Santa Clara University
School of Law

Santa Clara High Technology Law Journal

Volume 22 | Issue 4

Article 2

2006

RFID and Other Embedded Technologies Who Owns the Data

Lars S. Smith

RFID AND OTHER EMBEDDED TECHNOLOGIES: WHO OWNS THE DATA?

Lars S. Smith†

INTRODUCTION

You have just purchased an item of tangible personal property—a car, a refrigerator, or a new shirt. You own the item, of course, because under U.C.C. Article 2, when you pay consideration to the seller, title transfers to you.

Although you are the owner of the item, the manufacturer (or possibly the distributor) has placed devices on the item to help the manufacturer track the item. This is generally referred to as automated identification technologies (Auto-ID).[1] You are aware and probably approve of the use of bar codes, because they speed up the process of buying the item. Although you probably do not give it much thought, you usually throw away the packaging that contains the bar code, and so there is no risk that your use of the item can be tracked at a later date.

However, because of the need for human intervention and the potential for errors in capturing data, bar codes are not the best way to track an item through the distribution system. Barcodes must be scanned by a laser, which requires them to be within the line of sight of the scanner. Instead, the distributor, a major international retailer with the clout to make demands on its suppliers, now insists that a new form of Auto-ID be placed on the item, one that requires no

† Assistant Professor of Law, Louis D. Brandeis School of Law, University of Louisville. I am grateful for the many suggestions I received at the Santa Clara Computer & High Technology Law Journal symposium, *Privacy in the Information Age*, Jan. 27, 2006, where this article was first presented. In particular, I wish to thank Dorothy Glancy, Sonia Katyal, and Nicole Ozer, who took the time to provide in depth comments as members of the panel at the symposium. I would also like to thank Auric Steele and Robyn Lurding for their invaluable assistance in researching this article.

[1] Mark Roberti, *What is RFID*, RFID JOURNAL, http://www.rfidjournal.com/article/articleview/1339/1/129 (last visited Mar. 24, 2006). Also known as AIDC, see Automated Identification and Data Capture, http://en.wikipedia.org/w/index.php?title=Automated_identification_and_data_capture&oldid=47550267.

human intervention to read, and can be tracked down to the individual item anywhere along the supply chain—a radio frequency identification tag (RFID tag).[2]

These RFID tags, or just tags, can be quite small. A tag requires no direct human interaction to operate, can be activated remotely by radio transmissions, and can broadcast its signal through walls. In addition, the system is designed so that each tag has a unique identification code, allowing the merchant to distinguish between individual items containing tags. It's so unobtrusive that you the consumer do not even notice that your sweater has a tag attached to the collar. The tag may even allow the retailer to collect information about the item, such as where it has been anywhere on the globe, how it has been operated, and any other information tracked by sensors built into the tag. If the tag is embedded in your car, the amount of information tracked could be quite extensive. If the tag is more sophisticated, it may also have its own power source, which gives it the ability to store data about your location, the use of the item in which it is embedded, and any other piece of information the manufacturer can track through the tag. Should you care? And whose information is it, anyway?

At the moment, this technology is primarily being used for inventory control at the distribution level, with the tags being placed on containers and packages.[3] This allows major retailers to follow the product all the way through the supply chain, from the manufacturers' warehouses to the retailers' stores. Wal-Mart, for example, is requiring its one hundred largest suppliers to place an RFID tag on all palettes of products, which Wal-Mart has found can reduce out-of-stocks by as much sixteen percent.[4]

More sophisticated applications may be on the horizon. Hitachi has produced an RFID tag the size of a grain of sand, making item level tagging a distinct possibility. Industry proponents promote the

[2] Wal-Mart is one of the leading proponents of this technology. *See* Tutorial-Reports.Com, *Wal-Mart and RFID: A Case Study*, http://www.tutorial-reports.com/wireless/rfid/walmart/expectations.php.

[3] *RFID 101 The Future Is Here: A Beginner's Guide to RFID* (June 28, 2004), RFID GAZETTE, http://www.rfidgazette.org/2004/06/rfid_101.html ("The main application for this today is tracking products along a supply chain."). While such "supply chain management" is a large part of current RFID uses, RFID systems have been installed in other areas, such as asset management, tracking parts during manufacturing, and payment systems. *Getting Started RFID Business Applications*, RFID JOURNAL, http://www.rfidjournal.com/article/articleview/1334/1/129.

[4] Mark Roberti, *EPC Reduces Out-of-Stocks at Wal-Mart*, RFID JOURNAL, Oct. 14, 2005, *available at* http://www.rfidjournal.com/article/articleprint/1927/-1/1/.

technology as providing a wide variety of benefits to businesses[5] and consumers.[6] However, even if the technological challenges are overcome, it will likely be some time before the economics make sense.[7]

This article will explore the extent to which someone can own or control the information contained on the tag, and who that person is. Part I will discuss the technology—both currently available and under development—for implementing RFID. Part II will discuss direct ownership of the data contained on the tag under such theories as copyright law. Part III will discuss ownership of the data through ownership of the hardware. Part IV will discuss how a manufacturer might be able to control access to the data, even where it does not own the data or the hardware. While there are many interesting privacy issues related to RFID technology and tracking of personal information by companies and the government,[8] this article will focus on issues of ownership of the information contained on the chip.

I. THE TECHNOLOGY

The legal concerns discussed in this article are raised by the development of several different technologies: first, the development of "smart goods"; second, the miniaturization of computer technology; and third, the development of real time automatic tracking technology.

The concept of a "smart good" involves the merger of traditional manufactured goods with information technology by way of the inclusion of computer technology in goods other than computers. The typical example is that of the automobile, which in many cases has

[5] Mark Roberti, *Getting Started RFID Business Applications*, RFID JOURNAL, http://www.rfidjournal.com/article/articleview/1334/1/129/ (last visited Mar. 24, 2006).

[6] Mark Roberti, *Getting Started RFID Consumer Applications and Benefits*, RFID JOURNAL, http://www.rfidjournal.com/article/articleview/1332/1/129/ (last visited Mar. 24, 2006).

[7] Currently, passive tags are estimated to cost between 20¢ and 40¢ a piece, and active tags between $20 and $50. *See Getting Started RFID System Components and Costs*, RFID JOURNAL, http://www.rfidjournal.com/article/articleview/1336/1/129/ (last visited Mar. 24, 2006).

[8] *See, e.g.*, Gal Eschet, *Fips And Pets For Rfid: Protecting Privacy In The Web Of Radio Frequency Identification*,45 JURIMETRICS J. 301 (2005); 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 (2005); Jerry Kang & Dana Cuff, *Pervasive Computing: Embedding The Public Sphere*, 62 WASH. & LEE L. REV. 93 (2005).

dozens of onboard computers.[9] Another example would be a refrigerator with a built-in bar code scanner, which allows you to generate a digital shopping list by scanning containers as you are about to finish the item. The refrigerator would then send the list to your grocery store, which would have your groceries ready for you to pick up.[10]

The computers in cars not only monitor the operations of the car, but can also track information about the use of the car. For example, the Lotus Elise sports car has a component, referred to as the "engine control unit," which can track over time various engine statistics, such as revolutions per minute.[11] While clearly this helps the dealer maintain the car, it may also be used to see if the engine has been misused.[12] One owner of a Lotus Elise sports car had the dealer download the data for him summarizing the first 1,000 miles of use of the car.[13] He noted that the data contained information about the car's operation that was inconsistent with how he had driven the car.[14]

At the same time, computer chips are getting smaller.[15] This drive to reduce size is in part due to manufacturers' desires to meet

[9] Abby J. Hardwick, *Amending The Uniform Commercial Code: How Will A Change In Scope Alter The Concept Of Goods?*, 82 WASH. U. L.Q. 275, 288 (2004). *See also* U.C.C. § 2-103 cmt. 7 (2005) ("For example, the sale of 'smart goods' such as an automobile is a transaction in goods fully within this article even though the automobile contains many computer programs"); Jean Braucher, *When Your Refrigerator Orders Groceries Online and your Car Dials 911 After an Accident: Do We Really Need New Law for the World of Smart Goods?*, 8 WASH. U. J.L. & POL'Y. 241 (2002).

[10] Leander Kahney, *The Coolest Internet Appliance*, WIRED, Feb. 12, 1999, http://www.wired.com/news/technology/0,17894-0.html.

[11] Robert Collingridge, *Lotus Elise S2 Engine Control Unit*, http://www.elises.co.uk/components/s2/engine/ecu/index.html (last visited Mar. 24, 2006):

> The engine management system has been specified to include memory which Lotus intend to use for a future upgrade that will provide a data-logging facility for use on the track. At present this memory is used to gather data needed to onward develop the OBD system. There is also a 'snap-shot' logging facility which records the sensor outputs at the moment a fault is triggered to aid diagnosis by a dealer.

[12] *Id.* ("There is no 'black-box' system for accident investigation but, the data captured can be used by Lotus to check on how the car has been used during it's life. *This information could be used to decide whether a warranty claim is justified or not.*" (emphasis added)).

