RADIO FREQUENCY IDENTIFICATION: LEGAL ASPECTS

Reuven R. Levary,[*] *David Thompson, Kristen Kot and Julie Brothers*[**]

Cite as: Reuven R. Levary, et al, *Radio Frequency Identification: Legal Aspects*, 12 RICH. J.L. & TECH. 6 (2005), *at* http://law.richmond.edu/jolt/v12i2/article6.pdf

I. INTRODUCTION

[1] Radio frequency identification (RFID) is a wireless technology that identifies objects without having either contact or sight of them. Unlike optically read technologies such bar codes, RFID tags can be read despite fog, ice, snow, paint or widely fluctuating temperatures.[1] Additionally, RFID can identify moving objects.[2] Data in an RFID tag is stored in an integrated circuit, and sent to the reader via an antenna.[3] An RFID reader is essentially a radio frequency receiver controlled by a microprocessor or digital signal processor. The reader uses an attached antenna to capture

[*] Reuven R. Levary is Professor of Decision Sciences at Saint Louis University. He has held visiting positions at M.I.T., Princeton University, Rensselaer Polytechnic Institute, Yale University, Washington University and the Jet Propulsion Laboratory. His research, teaching and consulting activities are in the areas of computer integrated supply chains and computer simulation.

[**] David Thompson, Kristen Kot and Julie Brothers are completing joint JD/MBA degrees at Saint Louis University.

[1] Ass'n for Automatic Identification and Mobility, *What is Radio Frequency Identification (RFID)?*, http://www.aimglobal.org/technologies/rfid/what_is_rfid.asp (last visited Oct. 24th, 2005); *see also* Mikko Karkkainen and Jan Holmstrim, *Wireless Product Identification: Enabler for Handling Efficiency, Customization and Information Sharing*, 7 SUPPLY CHAIN MGMT: AN INT'L J. 242, 244 (2002).

[2] Ass'n for Automatic Identification and Mobility, *supra* note 1.

[3] *See id.*

the data transmitted from the tag and sends the information to a computer, where the data is processed.[4]

[2] Passive RFID tags have no external power source. Rather, their operating power is generated from a reader device.[5] Passive RFID tags are also very small and inexpensive. Further, they have a virtually unlimited operational life.[6] The characteristics of passive RFID tags make them ideal for tracking materials through supply chains.[7] Wal-Mart has required some manufacturers, suppliers, and distributors to incorporate RFID tags into their products and operations.[8] Other large retailers are following Wal-Mart's lead in requesting RFID tags to be installed in goods along their supply chain.[9] The tags follow products from the point of manufacture to the store shelf. Some manufacturers, like Gillette, see the technology as a major step forward in lowering distribution and product tracking costs.[10] Even the United States military plans to use RFID to improve the flow of supplies to military bases and troops stationed around the world.[11]

[3] RFID technology will significantly increase the effectiveness of tracking materials along supply chains and substantially reduce loss retailers accrue from thefts. The data transmitted via the tag can provide a wealth of information. For example, it can ascertain product identification and location as well as when and where the product was purchased. Sun Microsystems designed RFID technology to reduce or eliminate drug counterfeiting in pharmaceutical supply chains.[12] This technology "will make the copying of medications either extremely difficult or

[4] *Id.*
[5] *Id.*
[6] *Id.*
[7] *See* Karkkainen and Holmstrom, *supra* note 1, at 246.
[8] Alorie Gilbert, *Wal-Mart Tagging Fuels RFID Market*, CNET NEWS.COM, Dec. 22, 2004, http://rfidgazette.org/walmart/ (scroll to "Wal-Mart Pushes RFID Market;" then click on "Wal-Mart Tagging Fuels RFID Market").
[9] *Id.*
[10] Carol Sliwa, Gillette Shaves Costs with RFID, COMPUTERWORLD, Jan. 5, 2005, http://www.techworld.com (search for "Gillette Shaves Costs").
[11] Gilbert, *supra* note 8.
[12] Robert Jaques, *Sun Pushes RFID Drug Technology*, Feb. 20, 2004, http://www.vnunet.com (search "News" for "'Sun Pushes RFID Drug Technology'").

unprofitable."[13] Delta-Air Lines Inc. successfully used RFID tags to track pieces of luggage from check-in to planes.[14] The luggage tracking success rate of RFID was much better than that provided by bar code scanners.[15]

