoghue, *supra* note 223, at 233.

[231] *See* Acquisti, *supra* note 28, at 28.

[232] *See* Spiekermann et. al., *supra* note 202, at 40.

[233] *See* Acquisti, *supra* note 28, at 28.

[234] *Id.*

[235] *Id.* ("The conclusions we have reached suggest that individuals may not be trusted to make decisions in their own best interest when it comes to privacy.").

This behavioral economics framework provides important insights concerning the evolution of economics and privacy, including that individuals cannot act economically rational when making decisions about personal information. Although classical economic analysis perceived a request for information as a trade-off that individuals accept or reject based on their own preferences and valuations,[236] behavioral theory unequivocally demonstrates that is not the case. Second, transactions in privacy, although affected by typical economic factors such as incomplete information, are uniquely impacted by human psychological tendencies.[237] Taking steps to increase awareness of costs and benefits will not resolve sufficiently these tendencies. Third, some economists are calling for regulation to prevent the costs of privacy from increasing. RFID technology permits vast data collection, re-use and transfer. The legal understanding of privacy should consider this research, which indicates the faulty basis of notice and consent in this context.

B. Communication Privacy Management

Communication Privacy Management (CPM), a theory from the behavioral communications discipline, provides rules for coordinating disclosure of personal information.[238] This lens offers an important framework for understanding individuals' decisions to disclose personal information.[239] CPM focuses on the fact that privacy and disclosure are not mutually exclusive. Disclosing information involves agreeing to coordinate with the discloser about how this information is used.[240] Disclosure, then, is not the same as turning over control of information to the recipient.[241] Communication in any form is not about imparting information but rather entering a relationship as a co-manager of the information with others.[242]

1. Coordinating Privacy and Disclosure

---

[236] *See* Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 Geo. L.J. 2381, 2382 (1996); Posner, *supra* note 69, at 409; Strandburg, *supra* note 210, at 38 ("[I]n grossly oversimplified terms, the consensus of the law and economics literature is this: more information in the name of privacy is better, and restrictions in the flow of information in the name of privacy are generally not social wealth maximizing, because they inhibit decision making, increase transaction costs and encourage fraud.").

[237] *See* Acquisti, *supra* note 28, at 25 (including hyperbolic discounting, under insurance, self-control problems, and immediate gratification).

[238] *See* Petronio, *supra* note 33, at 2-5 (discussing the origin of Communication Privacy Management).

[239] For a more detailed discussion of CPM and its relation to RFID and ethics, see Cochran, *supra* note 13, at 223-24.

[240] *See* Petronio, *supra* note 33, at 88-120.

[241] *See* Ellen Alderman & Caroline Kennedy, THE RIGHT TO PRIVACY 45-55 (1995) (discussing privacy versus information).

[242] *See* Petronio, *supra* note 33, at 109-10.

In social settings, communicating information is necessary for any number of reasons -- to get to know someone better, to function in a group, or to gain more information—but, according to CPM, the communication is not a one-time effort because individuals expect to retain the right to decide how their own information is used in the future.[243] Communication is a bond formed to manage the information appropriately.[244] For example, when someone asks you to serve as a reference for a position in a new company, you know intuitively that you do not have permission to inform the current boss of the discloser that she is hoping to receive a job offer from a new company. Rather, you understand that you must wait to tell others about the job possibility – particularly people who might tell the discloser's boss—until given permission or a general announcement is made.

Communication begins with personal information contained within boundaries.[245] Disclosure results in boundaries overlapping with other individuals' boundaries.[246] Disclosure creates various boundary overlaps but CPM emphasizes that the boundaries themselves are not erased. Instead, individuals must manage a multitude of information with different degrees of control, depending on the nature of the information communicated.[247]

2. Rules for Managing Privacy

CPM explains the rules individuals must use to manage the boundaries of communications. These rules focus on the amount of access to personal information intended by its communication and how the bond formed by the communication is coordinated. Rules are developed based on five decisional criteria: cultural norms into which people are socialized,[248] gendered differences (similar to cultural socialization but gender related), motivations for disclosure (encompassing a variety of factors), context of the disclosure (both in terms of social environment and physical setting), and risk-benefit analysis.[249] Rules are formulated based on the five decisional criteria but are further refined.