[13] Lotus Elise: Engine Control Unit Information (last updated Oct. 2004), http://www.sandsmuseum.com/cars/elise/information/misc/ecudump.html.

[14] *Id.* ("The Max Engine Speed shows three recordings of greater than 8000 rpm. I know I did not do that, and the car only had 8 miles on it when I picked it up. So I am not sure when the engine encountered these high revs.").

[15] Chris Nuttall, *IBM set to unveil its skinniest microchip*, FIN. TIMES, Feb. 20, 2006, *available at* 2006 WLNR 2982886 ("IBM says its researchers have made a breakthrough in reducing the width of circuits on silicon chips to less than 30 billionths of a metre.").

consumer demand for smart goods.[16] This is also true in the field of radio frequency identification. Hitachi has developed an RFID tag that is so small it can be woven into currency.[17] Impinj, Inc. markets a chip, called the Zuma, which is the size of a grain of sand, has 41,798 transistors, and is comparable to the original Intel 8086 microprocessor.[18] Impinj describes the chip as a "[e]ssentially a microprocessor with an RF interface and nonvolatile memory."[19]

The final ingredient—leading to the raising of legal concerns—is the development of item level tracking. The technology behind this capability will be discussed in greater detail in the section that follows. However, one important aspect of RFID technology is the ability of an RFID tag to store more than just an identification code.[20] Thus, with the development of smart goods, the miniaturization of microprocessors, and the ability to track and store information about the goods to which the tag is attached, we are faced with the potential for a ubiquitous, but hidden, technology that will be able to track and store data about where we go and what we do.

A number of commentators have written about the tracking of personal data, and the control of access to the use of that data, from a privacy perspective.[21] This article considers whether the data itself is owned or can be legally controlled by the manufacturer and the consumer.

A. Embedded Tracking Technology

Radio frequency identification is a form of automatic identification system, or Auto-ID. A leading journal describes Auto-ID as "[a] broad term that covers methods of collecting data and entering it directly into computer systems without human

[16] Mike Fister, *Consumers Drive R&D Focus To Low Power, Smaller Goods*, ELECTRONICS WEEKLY, Mar. 1, 2006, *available at* 2006 WLNR 3439326 ("Consumers want products that do a million different things and do them well, all in a tiny package with a battery that never needs to be charged, and they will not wait for it.").

[17] CRM News, *Hitachi Develops Smallest IC Chip*, Feb. 6, 2006, *available at* http://www.crmbuyer.com/story/48693.html ("If an antenna is attached, the chip will still be thinner than copy machine paper, and the information can be obtained without being touched.").

[18] Rob Glidden, RFID: The Next Big Little Thing, slide 16 (Oct. 7, 2004) *available at* www.fcc.gov/realaudio/presentations/2004/100704/RobGlidden.pdf.

[19] *Id.*

[20] *See, e.g.*, ThingMagic, *GENERATION 2, A USER GUIDE*, *at* 12-13, (April, 2005), *available at* www.thingmagic.com/html/Generation2%20-%20A%20User%20Guide.pdf ("Class 2 tags add additional memory that can be changed frequently, for storing additional data – for example from an onboard sensor.").

[21] *See* notes 41-43 *infra* and accompanying text.

involvement."[22] One example of Auto-ID that consumers are well aware of is the bar code.[23] Bar codes usually appear on the packaging for a product. Manufacturers and retailers use the bar code to help track the item in the supply chain, and to scan the product at checkout. Bar codes often require a person to scan the item, and generally do not contain individualized tracking information about the particular item.

Manufacturers and retailers have been looking for a system to provide automatic, real time, individualized tracking to better control inventory distribution. Radio frequency identification is the technology that is being developed to provide such a system.

1. RFID

RFID tags are part of a system for remotely storing and retrieving data—in particular, identification information.[24] The RFID system contains two major components: the RFID tag, the device that stores and transmits the data, and the tag reader, the device that reads the data off the RFID tag by way of radio transmission.[25] The RFID tag (tag) is the component that is attached to an item, allowing the item to be tracked. The tag reader (reader) is the hardware that turns on the tag, telling it to transmit data, which the reader then relays to whomever is requesting it.[26]

The critical difference between bar codes, which provide information about the contents of the package using the universal product code (UPC), and RFID tags, is the electronic product code (EPC).[27] The UPC includes information about the manufacturer and the product type, but is not used to track individual items. By comparison, the EPC additionally includes the individual serial number of the item itself, facilitating the tracking of an individual item that contains a tag.[28] Currently, an organization called

[22] RFID Journal, RFID Journal Glossary, *available at* http://www.rfidjournal.com/glossary/automatic%20identification (last visited Mar. 15, 2006).

[23] *Id.* ("Technologies normally considered part of auto-ID include bar codes, biometrics, RFID and voice recognition.").

[24] Reuven R. Levary, et al., *Radio Frequency Identification: Legal Aspects*, 12 RICH. J.L. & TECH. 6, ¶ 1 (2005), *at* http://law.richmond.edu/jolt/v12i2/article6.pdf.

[25] KATHERINE ALBRECHT & LIZ MCINTYRE, SPYCHIPS, 13-14 (Nelson Current 2005) (hereinafter SPYCHIPS).

[26] *Id.*

[27] Katherine Albrecht, *Supermarket Cards: The Tip of the Retail Surveillance Iceberg*, 79 Denv. U. L. Rev. 534, 561-62 (2002). *See generally*, SPYCHIPS, *supra* note 25.

[28] EPCglobal: What is the Electronic Product Code, http://www.epcglobalinc.org/about/faqs.html#7 (last visited Mar. 24, 2006).

EPCglobal, Inc., a non-profit joint venture of GS1 (formerly known as EAN International) and GS1 US (formerly the Uniform Code Council, Inc.), is establishing the EPCglobal Network, a system that allows for the global real-time, automatic identification of information in the supply chain of any company, anywhere in the world.[29] EPCglobal has designed its tag numbering system to include 96 bits of data, which allows for 80 thousand trillion trillion individual items to be tracked,[30] easily covering all manufactured items for years to come.[31]

> What is the Electronic Product Code (EPC)?
>
> The Electronic Product Code™ (EPC) is the next generation of product identification. The EPC is a simple, compact "license plate" that uniquely identifies objects (items, cases, pallets, locations, etc.) in the supply chain. The EPC is built around a basic hierarchical idea that can be used to express a wide variety of different, existing numbering systems, like the EAN.UCC System Keys, UID, VIN, and other numbering systems.
>
> Like many current numbering schemes used in commerce, the EPC is divided into numbers that identify the manufacturer and product type. But, the EPC uses an extra set of digits, a serial number, to identify unique items. The EPC is the key to the information about the product it identifies that exists in the EPCglobal Network. An EPC number contains:
>
> 1. Header, which identifies the length, type, structure, version and generation of EPC
> 2. Manager Number, which identifies the company or company entity
> 3. Object Class, similar to a stock keeping unit or SKU
> 4. Serial Number, which is the specific instance of the Object Class being tagged
>
> Additional fields may also be used as part of the EPC in order to properly encode and decode information from different numbering systems into their native (human-readable) forms.

[29] About EPCglobal Inc, http://www.epcglobalinc.org/about/about.html (last visited Mar. 24, 2006).

[30] DAVID L. BROCK, THE COMPACT ELECTRONIC PRODUCT CODE, A 64-BIT REPRESENTATION OF THE ELECTRONIC PRODUCT CODE 4 (MIT Auto-ID Center Nov. 1, 2001), *available at* http://www2.hkana.org/files/epcGlobal/paper/MIT-AUTOID-WH-008.pdf; *see also*, RFID Journal, The Electronic Product Code, http://www.rfidjournal.com/faq/23 (last visited Mar. 24, 2006) ("The 96-bit EPC provides unique identifiers for 268 million companies. Each manufacturer can have 16 million object classes and 68 billion serial numbers in each class, more than enough to cover all products manufactured worldwide for years to come.").

> The Electronic Product Code (EPC) was conceived as a means to identify all physical objects. The primary purpose of the EPC was to serve as a reference to networked information. Used in conjunction with the Object Name Service, the EPC associates the physical object with information about the object – written in the Physical Markup Language (PML). Together these components allow physical objects to be networked together – creating essentially an 'Internet of Things'.
>
> Since the EPC identifies 'all physical objects,' it must be sufficiently large to enumerate at least those objects of interest for purposes of tracking and identification. The 96-bit version of the EPC code allows approximately $8x10^{28}$,

Tags come in two basic types: passive and active. A passive tag has no power source, and is generally only programmed with very limited information, usually its individual identification code. It is often described as a write once/read many device, meaning that once it has been programmed, the contents cannot be changed. It is activated by magnetic induction and so derives the power needed to broadcast a signal from coming close to a reader. Because a passive tag does not have a power source, it cannot collect information about its use; rather, tracking is left to the information received by the reader. The range of a passive tag is quite limited.[32]

By comparison, an active tag has a power source, which allows it both to transmit data further, and to process and store data internally. Because of this, an active tag may be programmed to do more than just report its unique identification code. In fact, an active tag's capability is limited only by its location.[33] If the tag is built into an automobile, it could have a very complex operating system and large storage capacity, running off of the car's battery. An active tag attached to an article of clothing would generally have to be small so as to be unobtrusive, and require a very sophisticated battery that is both flexible and small.[34]

Whether passive or active, a tag is activated to transmit information when it passes within range of a tag reader. Because the broadcasting power of a tag is limited, given its size and the size of the antenna, most readers only activate tags that come within 30 feet, at most. The EZPass toll collection device is an example of a tag consisting of a transponder that is activated when its possessor passes through a tollbooth.