[4] Active RFID tags, unlike passive tags, have an internal battery.[16] The tags have the ability to be re-written and/or modified.[17] The read/write capability of active RFID tags is useful in interactive applications such as tracking work-in-progress or maintenance processes.[18] Active RFID tags are larger in size and more expensive than passive RFID tags.[19] Because both passive and active RFID tags have a large, diverse spectrum of applications they have become the standard technologies for automated identification, data collection, and tracking. Vast amounts of data can be recorded by RFID tags. The storage and analysis of this data will pose new challenges to the design, management, and maintenance of data bases as well as to the development of data mining techniques. An extended list of RFID applications and implementations is given by Karkkainen and Holmstrom.[20]

II. CONSUMER PRIVACY CONCERNS

[5] While the retail and manufacturing industries see the many benefits RFID technology offers to their operations, many consumers and consumer advocacy groups see the advancement of RFID technology, and its application to everyday products as jeopardizing consumer privacy. The implementation of RFID will make it possible to create massive databases integrating unique tag data.[21] Conceivably, these databases will

[13] *Id.*
[14] Bob Brewin, *Delta Says Radio Frequency ID Devices Pass First Bag-Tag Test*, COMPUTERWORLD, Dec. 22, 2003, http://www.computerworld.com/industrytopics/travel/story/0,10801,88446,00.html.
[15] *Id.*
[16] *See* Ass'n for Automatic Identification and Mobility, *supra* note 1.
[17] *Id.*
[18] *Id.*; *see also* Karkkainen and Holmstrom, *supra* note 1, at 244.
[19] Ass'n for Automatic Identification and Mobility, *supra* note 1.
[20] Karkkainen and Holmstrom, *supra* note 1.
[21] Privacy Rights Clearinghouse, *RFID Position Statement of Consumer Privacy and Civil Liberties Organizations*, Nov. 20, 2003, http://www.privacyrights.org/ar/rfidposition.html.

be linked to personal identifying data.[22] Civil liberty organizations are trying to stop RFID tagging of consumer goods because the potential of this technology in affecting consumer privacy**.** Three of the most outspoken advocacy groups are the Consumers Against Supermarket Privacy Invasion And Numbering (CASPIAN), the American Civil Liberties Union (ACLU), and the Electronic Privacy Information Center (EPIC). These organizations joined together to publish the *RFID Position Statement of Consumer Privacy and Civil Liberties Organizations*.[23] This publication details many consumer concerns over the use of RFID technology in the retail industry.

[6] The first threat to privacy outlined in the RFID Position Statement relates to the fact that RFID tags can be hidden inside objects without customer knowledge.[24] This would make it possible for individuals to read the RFID tags for the lifetime of the product, without the consumer ever having knowledge of the tag's existence. This effect will be magnified if, as many experts believe, millions of RFID readers appear in airports, on highways, at seaports, in retail stores, and every location imaginable around the globe.[25] At each of these locations, RFID tags secreted in consumer goods can be read without consumer knowledge or consent.

[7] Advocacy groups also voice concerns that the receivers, like the tags themselves, can be hidden from consumer sight.[26] To proponents of RFID technology, however, the lack of a line of sight restriction is an advantage. "RFID readers have already been experimentally embedded into floor tiles, woven into carpeting and floor mats, hidden in doorways, and seamlessly incorporated into retail shelving and counters, making it virtually impossible for a consumer to know when or if he or she was being 'scanned.'"[27]

[8] With its initial RFID experimentation in stores, Wal-Mart demonstrated the consumer is typically unaware when an item they are

[22] *Id.*
[23] *Id.*
[24] *Id.*
[25] *See id.*, at attachment 1.
[26] *Id.*
[27] *Id.*

purchasing, wearing, or carrying contains an RFID tag.[28] A store, airport, or other establishment a consumer enters may be scanning his or her possessions without their knowledge. Consumer advocacy groups argue these two combined factors greatly reduce the ability of individuals to be anonymous consumers.[29]

[9] Concern about the advent of the Electronic Product Code (EPC) is also voiced in the RFID Position Statement.[30] An EPC is a product numbering standard being developed by the Uniform Code Council and EAN International.[31] Traditionally, products are identified by the Universal Product Code (UPC), but the UPC does not distinguish between like products. To a computer system scanning UPC, for example, two DVDs sharing the same title were equivalent. With the advent of EPC, these same DVDs could be distinguished from one another and the individual item or product uniquely identified.[32] Consumer groups worry individual items can be registered via a global item system and then linked to the purchaser of that item.[33] These groups are uncomfortable with new RFID technologies. They anticipate the creation of massive databases containing unique RFID tag data that can link tags and people, and then be used for unfair marketing.[34]