---

[243] *See* Leslie A. Baxter & Barbara M. Montgomery, RELATING: DIALOGUES AND DIALECTICS 178-181 (1996).

[244] *See* Petronio, *supra* note 33, at 111.

[245] *See* Baxter & Montgomery, *supra* note 243, at 178-81 (recognizing that boundaries are dynamic).

[246] *See* Petronio, *supra* note 33, at 88-90.

[247] *Id.*

[248] *See* Altman, *supra* note 38, at 71.

[249] *See* Petronio, *supra* note 33, at 38-39.

The first refinement concerns the manner in which individuals acquire rules.[250] Usually, individuals learn rules concerning communication management through socialization in a family or within a group or through negotiations about who is included in the communication. As time passes, rules are refined through experience, events, or other factors that help an individual manage all the personal information disclosures.[251] New situations may trigger new rules or changes in existing rules.[252] As co-owners of information negotiate their shared boundaries, positive or negative sanctions might reinforce the group privacy management rules.[253]

3. Clashes Over Privacy

CPM recognizes that the rules concerning managing the communication of personal information are not followed by everyone all the time. When clashes result from failure to manage information well there is "boundary turbulence."[254] Although turbulence might happen for a variety of reasons, our particular focus is when turbulence results from fuzzy boundaries.

Fuzzy boundaries occur when ownership of information is not defined clearly.[255] Technology may contribute to ownership confusion because it allows individuals to access personal information more readily than in the past.[256] However, access to personal information does not mean the unrestricted control of that information. CPM maintains that ownership of personal information is not wholly transferred through disclosure. Technology also causes an incongruity of access.[257] Privacy concerns occur when individuals believe that the use of their personal information does not follow established rules.

CPM addresses a fundamental issue of privacy: disclosure of personal information. The rules of communication require coordinating the dissemination of personal information after it is disclosed. Receiving information and taking full control of it without coordinating its maintenance within shared boundaries is not expected or understood and causes turbulence in the system. Nonetheless, data collected by RFID, including personal information, become wholly owned by the collector. CPM research indicates this is not typically the intent of those who agree to share such information, raising questions concerning notice and consent.

---

[250] *Id.* at 71-72.

[251] *Id.*

[252] *Id.* at 79-80.

[253] *Id.* at 81-82.

[254] *Id.*

[255] *Id.* at 177.

[256] *Id.* at 190.

[257] *Id.* at 224-25.

C. Social Network Theory

Social network theory contends that individuals are embedded in social relationships that in general can be characterized by either strong ties or weak ties.[258] Relationships characterized by strong ties are with people with whom we regularly share information, swap office gossip, eat meals, and so on.[259] Weak ties refer to other people that we know and recognize, with whom we exchange pleasantries and with whom we might exchange an occasional greeting card.[260] Recently, businesses have begun mapping these relationships in order better understand how information really flows within and across firms.[261] The result of the mapping can be very different from the relationships depicted on a typical organization chart.

1. Personal Information Connections

Mark Granovetter had a number of breakthrough observations concerning social networks.[262] One of his key observations was that most of the people with whom we have strong ties also have strong ties with each other. This is the group with whom an individual tends to form a social circle. Individuals within a social circle may share last names, employers, club memberships, neighborhoods, or alumni connections. The key point is that, in such a group, individuals all tend to have strong ties to each other. The connections within this network are dense and the networks are highly transitive. As a result no single individual is critical to this network. That is, the removal of any one individual will have minimal impact on the communications patterns within the network.[263]

On the other hand, weak ties are those ties to people outside of the individual's immediate social circle. People with whom a given individual has weak ties generally will not have ties to people within the individual's circle of strong ties. Weak ties thus serve a bridging function.[264] The absence of a weak tie between two groups, each closely

---

[258] *See* Strahilevitz, *supra* note 35, at 953-58.

[259] *See* John Scott, SOCIAL NETWORK ANALYSIS 32 (2000).