The RFID tag is divided into 3 primary parts: hardware, software and data. The hardware in turn consists of two main components: the chip and the antenna. For purposes of this article, the chip is the most important hardware component, and although it may be comprised of different components (in the same way as a computer is comprised of a processor, random access memory, and hard drive storage), such

> or 80 thousand trillion trillion objects – more than sufficient for man-made physical products.

Id. (citations omitted).

[31] RFID Journal, The Electronic Product Code, *supra* note 30.

[32] Levary, *supra* note 24, at ¶ 2.

[33] *Id.* at ¶ 4.

[34] NEC has developed just such a battery. *NEC Develops Thin, Flexible Battery*, PC WORLD, Dec. 9, 2005, *available at* http://www.pcworld.com/resource/printable/article/0,aid,123875,00.asp.

distinctions are not generally germane to the issue of ownership of the data on the chip. This article will therefore refer to all of the hardware associated with an RFID tag (other than the antenna) as the chip, much as people discuss a computer as a single item.

EPCglobal has currently established six classes of tags: [35]

EPC Tag Class	Tag Class Capabilities
Class 0	Read only (*i.e., the EPC number is encoded onto the tag during manufacture and can be read by a reader*).
Class 1	Read, write once (*i.e., tags are manufactured without the EPC number, which can be encoded onto the tag later in the field*).
Class 2	Read, write.
Class 3	Class 2 capabilities plus a power source to provide increased range and/or advanced functionality.
Class 4	Class 3 capabilities plus active communication and the ability to communicate with other active tags.
Class 5	Class 4 capabilities plus the ability to communicate with passive tags, as well.

The current generation of tags being used by companies is the Class 1 tag.[36] These tags are passive, and are only capable of being

[35] HARDWARE CERTIFICATION PROGRAM, APPENDIX B (EPCglobal, Inc. Aug. 27, 2004), *available at* http://www.epcglobalus.org/SubscriberResources/br>Ceritification%20Paper%20Final%208.27.04.pdf.

[36] The capability of these tags is summarized by EPCglobal as follows:

Class-1: Identity Tags (normative)

Passive-backscatter Tags with the following minimum features:

- An electronic product code (EPC) identifier,
- A Tag identifier (TID),
- A 'kill' function that permanently disables the Tag,
- Optional password-protected access control, and

written to once, which means that they have limited data storage capabilities.

While such technology is not generally available today, companies are developing an active tag that operates software and stores data.[37] As the size of chips shrinks, and processing and data storage capabilities rise, the ability to deploy sophisticated tags will naturally attract some businesses. Even now, however, it is possible to install quite sophisticated tags on automobiles, or many large household appliances, such as refrigerators. Where size and power source are not an issue, the technology currently exists to track the movements and operations of the items to which the tags are attached. For example, the Department of Transportation is actively pursuing the Vehicle Infrastructure Integration (VII) initiative, which will put transmitters on all cars to help avoid accidents.[38] The VII is being designed to include the ability to store and transmit traffic information: "Vehicles could serve as data collectors and anonymously transmit traffic and road condition information from every major road within the transportation network."[39]

The data contained on the tag includes the EPC and any additional information programmed into the tag by the merchant, or—if it is a Class 2 tag or better—by the system installed on the chip.

The EPC is the critical part of this system, allowing for the tracking of individual items. EPCglobal has developed a standard for the EPC based on the work done by the Auto-ID labs at the Massachusetts Institute of Technology. The standard establishes a 96-bit identification code, divided up into 4 primary parts: the Header, EPC Manager Number, Object Class, and Serial Number. The Header sets out what version of EPC is being used; the EPC Manager Number is the unique identifier for the merchant responsible for the tag; and the Object Class identifies the particular class of item being identified. Up to this point, the EPC is similar to the UPC, in that it only identifies the class of goods sold by a particular merchant. However, by adding the Serial Number to the EPC, the EPC is now

• Optional user memory.

[37] *Developer Offers Linux-based RFID*, COMPUTERWORLD, Dec. 2, 2004, *available at* http://www.computerworld.com.au/pp.php?id=388926509 (tag can store up to 100 bytes of data, but company working on increasing storage capacity).

[38] Vehicle Infrastructure Integration (VII), U.S. Dept. of Transportation, http://www.its.dot.gov/vii/ (last visited Mar. 24, 2006).

[39] Overview – ITS, U.S. Dept. of Transportation, http://www.its.dot.gov/vii/vii_overview.htm (last visited Mar. 24, 2006). The DOT does state that the transmission is intended to be anonymous.

able to individually link the tag to the particular item to which it is attached. As noted, the EPC is 96 bits long, designed to be able to track every item ever produced by humankind.

The protocol established by EPCglobal for RFID tags in their classification system also allows the tag to store and transmit additional data. While the EPC is limited to 96 bits, the standard established by EPCglobal allows for the user (i.e., the merchant of the goods to which the tag is attached) to build additional memory into the chip for storage of extra data beyond the EPC.

In order for such data tracking and storage to work, the chip would have to do more than merely store the item's serial number. Obviously, some form of computer code would also have to reside on the chip, as well sufficient memory to store the data. To the extent that the tag includes operating code in the form of software, it is assumed that this code is copyrightable and owned by the manufacturer. While this is likely, it is also possible that this code, or at least part of it, is licensed to the manufacturer. This distinction does not matter to the purchaser of the item, since no sale of the underlying code would likely occur under copyright law with the sale of the item. It is also possible that the code contains non-copyrightable elements, or is subject to unique licensing agreements, such as the GPL.[40] For simplicity, it is nevertheless assumed that the manufacturer owns the copyright to the code. This software is assumed to include whatever code is necessary to operate the tag, to track information about the use of the tag, and to handle other tracking or data collecting activities.

II. DIRECT OWNERSHIP OF DATA

A. Laws Governing Collected Information

In general, U.S. law provides limited protection for information as such, particularly for personal information.[41] A number of scholars

[40] The GNU General Public License allows users to freely distribute copies of software licensed under its terms. GNU GENERAL PUBLIC LICENSE (Free Software Foundation, June 1991), http://www.gnu.org/licenses/gpl.txt ("The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software—to make sure the software is free for all its users.").

[41] *See, e.g.*, Sonia K. Katyal, *Privacy vs. Piracy*, 7 YALE J. L. & TECH. 222, 257-58 n.136-43 (2004), Vera Bergelson, *It's Personal But Is It Mine? Toward Property Rights in Personal Information*, 37 U.C. DAVIS L. REV. 379, 403-04 (2003); *See generally*, Daniel J. Solove & Marc Rotenberg, INFORMATION PRIVACY LAW (Aspen 2003); Paul M. Schwartz & Joel R. Reidenberg, DATA PRIVACY LAW (Michie 1996).

have argued that imposing a property regime in personal data would solve many of the privacy concerns raised by commercial use of data.[42] However, many other scholars disagree.[43]

Nevertheless, under certain specific conditions, information may be owned, or at least access to it controlled. This section explores the extent to which the data itself is subject to protection under U.S. law.

1. Copyright

The Copyright Act only protects original works of authorship that are fixed in a tangible medium of expression—specifically, the original expression created by an author.[44] Thus, in order for copyright to attach to any information, it must embody a work of authorship.[45]

It is clear that writing information in an electronic form is a fixation covered by copyright law.[46] So long as the information can be read through some means, it is fixed.[47] Therefore, it is at least possible that the data stored on a tag could comprise a work under the Copyright Act.

The Copyright Act by its terms does not protect ideas, concepts, or discoveries, among other things.[48] In addition, the Supreme Court

[42] *See, e.g.*, Paul M. Schwartz, *Property, Privacy, And Personal Data*, 117 HARV. L. REV. 2055, 2095 (2004) ("[P]ropertized personal information can be shaped to respond to privacy market failure and the need for a privacy commons."); *Developments in the Law—The Law of Cyberspace*, 112 HARV. L. REV. 1574, 1634-49 (1999).

[43] *See, e.g.*, Bergelson, *supra* note 41, at 383; Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1143 (2000); Mark A. Lemley, *Private Property: A Comment on Professor Samuelson's Contribution*, 52 STAN. L. REV. 1545, 1551 (2000); Anita L. Allen, *Coercing Privacy*, 40 WM. & MARY L. REV. 723, 750-57 (1999).

[44] 17 U.S.C. § 102(a) (2000); Feist Publ'ns., Inc. v. Rural Tel. Serv. Co., 499 U.S. 340 (1991).

[45] *Feist*, 499 U.S. at 345 ("To qualify for copyright protection, a work must be original to the author."); *see also* Jane C. Ginsburg, *Creation And Commercial Value: Copyright Protection Of Works Of Information*, 90 COLUM. L. REV. 1865, 1873-83 (1990) (historical development of the concept of "authorship" under copyright law).