[10] Similarly, consumer groups fear that the unique identifying data stored in an RFID could be used to track and profile individuals.[35] For example, the RFID Position Statement writes, "a tag embedded in a shoe could serve as a de facto identifier for the person wearing it . . . identifying items people wear or carry could associate them with, for example, particular events like political rallies."[36] Monitoring would make it possible for the government to track individuals more easily, and for corporations to further intrude on individuals' private lives. Thus,

[28] *Id.*, at attachment 1.
[29] *See id.*
[30] *Id.*
[31] Wikipedia, http://en.wikipedia.org/wiki/Electronic_Product_Code.
[32] *See* Privacy Rights Clearinghouse, *supra* note 21.
[33] *Id.*
[34] *Id.*
[35] *Id.*
[36] *Id.*

consumer groups believe RFID technology may potentially interfere with an individual's right to travel in relative anonymity.

III. PROPOSALS FOR REGULATION

[11] Different interest groups, including CASPIAN and the ACLU, have expressed concerns over the use of RFID technology, and the need for adequate regulation.[37] Several states have already begun discussing legislation to protect consumer rights.[38] RFID industry leaders, however, want to take a prominent role in setting up guidelines for RFID use and are urging lawmakers to let them do so.[39]

[12] Advocacy groups are demanding RFID technology be regulated by both the states and the industry.[40] In 2003, CASPIAN introduced the RFID Right to Know Act of 2003 ("Act"), a model act designed to regulate the early stages of the RFID boom.[41] At least one state has used the Act as a model for legislation regulating RFID technology.[42] The proposed legislation states that consumer packages having an RFID tag must be labeled as such.[43] The label must explain that the tag can transmit

---

[37] *See* Privacy Rights Clearinghouse, *supra* note 21.
[38] Mark Roberti, *The Law and the Land*, Mar. 1, 2004, http://rfidjournal.com/article/print/811/-1/2/; Jerry Brito, *Relax Don't Do It: Why RFID Concerns are Exaggerated and Legislation is Premature*, 2004 UCLA J. L. TECH. 5, § III(A) (2004) (reporting that California, Utah, and Missouri legislatures have introduced bills regulating RFID, and a legislator in Massachusetts says he will follow suit).
[39] Alorie Gilbert, *California Lawmaker Introduces RFID Bill*, CNET NEWS.COM, Feb. 24, 2004, http://news.com.com/2102-1014_3-5164457.html (explaining that EPCglobal, Proctor & Gamble, Gillette, the National Retail Federation, and others have formed a lobbying group to influence public policy, and according to a spokesman from pro-RFID EPCglobal, the group has already met with members of Congress).
[40] *E.g.*, Privacy Rights Clearinghouse, *supra* note 21; Mark Baard, *Lawmakers Alarmed by RFID Spying*, WIRED NEWS, Feb. 26, 2004, http://www.wired.com/news/privacy/0,1848,62433,00.html; Spychips, *Consumer Group Unveils RFID Labeling Legislation*, June 11, 2003, http://www.spychips.com/press-releases/right-to-know-release.html.
[41] C.A.S.P.I.A.N., *RFID Right to Know Act of 2003*, http://www.nocards.org/rfid/rfidbill.shtml (last visited Oct. 22, 2005).
[42] Baard, *supra* note 40 ("Utah's Right to Know Act is based on federal legislation drafted by the consumer privacy group [CASPIAN].").
[43] C.A.S.P.I.A.N., *supra* note 41 (amending 15 U.S.C. § 1453(a) by inserting as subsection (7) "A consumer commodity or package that contains or bears a radio

unique identifying information to an independent reader both before and after purchase.[44] The legislation stipulates that this "warning label" must be conspicuous both in type-size and location, and should have print that contrasts with the background against which it appears.[45] The Act also states businesses shall not combine or link an individual's nonpublic personal information with RFID tag identification information beyond that which is needed to manage inventory.[46] CASPIAN's proposed legislation amends Title 15 of the United States Code. It inserts a section designating the Federal Trade Commission as the agency to establish standards for businesses to ensure the integrity and confidentiality of an individual's records and information, and specifies that businesses should not use RFID information to identify individuals.[47]

[13] RFID regulation based largely on CASPIAN'S proposed legislation has already begun in a number of states.[48] While these state bills do not go as far as many consumer groups might wish, it appears these regulations will deter many of the privacy infringements made possible by RFID technology.