[260] *Id. See also* Gabriel Weimann, *The Strength of Weak Conversational Ties in the Flow of Information and Influence*, 5 SOC. NETWORKS 245, 246 (1983).

[261] *The Office Chart That Really Counts*, BUSINESSWEEK.COM (2006), http://www.businessweek.com/magazine/content/06_09/b3973083.htm. *See also* Gregory N. Stock & Mohan V. Tatikonda, *External Technology Integration*, 26 J. OPERATIONS MGMT. 65-80 (2008) (discussing information and technology flows within and across firms).

[262] Mark Granovetter, *The Strength of Weak Ties*, 1 SOC. THEORY 201 (1983).

[263] *Id.* at 201-02.

[264] *Id*. at 205.

knit, will all but eliminate the possibility of communications between these groups. In other words, there is no bridge to cross over the structural hole.[265]

Social networks tend to be scale-free or "power-law" networks.[266] That is, connections are far from uniformly distributed throughout the network. Instead, the vast majority of individuals are relatively isolated. However, there are a few individuals who are highly connected, often through multiple weak ties. These are often called hubs or super-nodes.[267] Information that becomes system-wide thus must flow through these super-nodes. The Kevin Bacon game is a popular culture means of examining the function of super-nodes. Connecting the movie actor Kevin Bacon to another movie actor through the fewest number of links as possible (the links in the game typically are movies) demonstrates how one well-connected movie actor can connect to other movie actors, including those who are isolated (in terms of movie actor status) and remain on the periphery.[268] Connections between individuals is a dynamic process, because new connections are made while others weaken or disappear through geographic constraints, death, change in interests, or any number of other factors.[269]

2. Predicting Information Flow

Social network theory means any single piece of personal information potentially can spread around the world. However, if individuals become highly concerned about that potential for wide-spread dissemination, they might tend to keep their personal information more closely held then necessary.[270] The reality is that most networks have "structural holes" (disconnect between the nodes) and, therefore, disclosing personal information within such a network raises little concern that information will diffuse widely within that social network.[271] Virtually the only way that personal information can become public information is if it flows through one or more super-nodes and the information is interesting or valuable enough for wide dissemination. Thus, it is

---

[265] Ronald S. Burt, STRUCTURAL HOLES: THE SOCIAL STRUCTURE OF COMPETITION 18 (1992) ("The hole is a buffer, like an insulator in an electric circuit. As a result of the hole between them, the two contacts provide network benefits that are in some degree additive rather than overlapping.").

[266] *See* Strahilevitz, *supra* note 35, at 948.

[267] *Id.*

[268] *Id.* at 949-50 (The author discusses the origin of the Kevin Bacon game. Based on the Internet Movie Database (http://www.imdb.com) Kevin Bacon is a very well connected actor but 1,048 actors are even better connected based on their movies. Number 1 in the database? Rod Steiger.).

[269] *See, e.g.*, Karen Klein Ikkink & Theo van Tilburg, *Broken Ties: Reciprocity and Other Factors Affecting the Termination of Older Adults' Relationships*, 21 Soc. Networks 131, 142-45 (1999) (nonreciprocal relationships decay more than reciprocal).

[270] *See* Strahilevitz, *supra* note 35, at 952 (Two strangers seated next to each other on an airplane might "utter 'it's a small world' upon realizing that they both know someone in common . . . The danger, at least from a privacy perspective, is that people learn to stop being surprised by these encounters, and guard their personal information too much as a consequence.").

[271] *See* Burt, *supra* note 265, at 18.

important to evaluate network structure and cultural barriers to determine the extent to which information will flow through the network.[272]

Not all networks are created equal. The structure of each network can vary immensely, depending on such factors as the number of super-nodes within the network and prevalence of ties within the network. Information is diffused more rapidly through weak ties than strong ties. Therefore the prevalence of weak ties between super-nodes would aid in rapid dissemination of information. The concern about diffusing information this way, however, is that the information tends to be less accurate and credible than information transmitted through strong ties. In addition information that needs to be aggregated for the most useful result may be most effective when transmitted through strong ties. Information flows most efficiently through a high number of active linkages, but when trying to conceal information (e.g., a new business strategy) the network becomes much smaller and only the strong ties remain active. Therefore, although linkages might help information flow efficiently, social network theory does not demand that inevitably the information will flow throughout an individual's network.