[46] *See, e.g.*, Apple Computer, Inc. v. Franklin Computer Corp., 714 F.2d 1240, 1249 (3d Cir. 1983) ("We held that the statutory requirement of "fixation", the manner in which the issue arises, is satisfied through the embodiment of the expression in the ROM devices.").

[47] 17 U.S.C. § 101 (2000) ("A work is 'fixed' in a tangible medium of expression when its embodiment in a copy . . . is sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration."); *see also* MAI Sys. Corp. v. Peak Computer, Inc., 991 F.2d 511, 518 (9th Cir. 1993) (copying a computer program into a computer's random access memory is a fixation under the Copyright Act).

[48] 17 U.S.C. § 102(b) (2000) ("In no case does copyright protection for an original work of authorship extend to any idea, procedure, process, system, method of operation, concept,

has held that the Copyright Act does not protect either individual facts,[49] or informational works which present information in a fashion that is typical, commonplace or inevitable (such as the alphabetical white pages telephone directory at issue in the *Feist* case).[50] However, a compilation of data can be protected under the Copyright Act so long as "the resulting work as a whole constitutes an original work of authorship" due to the method of selecting, arranging, or coordinating the data.[51] Thus, in order for the data to be protected, the data must comprise a factual work protected as a compilation under copyright law.[52]

2. Copyright in Unique Identifier

The active tag that can track and store data contains two basic forms of information: first, the EPC, the individualized electronic product code; and second, the tracked data.

The first issue would be whether the manufacturer has rights in the tag's identification number by itself. The first question is whether the manufacturer is the "creator" of the number–in other words, how is it that the EPC is assigned? That number is created in compliance with the standards set forth by EPCglobal.[53] As described above, the EPC is created using four pieces of information. The first two, the Header and the Manager Number, are set according to the dictates of

principle, or discovery, regardless of the form in which it is described, explained, illustrated, or embodied in such work.").

[49] *Feist,* 499 U.S. at 344-48 ("'No one may claim originality as to facts.' This is because facts do not owe their origin to an act of authorship." (citations omitted)). The Supreme Court determined that the exclusion of facts from copyright protection is constitutionally required by the text of Article 1, section 8, clause 8 of the Constitution, which limits Congress's authority to grant exclusive rights to authors to their writings. *Id.* at 346. Please *see infra* notes 74-80 and accompanying text for a full discussion of the holding in *Feist.*

[50] *Id.* at 362 ("In preparing its white pages, Rural simply takes the data provided by its subscribers and lists it alphabetically by surname. The end product is a garden-variety white pages directory, devoid of even the slightest trace of creativity.").

[51] 17 U.S.C. § 101 (2000) (definition of "compilation"); *Feist,* 499 U.S. at 350-51 ("A factual compilation is eligible for copyright if it features an original selection or arrangement of facts, but the copyright is limited to the particular selection or arrangement. In no event may copyright extend to the facts themselves.").

[52] *See generally* Jane C. Ginsburg, *No "Sweat"? Copyright And Other Protection of Works of Information After Feist v. Rural Telephone,* 92 COLUM. L. REV. 338 (1992).

[53] EPCTM Tag Data Standards Version 1.1 Rev.1.24, at 11 (Apr. 1, 2004). In fact, it is EPCglobal that assigns a manager code. *Id.* ("EPCglobal assigns the General Manager Number to an entity, and ensures that each General Manager Number is unique.").

EPCglobal.[54] Thus, the manufacturer could make no claim to that information.

The third and fourth parts, the Object Class and Serial Number, are assigned by the manufacturer.[55] This part of the EPC could be subject to a claim of copyright protection as an "original work of authorship" by the manufacturer. The manufacturer would claim that because the Object Class and Serial Number portions of the EPC linked to a particular tag are unique and original, these portions of the EPC form a work of authorship protected under U.S. copyright law.

However, recent case law suggests that a manufacturer would not be able to claim any copyright ownership of the portion of the EPC assigned by the manufacturer.

In *Southco, Inc. v. Kanebridge Corp.*,[56] Southco, a manufacturer of rivets, fasteners, captive fasteners and other products, sued Kanebridge for copyright infringement based on Kanebridge's use of Southco part numbers in advertising.[57] Specifically, Kanebridge included Southco part numbers in comparison charts in its advertising and customer literature.[58] Southco claimed that its part numbers were copyrightable, because the part numbers created by Southco were unique and original, satisfying the low standard of originality under Copyright law.[59] The District Court agreed, because Southco did not assign random or arbitrary numbers, but rather used a system that evidenced "creativity and effort."[60]

The Third Circuit, in an en banc rehearing of a later appeal, held that no such copyright could exist in Southco's parts numbers.[61] The Third Circuit rejected Southco's arguments on two grounds. First, the court held that the numbers lacked sufficient originality to be

[54] IMPLEMENTATION NOTES: HOW TO OBTAIN YOUR EPC MANAGER NUMBER (EPCglobal, Inc. July 15, 2005), http://www.epcglobalus.org/SubscriberResources/IN_4_EPCManagerNumber_072205.pdf. *See also*, EPCTM Tag Data Standards Version 1.1 Rev.1.24, at 11 ("EPCglobal assigns the General Manager Number to an entity, and ensures that each General Manager Number is unique.").

[55] *See* IMPLEMENTATION NOTES, *supra* note 54, at 1.

[56] 390 F.3d 276 (3d Cir. 2004), *cert. denied*, 126 S. Ct. 336 (2005).

[57] *Id.* at 277-79.

[58] *Id.* at 279.

[59] Southco, Inc. v. Kanebridge Corp., No. CIV. A. 99-4337, 2000 WL 21257, at *4 (E.D. Pa.Jan. 12, 2000), *rev'd*, 258 F.3d 148 (3d Cir. 2001).

[60] *Id.*

[61] Southco Inc. v. Kanebridge Corp., 390 F.3d 276, 281 (3d Cir. 2004). An earlier panel had reversed the district court when it refused to issue an injunction because a different panel had held that the part numbers were not copyrightable. This later opinion was vacated by the later en banc decision of the Third Circuit. Southco Inc. v. Kanebridge Corp., 324 F.3d 190 (3d Cir. 2003) (appeal after remand), *vacated*, 390 F.3d 276 (3d Cir. 2004).

protected.[62] Relying on the Supreme Court's analysis in *Feist*,[63] the Third Circuit stated that the part numbers lacked originality because they were "rigidly dictated"[64] by the system developed by Southco for assigning part numbers.[65] Although the assignment of a part number was done by the part's designer,[66] the en banc panel held that in fact the numbering was dictated by the decisions made in the system developed by Southco. "Once these decisions were made, the system was in place, and all of the products in the class could be numbered without the slightest element of creativity."[67]

The Third Circuit also held that the part names were not copyrightable because they were similar to short phrases or titles of works.[68] The court based this analysis on the Copyright Office's practice of denying copyright registration for phrases and titles, a practice supported in a brief filed by the U.S. Government.[69] Although the court did not explore the question of whether this is an absolute requirement under the Copyright Act or the U.S. Constitution, many courts have deferred to the Copyright office's determination of copyrightability.[70]

Further, the U.S. Supreme Court has confirmed that individual facts themselves cannot be copyrighted: "That there can be no valid copyright in facts is universally understood."[71] Therefore, as a single piece of information, it is not likely that the individual serial number of the tag is copyrightable. Just because the manufacturer assigned that number to the item, it is a fact that the item has that number. In addition, there is no other way to refer to that individual tag without

[62] *Southco*, 390 F.3d at 281.

[63] *Feist*, 499 U.S. 340.

[64] 390 F.3d at 282.

[65] *Id.* at 281-85.

[66] 324 F.3d at 193-94

> These numbers were not dictated by any numbering system. Not only each number as a whole, but each group of digits and each digit in each number was created by me based upon the specific products which I had created and my determination of the values of those products to be represented and the digits to be used. The part number for each new part was created on the basis of my decisions.

Id. (quoting declaration of Robert H. Bisbing, designer of fasteners for Southco).

[67] 390 F.3d at 282.

[68] *Id.* at 285-87.

[69] *Id.* at 286. *See* 37 C.F.R. § 202.1(a) (2005) (Copyright Office's regulation prohibiting copyright registration for words and short phrases).

[70] MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT §7.26 (2005).

[71] *Feist*, 499 U.S. at 340, 344.

relying on its unique serial number. As a result, it is highly unlikely that the EPC can be owned by anyone under copyright law.

3. Copyright in Compiled Data

i. Mere Facts/Data – the Feist Problem

Depending on the capabilities of the tag, the data stored on the tag likely consists of more than a single piece of information. If the tag is an active tag with its own power source and non-volatile memory, it has the capability to store information in addition to the EPC. Such an active tag may track a series or stream of data written to the tag's memory over time, such as times, locations, accesses, or technical data about the item to which the tag is attached, such as oil pressure in a car. The resulting tracked information will consist of a database or compilation of the information tracked.