[14] The first state to pass legislation was Utah.[49] The Utah Bill, titled "Radio Frequency Identification- Right to Know Act," requires a retailer selling a product containing an RFID tag must inform the consumer about the tag's existence by labeling the package or posting notices both near the product and also at the location where the consumer transaction will be completed.[50] The notice must state that the product contains an RFID tag and that the tag can transmit information to a reader both before and after the sale.[51] The signs must be conspicuous in size and location, unless the seller automatically disables the tag prior to the completion of the sale.[52]

---

frequency identification tag shall bear a label as provided in paragraph (9) of this subsection.").
[44] *Id.*
[45] *Id.*
[46] *Id.*
[47] *Id.*
[48] Baard, *supra* note 40; Brito, *supra* note 38.
[49] Baard, *supra* note 40.
[50] H.B. 251, 56th Leg., Gen. Sess. (Ut. 2004).
[51] *Id.*
[52] *Id.*

[15] In February of 2004, State Senator Debra Bowen introduced similar legislation in California to address consumer privacy issues.[53] Her bill required businesses and agencies to notify consumers that an RFID system is in place that can track and collect information about them.[54] The bill required consumers to give express consent before businesses or agencies could track and/or collect information about them via RFID.[55] Additionally, the California bill required retailers obtain express consent before they are allowed to use loyalty cards in which they track purchases of the consumer.[56] This consent is necessary because consumers are apprehensive about how the data collected by the RFID tags can be "linked to an individual's credit card to identify them personally."[57] Senator Bowen suggests that "[i]t's one thing to know you are dealing with customer 442, and it's another thing to know you are dealing with Jane Doe and her social security number is such and such and her address so and so."[58] The California bill required businesses to destroy or detach the RFID tags before consumers leave a store.[59] However, the California legislature ultimately rejected Senator Bowen's bill.[60]

[16] Massachusetts State Senator Jarrett Barrios is drafting legislation to regulate the use of RFID technology.[61] His bill will most likely resemble the bills reviewed in California and Utah, and will emphasize "that consumers have a right to know RFID is being used, that consumers can opt out of using the technology at the point of purchase, and that consumers can deactivate that [sic] RFID tags at the point of purchase."[62]

---

[53] Gilbert, *supra* note 39.
[54] *Id.*
[55] *Id.*
[56] *Id.*
[57] *Bowen Seeks Balance in RFID Law*, RFID J., Mar. 1, 2004, http://www.rfidjournal.com/article/articleview /812/1/1/.
[58] *Id.*
[59] *Id.*
[60] Claire Swedberg, *California RFID Legislation Rejected*, RFID J, Jul. 5, 2004, www.rfidjournal.com/articleview/1015/1/1/.
[61] Beth Bacheldor, *RFID Legislation Gains Response*, InformationWeek, Apr. 27, 2004, http://www.informationweek.com/ (search "Bacheldor RFID Gains").
[62] *Id.*

[17] Producers and users of RFID technology seem to believe regulation is unnecessary.[63] They argue tags are not cheap enough to be used widely, and readers are not prevalent enough to track individuals seamlessly.[64] They also suggest the range of an RFID tag is too narrow to allow the tracking of an individual.[65] The RFID industry prefers deactivation at the point of purchase rather than legislated regulations.[66] The industry also suggests consumers who are opposed to RFID use should acquire an RFID blocker tag which will theoretically disrupt transmission of information sent via the RFID tag.[67] Such a blocker tag does not yet exist.[68]

IV. FEDERAL STATUTES

[18] "Title III/ECPA (Electronic Communications Privacy Act) outlaws wiretapping and other forms of electronic eavesdropping, possession of wiretapping or electronic eavesdropping equipment, use or disclosure of information obtained through illegal wiretapping or electronic eavesdropping, and in order to obstruct justice, disclosure of information secured through court-ordered wiretapping or electronic eavesdropping, 18 U.S.C. 2511."[69] In essence, this act prohibits "any person from intentionally intercepting, or endeavoring to intercept wire, oral or electronic communications by using an electronic, mechanical or other device unless the conduct is specifically authorized or expressly not covered . . . ."[70] Although wiretapping is not identical to RFID, it shares an abundance of similarities that may carry over to RFID technology.