Limiting information flow may be necessary for a variety of cultural reasons as well as strategic considerations.[273] Obviously, if accounting tricks are employed to help a firm's bottom line, pragmatic concerns require selective disclosure of the information, most likely to those individuals who are implicated in the activity so that reciprocity will keep the information contained. Another concern limiting information flow is the concern that the information will not reflect the original communication after several disclosures. Information tends to degrade as it is transmitted.[274] In other words, not everyone passes information along to the extent they could based on their ties. Studies suggest that people will pass the information on to others to the extent they believe the information is credible, interesting, and not redundant.[275] Opportunity costs also may be a factor.

In addition to these factors, another critical aspect of privacy involves the content of the information, whether or not a given piece of information is interesting.[276] Interesting information (e.g., an extra-marital affair) will tend to spread quickly within a network of people who share strong ties. Strong ties indicate each individual knows the people involved and, therefore, the information is of particular relevance for all.[277] However, such information has very little currency to someone linked with only a weak tie. Gossip about someone you do not know is not that interesting.

---

[272] *See* Strahilevitz, *supra* note 35, at 970-71.

[273] *See id.* at 971.

[274] *Id.* at 965. This is obvious to anyone who remembers playing the "telephone game" of whispering a message in the ear of the person sitting next to you in a circle and, after it is relayed through everyone in the circle, laughing at the resulting message.

[275] *Id.*

[276] *Id.*

[277] *Id.* at 956.

Thus, people reasonably may expect personal information shared only by people within their social network (both strong and weak tie) to remain private. Although such networks may be well in excess of 1000 people,[278] social network theory suggests that most information about non-public figures would remain confined to the network participants, and would not jump the gap to public knowledge. All such information remains inherently private because it is known only within the expected group.

The increased prevalence of technology may defy the expectations of privacy related to word-of-mouth communication. We all have experienced reading the same story through emails sent from various sources. Rapid diffusion technologies (such as email, text-messages, facebook.com, or blogging) may decrease the opportunity cost of disseminating information, even if it is about people we do not know. This cultural change impacts the flow of information and may expand networks.[279]

The social network theory highlights key privacy insights. First, there is a predictable network within which personal information is disclosed. The disclosure is based on cultural and strategic considerations. Second, how information is disseminated is explained through the strong and weak ties established within networks. Finally, an individual who discloses personal information within a network still expects that the information will remain private and be kept within a controlled group. Social network theory finds that personal information in all likelihood will not jump gaps between networks with any regularity. Data collectors using RFID can re-use and manipulate such data in ways that defy individuals' expectations described in social network theory. When information flows in unexpected ways it challenges whether consent to data collection is valid.

V. AN INTEGRATIVE PRIVACY APPROACH

Regulation of personal information acquired by private entities is largely based on the cornerstone principles of FIPP, notice and consent.[280] The notice and consent construct assumes that individuals reveal personal information and do not intend to retain some level of control over it. All of the theories presented speak to the problem of ownership of personal information. These theories from different academic perspectives agree that the idea of 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 individuals' privacy expectations. The theories demonstrate that 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 these theories as well. Recent economic theory advances the ideas of privacy

---

[278] *See* Peter D. Killworth, *Estimating the Size of Personal Networks*, 12 SOC. NETWORKS 289, 310 (1990) (give or take 400).

[279] Joel R. Reidenberg & Francoise Gamet-Pol, *The Fundamental Role of Privacy and Confidence in the Network*, 30 WAKE FOREST L. REV. 105, 119-20 (1995).

[280] *See supra* Part II.C.3.

regulation.[281] CPM and the social networks theories similarly recognize that advancing technology affects individuals' privacy uniquely.[282] The limitations of FIPP, and even the current relative under-utilization of FIPP tenets by businesses, increase the likelihood of government regulation that could increase technology costs and diminish its practical benefits. FIPP is not without value and represents a practical response to information gathering. However well intentioned, FIPP lacks the strong theoretical basis needed to address the complexities of data collection in the era of modern technology such as RFID. Given this, we offer theoretical research to fashion a more robust model of control and dissemination of personal information.