As discussed in the preceding section, it is clear that the individual facts contained on the chip will not be protected under copyright law. However, it may be that the data are protectable as a copyrightable compilation.[72] The Copyright Act specifically provides that a compilation "is a work formed by the collection and assembling of . . . data that are selected, coordinated, or arranged in such a way that the resulting work as a whole constitutes an original work of authorship."[73]

The Supreme Court has addressed when a compilation consisting of factual information is protected under this provision. In *Feist*, the Supreme Court had to decide whether the creation of a white pages telephone directory was protectable as a copyrighted work. Rural Telephone had compiled white pages phone books, listing alphabetically the names and phone numbers of residents of Northwest Kansas.[74] Feist, a competitor of Rural, copied entire sections of the phone book without permission,[75] creating its own directory.[76] Rural claimed that Feist had infringed its copyright in its

[72] *See generally* RAYMOND T. NIMMER, INFORMATION LAW § 3.6 (2005); Jane C. Ginsburg, *Copyright, Common Law, And Sui Generis Protection Of Databases In The United States And Abroad*, 66 U. CIN. L. REV. 151 (1997).

[73] 17 U.S.C. § 101 (2000).

[74] *Feist*, 499 U.S. at 348.

[75] Feist had tried to license the white pages from Rural, but Rural refused. *Id.* at 343.

[76] *Id.* By wholesale copying of Rural's directory, Feist inadvertently included four listings that were fictitious, inserted by Rural to detect copying.

telephone directory, which it claimed was a copyrightable compilation.[77]

The Court held that while the Copyright Act never protects facts, it is possible to obtain a copyright in a factual work, such as an original compilation of facts. So long as the compilation of facts is independently created by the author and contains some degree of creativity, then it is a copyrighted work.[78]

Nevertheless, the Court held that some original expression in the selection and arrangement of the information must exist for copyright to attach. As stated by the Court:

> The compilation author typically chooses which facts to include, in what order to place them, and how to arrange the collected data so that they may be used effectively by readers. These choices as to selection and arrangement, so long as they are made independently by the compiler and entail a minimal degree of creativity, are sufficiently original that Congress may protect such compilations through the copyright laws.[79]

Ultimately, the *Feist* Court held that the arrangement of the names of telephone subscribers in alphabetical order can never be protected by copyright, because the arrangement is obvious, even necessary.[80]

Thus, for the compilation of data stored on the tag to be copyrightable, the manufacturer would have to show that the database created based on the tracking reflects original selection, coordination or arrangement of the data by the author. The level of creativity needed is low, as explained by the Supreme Court in *Feist.* For example, mundane compilations, such as a listing of the best restaurants in a city, have been held to demonstrate enough creativity to be protected as original works of authorship.[81] Even a blank form used to display particular information from publicly available statistics about sporting events could be sufficiently creative to be protected, if the choice of statistics presented is original to the creator

[77] *Id.* at 347.

[78] *Id.* at 348.

[79] *Id.*

[80] *Id.* at 363 ("[T]here is nothing remotely creative about arranging names alphabetically in a white pages directory. It is an age-old practice, firmly rooted in tradition and so commonplace that it has come to be expected as a matter of course.").

[81] Adventures in Good Eating v. Best Places to Eat, 131 F.2d 809 (7th Cir. 1942).

of the form.[82] Thus, very little original expression is necessary to make a compilation copyrightable.[83]

Several courts have had to distinguish between copyrightable and uncopyrightable compilations based on the nature of the selection process of the facts comprising a compilation. The Seventh Circuit held in *Mid America Title Co. v. Kirk* that the selection of data presented in a title insurance commitment was not original.[84] In the *Kirk* case, the court found that the decision to include facts in the title commitment was not based upon the individual judgment of the title examiner, but "instead it was a matter of convention and strict industry standards."[85] Because the selection process was "too rote and mechanical," the compilation was not copyrightable.[86]

By comparison, the process of selection of what businesses to include in a yellow pages directory compiled for the Chinese-American community in New York was copyrightable.[87] As stated by the Second Circuit, "[s]election implies the exercise of judgment in choosing which facts from a given body of data to include in a compilation."[88] Because the authors of the directory had to choose among many possible businesses to include in a yellow pages directory compiled for a particular audience, the author of the directory had created an original compilation of otherwise uncopyrightable facts.[89]

Thus, in order for the data on the tag to be a protected compilation, the data would have to be selected in an original fashion. If the tag is tracking all relevant information about a certain sensor data, such as the oil pressure in an engine at set intervals, this likely does not reflect any original selection of the data. Where the

[82] Kregos v. Associated Press, 937 F.2d 700, 704-05 (2d Cir. 1991); *see also* Bucklew v. Hawkins, Ash, Baptie & Co., 329 F.3d 923 (7th Cir. 2003).

[83] *See, e.g.*, CCC Info. Serv., Inc. v. Maclean Hunter Mkt. Reports, 44 F.3d 61 (2d Cir. 1994) (Red Book valuations of used cars copyrightable); CDN, Inc. v. Kapes, 197 F.3d 1256 (9th Cir. 1999) (numerical price estimates of coins was copyrightable).

[84] Mid America Title Co. v. Kirk, 59 F.3d 719, 723 (7th Cir. 1995).

[85] *Id.* at 722.

[86] *Id. See also* Financial Info., Inc. v. Moody's Investors Serv., Inc., 808 F.2d 204, 206-08 (2nd Cir. 1986) (recording five basic facts about municipal bond redemptions on to index cards evidenced no original selection and arrangement).

[87] Key Publ'ns. v. Chinatown Today Publ'ng. Ent., 945 F.2d 509, 513-14 (2nd Cir. 1991).

[88] *Id.* at 513.

[89] *Id.*

compilation seeks to be comprehensive,[90] or uses a standard set of selection criteria, then the compilation is not copyrightable.[91] In a similar fashion, the Second Circuit denied copyright protection for West Publishing's pagination system.[92] Noting that the page breaks were inserted into court opinions by a computer program, the court held that resulting page numbers were not protected by copyright law because "the internal pagination of West's case reporters does not entail even a modicum of creativity."[93] Thus, if the tag is tracking everywhere the item has been, or all statistical information about the item's use or operation, then likely the compilation will not be held to be copyrightable.

Perhaps an argument can be made that the selection of what data to track specified in the tag's programming requires some creativity by the author.[94] For example, in *Compaq Computer Corp. v. Procom Technology, Inc.* a competing hard drive vendor was held liable when it sold hard drives that included data on the hard drive's firmware copied from Compaq Computer's hardware.[95] Compaq had designed a program called the Compaq Insight Manager (CIM) that determined when failure of a hard drive was imminent based upon a limited set of threshold values from a large number of possible parameters.[96] Procom, the competitor, copied those values onto its hard drives in order to make them compatible with the CIM used in Compaq's ProLiant line of servers.[97] The court ruled that Compaq had exercised discretion in choosing the number of parameters and which particular parameters to monitor. In addition, because the thresholds picked were based upon both estimates of when the drives would fail and the cost of replacing those drives under warranty, those threshold values were not facts.[98]

[90] Warren Publ'ng., Inc. v. Microdos Data Corp., 115 F.3d 1509, 1518 (11th Cir. 1997) (factbook containing lists of cable systems not copyrightable because it included entire relevant universe of such cable companies).

[91] *See Financial Info.*, 808 F.2d at 206-08 (recording five basic facts about municipal bond redemptions on index cards evidenced no original selection and arrangement); NIMMER, *supra* note 70, § 3.7.

[92] Matthew Bender & Co., Inc. v. West Publ'ng. Co., 158 F.3d 693, 699-700 (2d Cir. 1998).

[93] *Id.* at 699.

[94] *See infra* notes 109-130 for a discussion of who the author of the database is.

[95] Compaq Computer Corp. v. Procom Tech., Inc., 908 F. Supp. 1409 (S.D. Tex. 1995).

[96] *Id.* at 1414-15.

[97] *Id.* at 1415-17.

[98] *Id.* at 1417-18.

In a recent case, the Seventh Circuit Court of Appeals considered whether the extraction of data compiled by a copyrighted program imposing a unique system for arranging otherwise uncopyrightable data constituted infringement. Assessment Technologies (AT) licensed a program called "Market Drive" to local municipalities to aid them in compiling data about property in the community for assessing property taxes.[99] The data were entered into the program by tax assessors, and the program allocated the data into 456 fields and 34 master categories.[100] WIREdata asked several municipalities for the data contained in the databases, and AT sued to prevent WIREdata from obtaining the information, claiming that AT owned the copyright in the resulting databases created by the Market Drive program.[101] The Seventh Circuit ruled first that AT did have a valid copyright in its program, because "no other real estate assessment program arranges the data collected by the assessor in these 456 fields grouped into these 34 categories, and because this structure is not so obvious or inevitable as to lack the minimal originality required. . . ."[102] If WIREdata had copied the data in the structure setup in Market Drive, WIREdata would have infringed AT's copyright.[103]

However, WIREdata only wanted access to the underlying raw data contained in the databases, not the data as formatted by the Market Drive program. The issue then was whether the data could be extracted from the database without violating the Market Drive program.[104] The court held that because WIREdata sought only the raw data, and the data was in the public domain, copying that data was legal so long as they did not use the Market Drive system to copy the data.[105] The court noted that AT did not create the databases that it was seeking to protect—the tax assessors were the ones to actually enter the data. Instead, all that AT had created was the empty bin that the data went into:

> It created the compartments in the bin and the instructions for sorting the data to those compartments, but those were its only innovations and their protection by copyright law is complete. To try by contract or otherwise to prevent the municipalities from

[99] Assessment Techs. of Wis., LLC v. Wiredata, Inc., 350 F.3d 640, 642 (7th Cir. 2003).