---

[63] Swerdberg, *supra* note 61 (discussing how Hewlett Packard and the Grocery Manufactures of America were among the groups opposed to Sen. Bowen's RFID legislation in California).
[64] Electronic Privacy Information Center, *Radio Frequency Identification (RFID) Systems*, Oct. 7, 2005, http://www.epic.org/privacy/rfid/ (stating that although the cost of tags is declining, readers represent a considerable investment for consumers).
[65] Declan McCullagh, *RFID Tags: Big Brother in Small Packages*, CNET NEWS.COM, Jan. 13, 2003, http://news.com.com/ (search "RFID Tags Big Brother") (discussing the limited range of current RFID technology).
[66] Privacy Rights Clearinghouse, *supra* note 21.
[67] *Id.*; *see also* Matt Hines, *RSA Polishes RFID Shield*, CNET NEWS.COM, Feb. 24, 2004, http://news.com.com/2100-1029-5164014.html (discussing a cloaking system to confuse RFID readers outside a certain range).
[68] Privacy Rights Clearinghouse, *supra* note 21.
[69] GINA STEVENS & CHARLES DOYLE, PRIVACY: WIRETAPPING AND ELECTRONIC EAVESDROPPING 8 (2002).
[70] *Id.* at 9.

Capturing wire, oral, or electronic communications violates the ECPA only if "the conversation or other form of communication intercepted is among those kinds which the statue protects, in over simplified terms - telephone (wire), face to face (oral), and computer [sic] electronic)."[71] RFID technology will likely fall under the electronic category. "Congress used the definitions of three forms of communications to describe the communications beyond the Act's reach as well as those within its grasp."[72] For example, "[r]adio and data transmissions are generally 'electronic communications.'"[73] "[E]lectronic communication means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric or photo-optical systems that affects interstate or foreign commerce . . . ."[74]

[19] Although the legalities of interceptions of oral, wire, or electronic communications were detailed above, there are exemptions. One is consent interceptions.[75] "Wiretapping or electronic eavesdropping by either the police or anyone else with the consent of at least one party to the conversation is not unlawful under the federal statute."[76] Consent, under federal law, may be either explicit or implicit.[77]

[20] At the base level, the Wiretap Act sets the stage for accessing information and the ramifications of doing so. In summary, it suggests what constitutes a criminal act (e.g. intentional access to electronic communication without authorization) and stipulates punishment.[78] In some instances, an act must demonstrate both intent and action. *Mens rea*, or "guilty mind," is critical in such a case. Obtaining the information is not in itself a crime; it is the intention that matters.[79] The language "for the

[71] *Id.* at 13.
[72] *Id.*
[73] *Id.*
[74] *Id.* at 14 n.31 (quoting 18 U.S.C. § 2510(12) (2000 & Supp. 2002)).
[75] STEVENS & DOYLE, *supra* note 69.
[76] *Id.* at 14–15.
[77] *Id.* at 15.
[78] 18 U.S.C. § 2511 (2000 & Supp. 2002); *see generally* STEVENS & DOYLE, *supra* note 69, at 8–20 (laying out the various elements of the ECPA).
[79] *See In re* Pharmatrak, Inc., 329 F.3d 9, 22 (1st Cir. 2003), *rev'g* 220 F. Supp. 2d 4 (D. Mass. 2002).

purposes of" places a high burden of proof on the prosecutor.[80] Simply knowing or being aware a crime might or is taking place is insufficient to meet the burden.