Industry self-regulation that considers both the on-going interest of individuals and their personal information, and the needs of industry to operate efficiently and effectively, is preferable to piecemeal government regulation. For technology to thrive, the legal model must address the growing issue of personal privacy threats without impinging on business advances. The primary intent of this research was to frame the privacy aspects of indiscriminate data collecting technology such as RFID through theoretical lenses to broaden the discussion of privacy and its legal implications. We summarize our findings by concluding that an effective self-regulation system must first recognize three principles that we identify as the Integrative Considerations. Integrative Considerations are prevalent in research concerning privacy but utterly lacking in law and policy models for promiscuous technology such as RFID.

A. Integrative Considerations

1. The All-or-Nothing Fallacy

First, individuals expect to own, control, and share personal information even after disclosing it. In contrast, the law traditionally understands private information as an asset of the firms to which it is disclosed.[283] Even if an "opt-in" system is utilized, which allows for specific consumer consent for the use of personal information, firms assume full control of information after consent is demonstrated through opting-in.[284] Any privacy protection offered by collecting firms typically reserves the right to change the protections based on the firms' needs.[285] Assuming full control of personal information

---

[281] *See* Acquisti, *supra* note 28, at 27.

[282] *See* Petronio, *supra* note 33, at 45; s*ee* Strahilevitz, *supra* note 35, at 988

[283] *See supra* Part III.

[284] *See* Cate, *supra* note 62, at 38 (noting that economic costs are imposed in this system but that there is no corresponding increase in privacy protection).

[285] *See* Schwartz, *supra* note 30, at 2059. Most credit card owners receive updates to privacy statements on a regular basis. Some businesses put the onus on the consumer to check a website regularly for updates. For example:

> The terms of this policy will govern the use and any information collected while it is in place. SEL reserves the right to change this policy at any time, so please re-visit this page as often as you wish. In case of any material change, we will change the "Last Update Date" in this

disclosed, either by itself or in the aggregate with other disclosed information, as an asset of the firm fails to consider individuals' expectations concerning personal information. Individuals intend to share information. All-or-nothing is a fallacy.

An all-or-nothing approach to disclosure of personal information impedes the ability of individuals to make rational economic trade-off calculations about whether to reveal personal information.[286] Individuals lack key pieces of information because firms treat the personal information as an asset with infinite number of uses now and in the future.[287] CPM emphasizes that individuals' expectation is to coordinate use of personal information after it is disclosed.[288] Information remains within individuals' boundaries, even after it overlaps with the recipients' boundaries. Coordination requires much more than notices that firms have changed their privacy policy.[289] Social network theory implies that coordination involves dissemination of the personal information only within the reasonable networks expected and anticipated by the discloser.[290] Firms that receive personal information do not have full control of that information. Instead, individuals remain the primary owners of their information.

2. Technology as a Rationality-Dampening Influence

Notice and consent as a foundation of privacy law fails to address the reality of advancing technologies.[291] RFID and the vast reach of similar technologies do not permit individuals to understand fully privacy implications of disclosure and to evaluate effectively the opportunity prior to consent.[292]

There is more at work here than simply a lack of adequate explanation when given notice about an RFID device collecting information. Studies show that even sophisticated individuals fail to calculate the risk effectively prior to consent.[293] Rather,

---

> privacy policy and/or post a notice on the site. Changes to this privacy policy are effective as of the stated "Last Update Date" and your continued use of this site on or after the "Last Update Date" will constitute acceptance of, and agreement to be bound by, those changes.

Sony Electronics, Inc. Privacy Policy, *available at* http://products.sel.sony.com/SEL/legal/privacy.html (last visited October 1, 2008).

[286] *See* Acquisti, *supra* note 28, at 24-25.

[287] *See* Nehf, *supra* note 140, at 20-21 (describing DoubleClick's plan to merge data collected online with consumer residence information obtained from a database it acquired).