[100] *Id.* at 642-43.

[101] *Id.* at 642.

[102] *Id.* at 643.

[103] *Id.* (citing *Key Publ'ns.*, 945 F.2d at 513-14).

[104] *Id.* at 643-44.

[105] *Id.*

> revealing their own data, especially when, as we have seen, the complete data are unavailable anywhere else, might constitute copyright misuse.[106]

In fact, the Seventh Circuit held that it would not infringe AT's copyright when the municipalities use the Market Drive program to extract the data, save it in a separate file and then give that file to WIREdata.[107]

In much the same way, the manufacturers of the tag create empty bins into which the tracked data is sorted and stored. While the program for doing so may be copyrightable (it is assumed to be so for this article), the resulting data is not selected by the manufacturer. Thus, where the selection is done according to a pre-programmed system, the resulting compilation should not be protected by copyright.

In addition, the data contained in the tag is not compiled according to a fixed selection and arrangement. That is, the software on the chip merely tracks and stores data according to a set of criteria, identifying each particular datum as it is received according to those criteria. It is not until the data are later viewed that the selection and arrangement is really imposed. Thus it is the software used by the reader to organize the data that imposes the arrangement on the data. Therefore, a strong argument can be made that no arrangement of the data is made until it is viewed by the person wishing to analyze the data.[108] Of course, the selection of the data to be tracked is based upon the decision of the author of the software, and that software itself may reflect some creativity.

Even if the compilation were copyrighted, a single fact taken from that compilation is not subject to copyright protection, and

[106] *Id.* at 646-47.

[107] *Id.* at 644.

> To summarize, there are at least four possible methods by which WIRE data can obtain the data it is seeking without infringing AT's copyright; which one is selected is for the municipality to decide in light of applicable trade-secret, open-records, and contract laws. The methods are: (1) the municipalities use Market Drive to extract the data and place it in an electronic file; (2) they use Microsoft Access to create an electronic file of the data; (3) they allow programmers furnished by WIREdata to use their computers to extract the data from their database-this is really just an alternative to WIREdata's paying the municipalities' cost of extraction, which the open-records law requires; (4) they copy the database file and give it to WIREdata to extract the data from.

Id. at 647-48.

[108] Bellsouth Adver. & Publ'ng. Corp. v. Donnelly Info. Publ'ng., 999 F.2d 1436 (11th Cir. 1993).

another person may use it for his or her benefit. Thus, even if the data on the chip is copyrightable as a compilation, accessing the chip and obtaining a single piece of information is not likely to be deemed copyright infringement. So, for example, if an independent automobile dealer downloads the oil pressure of a car at a particular instant, this is not likely to be an infringement of the compilation of data regarding oil pressure over time.

ii. Authorship

Another concern with the data is that it is generated by the software contained on the chip without direct human input. Although there clearly is an author of the software, the resulting data compilation is generated automatically based upon pre-selected criteria, and not on the basis of creative judgment of a human author. Thus, a question arises as to whether there is any author of the data at all.

One possibility is that the data is "authored" by the programs contained on the chip. The Copyright Act does not specifically require that a work be authored by a human in order to receive copyright protection.[109] However, the Patent and Copyright Clause of the U.S. Constitution does mention "author,"[110] and the Supreme court has stated that "[a]s a general rule, the author is the party who actually creates the work, that is, the person who translates an idea into a fixed, tangible expression entitled to copyright protection."[111]

This is consistent with the Court's holdings in two separate cases decided over a century earlier. In the first case, the *Trade-Mark Cases*, the Court described a protectable writing as an original work of the mind.[112] Five years later, in holding that a photograph of Oscar

[109] 17 U.S.C. § 102(a) (2000) ("[C]opyright protection subsists . . . in original works of authorship fixed in any tangible medium of expression, . . . from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device."). *See also* Urantia Found. v. Maaherra, 114 F.3d 955, 958 (9th Cir.1997) (noting that even thought the Copyright Act does not specifically require human authorship, nevertheless the law was not intended to protect a work claimed to be authored by celestial beings).

[110] U.S. CONST. art. I, § 8, cl. 8. ("[The Congress shall have power] [t]o promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries.").

[111] Community for Creative Non-Violence v. Reid, 490 U.S. 730, 737 (1989).

[112] United States v. Steffens, 100 U.S. 82, 94 (1879) ("And while the word writings may be liberally construed, as it has been, to include original designs for engravings, prints, &c., it is only such as are original, and are founded in the creative powers of the mind. The writings which are to be protected are the fruits of intellectual labor, embodied in the form of books, prints, engravings and the like.").

Wilde was copyrightable, the Court stated that copyright is "the exclusive right of a man to the production of his own genius or intellect."[113] David Nimmer has noted that "rivers of ink" have been spilt in the secondary literature on whether a computer can be an author for purposes of copyright law.[114] While some commentators have argued that a computer could, theoretically, be an author, at least with respect to works created through use of artificial intelligence,[115] most reject the idea.[116] The same result was reached by the National Commission on New Technological Uses of Copyrighted Works when it issued its Final Report in 1979.[117]

In fact, the human involvement in creating the "compilation" in the tag ends with the authoring of the software. The data have not yet come into existence when the human element ends. At the time that the data are subject to tracking on the chip, no human has viewed the data, let alone made any creative decisions about whether to include

[113] Burrow-Giles Lithographic Co. v. Sarony, 111 U.S. 53, 58 (1884). *But see* Arthur R. Miller, *Copyright Protection For Computer Programs, Databases, And Computer-Generated Works: Is Anything New Since CONTU?*, 106 HARV. L. REV. 977, 1062 (1993) ("There are limits to literal reading. By making references to 'he' and 'man,' the Court was no more excluding machines from eligibility for authorship than it was excluding women. There simply is less than meets the eye in the language of the opinion.").

[114] NIMMER, *supra* note 70, § 5.01.

[115] *See, e.g.*, Karl F. Milde, Jr., *Can a Computer Be an "Author" or an "Inventor"?*, 51 J. PAT. OFF. SOC'Y 378 (1969).

[116] *See, e.g.*, William T. Ralston, *Copyright In Computer-Composed Music: Hal Meets Handel*, 52 J. COPYRIGHT SOC'Y U.S.A. 281, 302-03 (2005) (Rejecting the computer as author, and favoring the user as author); Ralph D. Clifford, *Intellectual Property In The Era Of The Creative Computer Program: Will The True Creator Please Stand Up?*, 71 TUL. L. REV. 1675, 1682-86 (1997) ("Author" is a term of art under the Copyright Act, meaning the actual individual that created the work); David Nimmer, *Brains And Other Paraphernalia Of The Digital Age*, 10 HARV. J.L. & TECH. 1 (1996); Miller, *supra* note 113, at 1056-73 ("[I]f the day arrives when a computer really is the sole author of an original artistic, musical, or literary work (whether a novel or a computer program), copyright law will be embracive and malleable enough to assimilate that development into the world of protected works."); Pamela Samuelson, *Allocating Ownership Rights In Computer-Generated Works*, 47 U. PITT. L. REV. 1185, 1192-1200 (1986) ("Only those stuck in the doctrinal mud could even think that computers could be 'authors.'").

[117] NATIONAL COMM'N ON NEW TECHNOLOGICAL USES OF COPYRIGHTED WORKS, FINAL REPORT, at 44 (1979) (hereinafter CONTU REPORT) ("On the basis of its investigations and society's experience with the computer, the Commission believes that there is no reasonable basis for considering that a computer in any way contributes authorship to a work produced through its use."). As stated in the report, "The National Commission on New Technological Uses of Copyrighted Works (CONTU) was created by Congress as part of the effort to revise comprehensively the copyright laws of the United States." *Id.* at 1. It's particular focus was on "changes in copyright law or procedure needed both to assure public access to copyrighted works used in conjunction with computer and machine duplication systems and to respect the rights of owners of copyrights in such works, while considering the concerns of the general public and the consumer." *Id.*

any of the data, or how to arrange them. Human interaction does not come into play again until the data compilation is accessed by a reader and acted upon by the person interpreting the data. One possible argument, then, is that there is no author at all, and the data is completely uncopyrightable.[118] However, most commentators do not believe that this is likely to be held to be the case.[119]

Another argument is that the author who created the code establishing the criteria for tracking the data is the author of the resulting compilation created using that criterion.[120] This would make the manufacturer the author of the resulting database contained on the tag. The problem with this argument is that while there is an author of the "structure" of the compilation, the compilation only comes into existence by imposing this structure on the data, without regard to the selection or arrangement of the particular data contained in the database. However, since the author of the code did not cause the data to be recorded (fixed, in the language of copyright), at best it can be argued that the manufacturer created the circumstances under which the data was recorded.[121]

[118] *See* Samuelson, *supra* note 116, at 1224-28 (noting that it is not necessary to grant a human being rights to encourage the creation of computer generated works).