[21] In one case invoking this statute, the plaintiffs brought a class action suit against an Internet research company that had been placing "cookies" on their personal computers to track activity. The district court held that, "[p]laintiffs have produced no evidence 'either (1) that the primary motivation, or (2) that a determinative factor in the actor [Pharmatrak's] motivation for intercepting the conversation was to commit a criminal [or] tortuous . . . act.'" [81]

[22] To be criminally or civilly liable under the Electronic Communications Privacy Act (EPCA), the unlawful interception must be intentional.[82] While First Circuit Court of Appeals reversed and remanded the district court's decision in *Pharamtrak*, it did set out the legal standard to be applied in deciding intention.[83] The court noted that in the 1986 amendment of the EPCA Congress changed the state of mind requirement from "willful" to "intentional."[84] The ECPA's legislative history notes the term "intentional" requires more than voluntary conduct. "Such conduct or the causing of the result must have been the person's conscious objective."[85] The court went on to explain that by defining "intentional" in such a narrow manner, "Congress made clear that the purpose of the amendment was to underscore that inadvertent interceptions are not a basis for criminal or civil liability under the EPCA."[86]

[80] *Id.* at 19.
[81] *Id.* at 12 (quoting United States v. Vest, 639 F.Supp. 899, 904 (D. Mass. 1986)); *See generally* Griggs-Ryan v. Smith, 904 F.2d 112, 117-19 (1st Cir. 1990); Gilday v. Dubois, 124 F.3d 277, 297 (1st Cir. 1997); Williams v. Poulos, 11 F.3d 271, 281-82 (1st Cir. 1993); United States v. Footman, 215 F.3d 145, 155 (1st Cir. 2000); Berry v. Funk, 146 F.3d 1003, 1010–1011 (D.C. Cir. 1998); Watkins v. L.M. Berry & Co., 704 F.2d 577, 581 (11th Cir. 1983).
[82] § 2511.
[83] *In re Pharmatrak, Inc.*, 329 F.3d at 23.
[84] *Id.* at 23.
[85] S. Rep. No. 99-541, at 23 (1986).
[86] *In re Pharmatrak, Inc.*, 329 F.3d at 19.

[23] The statute presents an overview of the possible legalities that may be applicable to RFID technology. It indicates that anyone who intercepts electronic communication will be held in violation of it if proper consent has not been obtained.[87] As RFID technology will most likely be classified as electronic communication, it is reasonable to assume that it, too, cannot be employed to obtain and use information legally unless consent is given. While the statute refers specifically to wiretapping, RFID is incredibly similar to wiretapping in its use in that those persons using a wiretap or RFID technology are trying to gather information.

[24] "RFID technology and its implementation must be guided by strong principles of fair information practices."[88] The Privacy Guidelines of the Organization for Economic Co-operation and Development (OECD) offers useful advice related to the disclosure of RFID technology use and the purpose behind its use.[89] Once businesses equip products and goods of any kind with RFID tags, businesses will have a duty to disclose the use of this technology.

> RFID users must make public their policies and practices involving the use and maintenance of RFID systems, and there should be no secret databases. Individuals have a right to know when products or items in the retail environment contain RFID tags or readers. They also have the right to know the technical specifications of those devices. Labeling must be clearly displayed and easily understood. Any tag reading that occurs in the retail environment must be transparent to all parties. There should be no tag-reading in secret.[90]

[25] Additionally, users of this technology should make public the purpose for which the readers and tags are being used.[91]

> The duty to disclose and the corresponding liability for a failure to disclose may also arise when a party fails to

[87] 18 U.S.C. § 2511 (2000 & Supp. 2002).
[88] *See* Privacy Rights Clearinghouse, *supra* note 21.
[89] *Id.*
[90] *Id.*
[91] *Id.*

> exercise reasonable care to disclose a material fact which may justifiably induce another party to act or refrain from acting, and the nondisclosing party knows that failure to disclose such information to the other party will render a prior statement or representation untrue or misleading.[92]

V. CONTRACTS

[26] Once RFID is implemented, contracts between businesses and consumers will probably be created. Consent to use of RFID technology will likely be given, similar to the consent of wiretapping and electronic eavesdropping. The consent is apt to be considered a contract between the consumer and the business; creating contracts that are both express and implied. An express contract is one where terms are stated by the parties, either orally or in writing.[93] An implied contract is one in which some or all of the terms are "inferred from the conduct of the parties and the circumstances of the case, though not expressed in words."[94] An implied contract can either be implied in fact or in law. An implied in fact contract "is a true contract, which arises if the assent of the parties is manifested by conduct rather than words . . . ."[95] A contract implied in law, also known as a quasi contract, "is an obligation created by law in the absence of any agreement between the parties."[96] An implied contract "has the same legal effect as an express contract; it carries as much weight and is as binding as an express contract."[97]