[288] *See* Petronio, *supra* note 33, at 88-90.

[289] *See supra* note 285.

[290] *See* Strahilevitz, *supra* note 35, at 953-958.

[291] *See supra* notes 133-35 and text accompanying.

[292] *See* Nehf, *supra* note 140, at 19 (noting weak market incentives for evaluating personal information prior to disclosure).

[293] *See supr*a notes 231-33 and text accompanying.

in the face of privacy-invading technology such as RFID, individuals tend to reveal more.[294] This is not solely the result of lack of transparency about the process of collecting information, but a combination of factors that cause individuals essentially to give up trying. Given the growing prevalence of privacy invading devices, individuals have succumbed to a sort of inevitability about disclosures.[295]

This rationality-dampening influence of advancing technologies that significantly challenges individuals' comprehension of the use of their personal information is not a positive result for firms. The predictability of boundaries and social networks provided a basis for regulation through notice and consent. Now, technologies require firms to assume more of the burden of protecting individuals' personal information.

3. The Vast Reach of the Secondary Market

We all expect firms to disseminate information we reveal to a certain extent. A retailer may have customers that are happy to offer personal identity information in return for a store credit card or email communication about discount offers. Behavioral and sociological research offers insights concerning how individuals expect the dissemination of such information. However, a significant threat to personal privacy arises not from the initial disclosure of personal information but more problematically from the subsequent re-use, transfer to third parties, and aggregation of that information.[296]

The market for personal information is vast.[297] Subsequent re-use of information is particularly troublesome because individuals have lost all control of the information.[298] Individuals are not able to make informed decisions about disclosure.[299] But each of these uninformed decisions that reveals relatively small amounts of personal information permits, over time, a detailed picture of an individual to develop.[300] These disclosures have no adequate verification system so the accuracy of that picture is questionable. Information tends to degrade as it is transmitted.[301] Nonetheless firms engage in buying and selling on a vast secondary market with no regard for the personal privacy implications.

---

[294] *See supra* notes 232-33 and text accompanying.

[295] *See* Acquisti, *supra* note 28, at 28 (concluding that individuals cannot make the best decisions concerning privacy for themselves).

[296] *See also* Nehf, *supra* note 140, at 22 ("It is difficult enough to value information when we know about a single user's intended purpose. It is impossible to value when the ultimate destination, aggregation, and use of the information are unknowable.")

[297] *See supra* note 8.

[298] *But see* Schwartz, *supra* note 30, at 2098 (proposing a system that requires a data collector to negotiate further use of transfer of data).

[299] *See* Strandburg, *supra* note 210, at 44.

[300] *See supra* note 226 and accompanying text.

[301] *See* Strahilevitz, *supra* note 35, at 971.

B. Applying Integrative Considerations to RFID

Incorporating these integrative considerations into the discussion of RFID and privacy standards will advance efficiency and effectiveness through technology applications while at the same time advancing legal models beyond a narrow understanding of privacy.[302] Users interested in the vast capabilities of RFID devices should adopt policies that recognize that: 1) individuals expect to own, control, and share personal information, even after disclosing it; 2) advancing technologies raise concerns about bounded rationality and ineffective analysis of the costs and benefits of disclosing personal information; and 3) the significant threat to personal privacy comes not from the initial disclosure of personal information but from the subsequent re-use, transfer to third parties, and aggregation of that information.

A secondary intent of our research is to begin the discussion of potential solutions to managing private data obtained through RFID technology, using the three policy considerations derived from the Integrative Considerations. We offer three specific initial goals for self-regulation of RFID devices: limiting the types of information gathered, setting a timeline for expiration of this information, and protecting the information from re-use and transfer. None of these goals are unique and many businesses currently regulate their data collection using one or more of these goals. However, using these three goals in tandem with an understanding of the Integrative Considerations will result in the best RFID privacy policy. In particular, businesses' data retention policies should include carefully rationalized data expiration policies to minimize the risks associated with personal identity information.