[119] For example, Professor Samuelson concludes that the "no author" result is not likely to be adopted, although a "seemingly sensible proposal" because "it conflicts with the temper of the times." *Id.* at 1225. *Accord* Miller, *supra* note 113, at 1058-59 ("Although commentators have differed as to who should be considered the author of a computer-generated work, they seem to agree that it should be a human being or legal entity, even though identifying that author may not always be easy. . . .") (citing Samuelson, *supra* note 116, at 1224-28). One recent article argues that the 1997 Ninth Circuit opinion in Urantia Found. v. Maaherra 114 F.3d 955 (9th Cir. 1997), which held that a work written based on answers from celestial beings was authored by the persons that created the written work, would support this result. *Id.* at 959. *See* Christina Rhee, Note, *Urantia Foundation v. Maaherra*, 13 BERKELEY TECH. L.J. 69, 76 (1998) ("If courts strictly apply the Urantia decision to future copyright claims over computer-generated works, they will grant the copyright to a human, most likely the computer program user.").

[120] *See* Samuelson, *supra* note 116, at 1205-21 (concluding that the programmer is not the author of a computer-generated work, whether directly or as a derivative work).

[121] *Accord Burrow-Giles Lithographic Co.*, 111 U.S. at 60-61. The Court cited with approval an earlier English case, Nottage v. Jackson, 11 Q.B. Div. 627, which decided on the issue of authorship of a photograph. As described by the U.S. Supreme Court, "[t]he question in the case was whether the plaintiffs, who owned the establishment in London, where the photographs were made from the negative, and were sold, and who had the negative taken by one of their men, were the authors, or the man who, for their benefit, took the negative." The English court held that the person that "took the negative" was the author. *Id.*

> The nearest I can come to is that it is the person who effectively is as near as he can be the cause of the picture which is produced; that is, the person who has superintended the arrangement, who has actually formed the picture by putting the persons in position, and arranging the place where the people are to be-the man who is the effective cause of that.

So, for example, where the pagination in West's reporters was generated automatically by the software, the court held that no copyright existed because it did not entail even a modicum of originality.[122] Similarly, as the Court in *Assessment Technologies* held, the manufacturer had only created an empty database, a bin that could be filled with data.[123] By comparison, the creator of the Red Book of automobile values takes the raw data and uses creativity in choosing values from that data to represent the values of automobiles throughout the United States. There is a human author that acts upon the data to create a copyrightable database. The values are arrived at using skill and judgment, which means that the information consists of the original expression of the Redbook valuations.[124]

Even if there is a human author of the data, that author is at least in part the consumer that purchased the item and began using it.[125] It is the interaction of the software with the consumer's actions that generates the data, not the author of the software itself. Much like a person who uses Microsoft Word to create a literary work, it is the person *using* the software that is the author, not Microsoft.[126] This result is consistent with the CONTU Report.[127]

Burrow-Giles Lithographic Co., 111 U.S. at 61 (quoting Nottage v. Jackson).

[122] Matthew Bender & Co., v. West Publ'ng. Co., 158 F.3d 693 (2d Cir. 1998).

[123] *Assessment Techs.*, 350 F.3d at 646. *But see* Madison River Mgmt. Co. v. Bus. Mgmt. Software Corp., 387 F. Supp. 2d 521 (M.D.N.C. 2005) (holding that Madison River Management violated Business Management Software's (BMS) copyright in a database created by BMS's ProvideC software, where Madison River had copied the entire database). This case seems to misapply the rule set out in *Assessment Techs.*, which held that the Business Management Software Corp.'s "database is covered by [BMS's] copyright over its [] software." *Id.* at 534-35. The *Madison River* court states that the Seventh Circuit had determined that the *database* was held to be copyrightable, when in fact what the Seventh Circuit found was that the plaintiff's Market Drive *program* was copyrightable. *See Assessment Technologies*, 350 F.3d at 643. Nevertheless, the *Madison River* court based its holding on the fact that Madison River had copied the entire database, including its structure, not for the purposes of extracting the raw data as in *Assessment Technologies*, but to use that structure to run reports from the entire database. *Madison River*, 387 F. Supp. 2d at 537 (citing *Assessment Techs.*, 350 F.3d at 643).

[124] CCC Info. Serv. v. Maclean Hunter Mkt. Reports, 44 F.3d 61 (2d Cir. 1994).

[125] *See* CONTU Report, *supra* note 117, at 45. ("Finally, we confront the question of who is the author of a work produced through the use of a computer. The obvious answer is that the author is one who employs the computer").

[126] *See* Samuelson, *supra* note 115, at 1200 n.71.

[127] CONTU REPORT, *supra* note 117, at 45:

> To be used in the creation of a work, a computer must be controlled by a program and must ordinarily utilize data input from other sources. Both the program and the data may be copyrighted works or parts of copyrighted works. The question has been raised whether authorship or proprietorship of the program or data base establishes or may establish a claim of authorship of the final work. It appears to the Commission that authorship of the program or of the input data is entirely

In limited circumstances a work may be a work made for hire, which changes the nature of authorship. If a work is made for hire, then the author is not the person actually creating the work, but the company or individual that hired them to create the work.[128] All works created by employees in the scope of their employment are works for hire,[129] as are a certain group of limited types of specially ordered or commissioned works, such as movies and compilations, where the author has executed a written agreement acknowledging that the work is made for hire.[130]

Since the consumer is not likely to be an employee of the person creating the data compilation, this type of authorship under the work for hire doctrine would not apply. In addition, the consumer is also not likely to be an independent contractor hired to assist in the creation of the work. Even if the resulting database is held to be a work for hire compilation, an independent contractor must agree in a signed writing that the work is a work for hire. Unless the consumer purchased the item using some form of signed writing, such as a charge slip, and that charge slip specifically included work for hire language, the resulting data is not likely to be deemed a work for hire.

4. Database Protection

Given the holding in *Feist*, databases that consist of electronically generated compilations of facts are not likely to be protected under U.S. copyright law unless some original selection and arrangement is applied to the database.[131] Further, there exists no sui generis protection for databases under current U.S. law. Although attempts have been made to pass database protection legislation in the U.S., at the moment no such protection exists.[132]

separate from authorship of the final work, just as authorship of a translation of a book is distinct from authorship of the original work.

[128] 17 U.S.C. § 101 (2000); NIMMER, *supra* note 70, § 5.03.

[129] 17 U.S.C. § 101 (2000); *Community for Creative Non-Violence*, 490 U.S. at 739-41 (status as employee should be analyzed under the general common law of agency).

[130] 17 U.S.C. § 101 (2000). Specifically, such works include:

> a work specially ordered or commissioned for use as a contribution to a collective work, as a part of a motion picture or other audiovisual work, as a translation, as a supplementary work, as a compilation, as an instructional text, as a test, as answer material for a test, or as an atlas, if the parties expressly agree in a written instrument signed by them that the work shall be considered a work made for hire.

[131] Jane C. Ginsburg, *Copyright, Common Law, And Sui Generis Protection Of Databases In The United States And Abroad*, 66 U. CIN. L. REV. 151, 153 (1997).

[132] *Assessment Techs.*, 350 F.3d at 645; Ginsburg, *supra* note 131, at 171.

Although not directly relevant to the discussion of whether the data contained on a tag is protected under U.S. law, the European Commission's directive regarding ownership of databases, the EU Database Directive,[133] may be adopted in some form in the United States. This Directive prevents extraction or reutilization of data from a database, even if the data are not subject to copyright protection.[134] The EU has thus created a right against misappropriation of data under certain proscribed circumstances. In order to receive this protection, there must have been a substantial investment in the database, and the infringer must either copy all or substantially all of the database, or, if the infringer has only taken an insubstantial part, have done so on a regular basis.[135]

As a result, under the sui generis protection for databases conferred by the Database Directive, a different analysis from copyright law is required to find liability. The first consideration is whether the owner of the item is the creator of the database or the manufacturer and distributor of the chip. The Directive states that the sui generis rights apply to the "maker" of the database.[136] However, no definition of maker is included in the Directive.

If the owner of the item is the chip manufacturer and distributor rather than the database creator, there is an interesting question as to whether it has made a substantial investment in the database (as opposed to the chip and its software). Although clearly great effort may have gone into designing the chip and writing the software, the

[133] Directive on Legal Protection of Databases (Database Directive), 96/9/EC, O.J. 77 (Mar. 27, 1996). *See generally*, W. R. Comish, *European Community Directive On Database Protection*, 21 COLUM.-VLA J.L. & ARTS 1 (1996).

[134] Database Directive, *supra* note 133, at Chapter III, arts. 7-11 (Sui Generis Protection provisions). Specifically, the Directive states that

> Member States shall provide for a right for the maker of a database which shows that there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents to prevent extraction and/or re-utilization of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database.