[27] Thus, users of RFID technology will likely be obliged to disclose their use of it. Customers and patrons will have to be made aware of the fact that the products in that users' store are being electronically tracked. This will, in turn, necessitate that users attain consent from patrons. The consent could be obtained through an express written agreement, giving rise to an express contract. In such a case, the patron will likely have to sign or orally consent to the RFID tags. However, this consent may just be implied. If so, it will give rise to an implied contract. By patrons

[92] 37 AM. JUR. 2D *Fraud And Deceit* § 204 (2001).
[93] 17A AM. JUR. 2D *Contracts* § 12 (2004).
[94] *Id.*
[95] *Id.*
[96] *Id.*
[97] *Id.*

shopping in the store, as long as the RFID user had visibly disclosed that the technologies were in use, would imply consent to the contract. The Computer Fraud and Abuse Act of 1986 (CRAA) makes it illegal to access a computer that is protected unless there is "authorization."[98] The Act forbids a person who has a legitimate and authorized right of access from "exceeding authorized access."[99] The CRAA also prohibits dissemination of malicious software[100] or trafficking of stolen passwords.[101] The CRAA allows for civil relief through compensation or injunction.[102]

[28] Given the paramount importance of privacy to many consumers, express contracts may conceivably be formed when RFID technology is initially implemented in the retail industry. This actual signing of a contract will make the public fully aware of the rights that they have and the liabilities businesses assume if misuse of information occurs. Once the implementation and acceptance phase of RFID tags has come and gone, and the public has been reassured regarding proper usage of the technology, it is conceivable that implied contracts will become more standard.

VI. PRINCIPLES OF FAIR INFORMATION PRACTICE

[29] RFID technology not only has the ability to track products and persons, it also has the ability to collect individual information. As such, the Principles of Fair Information Practice[103] would seem to play a role in the legalities of RFID. The Federal Trade Commission of Consumers has developed the Fair Information Practice Principles. It address "the safeguards required to assure those practices are fair and provide adequate privacy protection."[104] Government agencies in the past quarter century have deliberated the way in which entities gather, collect, and use personal

[98] 18 U.S.C. § 1030 (2000 & Supp. 2005)
[99] *Id.* at § 1030(a)(1).
[100] *Id.* at § 1030(a)(5)(A)(i).
[101] *Id.* at § 1030(a)(6).
[102] Mark G. Milone, *Hacktivism: Securing the Infastructure,* COMPUTER AND INTERNET LAWYER, March 2003.
[103] Federal Trade Commission, *Fair Information Practice Principles,* http://www.ftc.gov/reports/privacy3/fairinfo.htm (last visited Oct. 25, 2005).
[104] *Id.*

information. A succession of reports and guidelines identified five central principles of privacy protection:

1. Notice and awareness of collection of information.

2. Choice and consent as to how this information can be used.

3. Access to the individual's gathered information, and the ability to contest the accuracy of the collected data.

4. Integrity and security of data.

5. Enforcement of the aforementioned principles[105]

[30] Because RFID technology can be used as a marketing tool, a tracking device, and a way to collect personal information, these principles will play an active role in addressing some of the vital concerns that have arisen with the evolving RFID technology. Although these principles were developed to address privacy concerns, they speak to the topics discussed previously including the duty to disclose (notice and awareness) and the contracts likely to be created (choice and consent).

VII. SEARCHES, SEIZURES, AND LAW ENFORCEMENT USES

[31] RFID technology will likely affect law enforcement's ability to gather evidence to prosecute crimes. The Fourth Amendment of the Constitution protects citizens from unreasonable searches and seizures by the government and specifies that warrants can not be issued without probable cause.[106] Information generated from RFID technology could be useful in conducting an investigation, but the methods of obtaining the information must coincide with the rights of the citizens. To determine a method for using RFID, it would be reasonable to draw analogies from laws regarding electronic and wireless information.

[105] *Id.*
[106] U.S. CONST. amend. IV.