Personal identity information[303] is the data that presents the most serious privacy consequences. Despite this, businesses tend to collect such information routinely, without identifying a clear business need and a plan for protecting the information adequately.[304] Individuals are so accustomed to providing the information that many do not realize information like an email address qualifies as personal identity information. The issue of re-use, transfer, and aggregation means that RFID users must carefully consider the information required and balance that with the privacy concerns of individuals. Keeping this data indefinitely increases the aggregation threat to individuals and risk of liability for data loss to the collectors. A balance of interests necessarily must

---

[302] The increased interest states are showing in legislating RFID presents inefficiencies for businesses required to address the varying requirements of each state based on antiquated notions of privacy. *See supra* Part II.C.2. *But see* Nehf, *supra* note 140, at 55 (suggesting a passive approach to privacy legislation and stating: "Because information privacy in the digital era is still a relatively new concern, a consensus about legitimate entitlements has yet to coalesce. Through experience and experimentation over time, however, those entitlements may emerge."); Stein, *supra* note 113, at 22 (arguing for federal legislation to avoid the inefficiencies of differing state legislation).

[303] Personal identity information is any information that can reveal an individual's identity (including phone number, name, address, physical characteristics, email address, Internet cookies, or personal identification numbers).

[304] The EU Data Privacy Directive contains stringent regulations concerning the collection and use of personal identity information. *See supra* notes 91-95 and text accompanying.

go beyond cost-benefit analysis to consider the implications for individual privacy as detailed in the Integrative Considerations.[305]

Expiration of the data collected is a best practice to address the Integrative Considerations. Many businesses now include expiration of data to protect the privacy of their users.[306] Although a range of time for holding personal identity information may be appropriate for different industries (shopping patterns as opposed to private medical data, for example), we recommend consideration of a twelve-month policy of holding data. Given the rapid dissemination of information and the lack of a universal verification system,[307] twelve-month data expiration allows time for RFID users to utilize accurate data efficiently.

The last goal for an RFID privacy policy potentially is the most difficult to self-regulate. The re-use and transfer of data is one way that businesses profit from a perceived asset of the business. The Integrative Considerations gleaned from diverse academic disciplines demonstrate clearly that the expectation of individuals is for information to remain within expected networks so that the discloser can continue to coordinate the dissemination of that information. Users of RFID devices should study the expected and reasonable network for any information collected through their RFID systems and limit re-use and transfer of data only to firms reasonably related to the initial recipient of information, as documented by the study. Further, the firms that acquire the information must agree to the policy of data expiration and delete transferred data in their own systems consistent with the original collectors' policy dating from the time it was originally collected, not transferred.[308]

VI. CONCLUSION

RFID is a disruptive technology in that it represents a fundamental change in the way individuals live and organizations function. It is not the only disruptive technology with important privacy issues, but we have limited our focus here to applying research across disciplines to the RFID context. At this juncture, a thoughtful approach to RFID standards is critical and that is not possible using outdated privacy models.

We examined relevant research and literature from three diverse disciplines: behavioral economics, communications privacy management, and social networks. From

---

[305] *See* Nehf, *supra* note 140, at 55 (noting the limitations of cost-benefit analysis in privacy policy, stating: "Setting privacy policy is different, however, because important costs and benefits associated with this basic entitlement cannot reliably be reduced to economic terms.").

[306] *See* Rampell, *supra* note 3 (citing Google, Microsoft, Yahoo and AOL as companies that have implemented expiration dates for collected data ranging from 13 months to 18 months).

[307] But see Schwartz, supra note 30, at 2115 (recommending verification through a separate association of decentralized data markets).

[308] Self-regulation potentially could be accommodated within already-existing corporate social responsibility and ethics frameworks of the firm. *See* Gary R. Weaver, Linda Klebe Trevino & Philip L. Cochran, *Corporate Ethics Programs as Control Systems*, 42 ACAD. MGMT. J. 41-57 (1999).

this research we advocate utilizing the Integrative Considerations to guide privacy policy. Finally, these Integrative Considerations can be applied to attempts at self-regulation of the privacy concerns raised by RFID devices. In that regard, we recommend taking account of three crucial goals: limiting the types of information gathered, setting timelines for expiration of collected information, and protecting the information from re-use and transfer.