[32] Since computers are often the source of electronic information, they could conceivably offer a gold mine of evidence. If an employee used an employer's computer to commit an illegal activity, for example, the employer who inadvertently discovered that information through routine computer maintenance could contact the authorities.[107] Two federal cases have upheld instances where employers had found evidence of illegal activity and the evidence was allowed because the employer's policies made it possible to cooperate with police.[108] Whether the place of employment is public or private, the employer must make their policies quite clear to employees. Employees must not have an expectation of privacy from employers if privacy is actually non-existent.[109]

[33] The USA Patriot Act of 2001[110] gave law enforcement more leeway regarding criminal investigations. The 400-page piece of legislation composes primarily of amendments to previous laws' regulation investigation procedures.[111] Although the legislation was initially intended to combat terrorism, other implications exist. For example, the standards of obtaining a warrant were lowered to make them relevant to any ongoing investigation, the government can delay notification of the warrant.[112] Further, employers may monitor "computer trespassers" without a warrant.[113] If computers affect interstate or foreign commerce or communication, the US government can monitor them even if they are located outside the country.[114]

[34] RFID may be an effective tool in criminal investigations. It is conceivable, for example, that an RFID chip could be used to identify the

[107] Frank C. Morris, Jr., *The Electronic Platform: Email and Other Privacy Issues in the Workplace,* 20 NO. 8 COMPUTER & INTERNET LAW. 1, 6 (2003).
[108] *Id.* at 7 (referencing United States v. Slania, 283 F.3d 670 (5th Cir. 2002); and United States v. Angevine, 281 F.3d 1130 (10th Cir. 2002)).
[109] *Slania*, 283 F.3d at 675–677.
[110] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) [hereinafter Patriot Act].
[111] *Id.*
[112] Morris, *supra* note 106, at 8 (citing Patriot Act § 213(b)(1)).
[113] *Id.* (citing Patriot Act § 217(21)(A)).
[114] Milone, s*upra* note 101, at 3 (citing 18 U.S.C. § 1030(e)(2)(B)).

original purchaser of an item found at a crime scene.[115] Crime Scene Investigators might also find RFID useful in keeping track of the evidence collected from crime scenes. Further, tagging of evidence might help to reduce the human error connected with cataloging.[116] The technology could also be used to identify someone in a crowd.[117] FBI agents use wireless technology to monitor criminal activity. RFID technology could replace wireless in the future.[118]

[35] Finally, RFID technology could be useful in deterring shoplifting and other theft. Clearly, it would be impossible for a person to pick up and walk off with a store item carrying an RFID chip. The sensor would, of course, go off. By using such technology to catch people "red-handed," RFID would likely deter some criminals and undoubtedly help in the prosecution of others. However, while this technology appears promising, it is not foolproof. Evidence from an RFID sensor would be hard to refute, but malfunctions occur with technology. The possibility of false arrests and convictions are legal realities that should be considered by RFID users.

VIII. CONCLUSIONS

[36] As RFID technology rapidly becomes a mainstream part of the retail industry, it will most assuredly revolutionize production and operation management throughout the world. The technology, however, comes with a cost. This cost is the invasion of consumer privacy. People may be monitored unknowingly by businesses or the government and personal liberties jeopardized. To protect consumer privacy rights, advocacy groups are banding together to stipulate fair and forthright uses of this new

---

[115] *See generally, Talk of the Nation: Radio Frequency Identification Causes Privacy Concerns* (NPR radio broadcast Oct. 13, 2004) (describing how experts have anticipated both beneficial and problematic uses for RFID tags).

[116] *See RFID Tags DNA Samples in World First,* SUPPLY CHAIN, Sept. 28, 2005 (magazine), *available at* http://www.supplychainreview.com.au/index.cfm?li=displaystory&StoryID=24624; and *World First fpr Queensland Forensic Lab*, FERRET, Sept. 27, 2005, http://www.ferret.com.au/articles/65/0c037065.asp (discussing an Australian forensic lab's use of RFID to ensure the integrity of DNA samples).

[117] *Id.*

[118] *See* Larry Barrett and Sean Gallagher, *NORA and ANNA*, EWEEK.COM, April 4, 2004, http://www.eweek.com/article2/0,1895,1567701,00.asp.

technology.[119] States are beginning to regulate the RFID industry by enacting legislation that keeps with the demands of the consumer advocacy groups.[120]

[37] RFID technology fast approaches the massive implementation phase in a number of industry sectors,[121] and the legal issues that come to life with its uses are vast. The definition of privacy will eventually define technological crimes. New crimes will be created, but new methods of crime prevention and investigation will be created as well. While the law is always inevitably a few steps behind technology, the law always catches up. In time, laws will closely guide both manufacturers and users of RFID technology.

[119] Privacy Rights Clearinghouse, *supra* note 21.
[120] Roberti, *supra* note 38.
[121] Gilbert, *supra* note 8.