Id. at art. 7(1).

Chapter II of the Database Directive also contains provisions regarding copyright protection for databases, which extends copyright protection to "databases which, by reason of the selection or arrangement of their contents, constitute the author's own intellectual creation shall be protected as such by copyright." *Id.* at art. 3(1). However, the copyright in such databases "shall not extend to their contents and shall be without prejudice to any rights subsisting in those contents themselves." *Id.* at art. 3(2).

[135] *Id.* at art. 7(1).

[136] *Id.* at art. 7(1). For copyright protection, the author is "the natural person or group of natural persons who created the base or, where the legislation of the Member States so permits, the legal person designated as the rightholder by that legislation." *Id.* art. 4(1).

manufacturer and distributor have not made any independent effort to create the database contained on the RFID tag. That effort clearly was made by the owner of the item.

If it is the owner of the item that creates the database, then presumably the rights to the database would accrue to the owner him or herself, if anyone at all. If the database is created merely by tracking the use of the item that the tag is attached to, it may be that this will be deemed to be insubstantial, at least to the extent that it is unintentional. Even if this effort is deemed substantial, the owner of the chip would nevertheless be the proper party to assert rights in the database, not the manufacturer. Unless the EU courts are willing to extend to the manufacturer the right to assert the interest of the item's owner, it is not likely that anyone capturing data from an RFID tag would be liable to a manufacturer under the Directive.

A separate question would be how much of the database is taken when the chip broadcasts its contents upon being turned on. If the chip "voluntarily" gives up its contents to the reader, presumably this would not be an unauthorized extraction. Even so, it might be an unauthorized reutilization. If only the latest data is used, such as the current oil pressure in a car, the test would be whether it was a repeated and systematic reutilization. It may be that the data taken from a particular item is only used once. If so, it is not likely that this would be seen as a systematic use of the data. However, perhaps where the reader is taking data from numerous separate databases, this could be seen to be systematic and repeated. Such an interpretation would likely be at odds with the language of the Directive, though, which speaks in terms of single databases, and not reutilization of limited data across numerous databases.[137]

5. Trade Secret

In the United States, trade secrets are protected under state law. Although there is no single method of protecting trade secrets, most states in the U.S. have adopted some version of the Uniform Trade Secrets Act (UTSA).[138] The Restatement (Third) of Unfair

[137] *Id.* art 7(2)(a)-(b) ("extraction" and "reutilization" are defined as transferring or making available to the public, respectively, "all or a substantial part of the contents of *a* database") (emphasis added).

[138] UNIF. TRADE SECRETS ACT § 1, 14 U.L.A. 433-67 (1990). Forty five states and the District of Columbia have passed some version of the UTSA. UNIF. TRADE SECRETS ACT § 1, 14 U.L.A. 433-67 Refs. and Annos. (1990). There are several federal laws that criminalize theft of trade secrets, as well. *See, e.g.*, 18 U.S.C. §§ 1341, 1343 (2000) (mail fraud); Economic Espionage Act, 18 U.S.C. § 1831 (2000); National Stolen Property Act, 18 U.S.C. § 2314

Competition also contains a definition of trade secrets.[139] Even though there is some variation in the language of various definitions for trade secrets,[140] they are nevertheless generally seen as consistent.[141] The Restatement (Third) of Unfair Competition sets forth the most succinct definition: "A trade secret is any information that can be used in the operation of a business or other enterprise and that is sufficiently valuable and secret to afford an actual or potential economic advantage over others."[142]

As this definition makes clear, virtually any information can be a trade secret, provided that it gives a competitive advantage to its

(2000). An older common law formulation from the first Restatement of Torts, section 757 of the original Restatement of Torts, RESTATEMENT OF TORTS § 757 (1939), is still commonly relied upon by courts. *See* MILGRIM, § 1.

[139] RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 (1995). The Restatement (Third) of Unfair Competition is intended to be the modern restatement of the common law protection of trade secret law. *Id.* § 39 reporters' note (also noting the applicability of the Restatement to UTSA cases).

[140] The Uniform Trade Secrets Act defines a trade secret as follows:

> "Trade secret" means information, including a formula, pattern, compilation, program, device, method, technique, or process, that:
>
> > (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and
> >
> > (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

UNIF. TRADE SECRETS ACT § 1, 14 U.L.A. 438 (1990).

The Restatement (Third) of Unfair Competition defines trade secrets: "A trade secret is any information that can be used in the operation of a business or other enterprise and that is sufficiently valuable and secret to afford an actual or potential economic advantage over others." RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 (1995).

The definition of a trade secret is also contained in the comments to section 757 of the first Restatement of Torts: "A trade secret may consist of any formula, pattern, device or compilation of information which is used in one's business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it." RESTATEMENT OF TORTS § 757 cmt. b (1939).

[141] ROGER M. MILGRIM, MILGRIM ON TRADE SECRETS § 1.01[2][a] (2005). One difference between the definition of trade secrets contained in the UTSA and the Restatement (Third) of Unfair Competition, on the one hand, and the Restatement of Torts section 757, on the other, is that section 757 states that information of short duration should not be protected as a trade secret, where the UTSA and Restatement (Third) of Unfair Competition contain no such restriction. *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. d (1995); RESTATEMENT OF TORTS § 757 cmt. b (1939); UNIF. TRADE SECRETS ACT § 1, 14 U.L.A. (1990).

[142] RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. d (1995). The drafters of the Restatement intended this to be consistent with the definition of trade secrets under the UTSA. *Id.* cmt. b.

owner and the owner keeps it a secret.[143] The information is only protected if it is subject to reasonable efforts to maintain its secrecy.[144] However, the owner is not required to go to extraordinary lengths to maintain secrecy; all that is needed is that he or she takes reasonable steps to ensure that the information does not become generally known.[145] Care must be taken to limit access to the information,[146] and such information should only be disclosed in confidence.

A limited disclosure may not cause the information automatically to lose its trade secret status, so long as it is still possible to keep the information secret in the future.[147] One important issue will be whether the trade secret owner is owed a duty of confidentiality by those who receive the information. Such duties can be implied in law, such as between an employer and employee, or based upon an express agreement to keep the information confidential, such as with a non-disclosure agreement between those that receive the information. The lack of such an obligation will likely cause the owner to lose the trade secret status of the information.

i. What Information May Be Protected?

What is interesting about the definition of trade secrets, whether under the UTSA or the Restatement (Third) of Unfair Competition, is that it consistently states that "any information" can function as a trade secret. Under that definition, it would appear that even the information contained on the chip owned by the consumer would be included. So long as this information is subject to reasonable efforts to maintain its secrecy, then the manufacturer should be able to make a reasoned argument that the data contained on the chip is its trade secret. This would be true even with the unique identifier, so long as it cannot be retrieved through normal means—that is, if it is only

[143] MILGRIM, *supra* note 141, § 1.05.

[144] The term "secret" is used in the definition of trade secret in all three formulations. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 (1995); RESTATEMENT OF TORTS § 757 cmt. b (1939); UNIF. TRADE SECRETS ACT § 1, 14 U.L.A. (1990).

[145] RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. f (1995) ("Information known by persons in addition to the trade secret owner can retain its status as a trade secret if it remains secret from others to whom it has potential economic value."); MILGRIM, *supra* note 141, § 1.05.

[146] RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. g. *See also id.* § 39 reporters' note cmt. f. ("the precautions required of the trade secret owner may increase with increasing dissemination").

[147] *Id.* § 39 cmt. f.

transmitted to a "trusted" reader. The same analysis would hold true with the data.

The interesting part of this analysis is whether the person claiming trade secret status in the information can make this claim when the hardware containing the information—the chip on the tag—is likely owned by the consumer. Assuming that the consumer has not expressly agreed to keep the data confidential and not to share it with anyone else, would a court nevertheless protect the data as a secret under these circumstances?

A distinction should be made between the right of the consumer to access the data (or more likely, to permit a third party to access the data), and a third party accessing the data without the consumer's knowledge. In the case of consumers accessing the data, it would seem unlikely that a court would hold them liable for misappropriation of data contained on a chip that they themselves owned, at least without an express agreement to keep the data secret.

ii. Duty of Confidence

Information is protected under trade secret law where there is a duty to keep that information secret. That obligation is created either by implication,[148] as through the duty of loyalty imposed on employees,[149] or expressly by contract.[150] Based on the assumptions in this article, the consumer will not have expressly entered into any such agreement with the purchase of the item. It is possible, however, that a consumer may have expressly agreed to provisions in a contract to keep the data secret, such as the purchase agreement signed when a consumer buys a car, or a click wrap agreement entered into when the consumer installs software. In fact, most agreements relating to the sale of goods are contained in the manuals and warranty documents that a consumer receives along with the product. For purposes of this article, though, it is assumed that no specific agreement relating to confidentiality is included in these agreements.

[148] RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 41(b) (1995); MILGRIM, *supra* note 141, § 1.05, §3.01.

[149] RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 42 (1995); MILGRIM, *supra* note 141, § 5.02[1] ("The relationship between an employer and an employee is a confidential one. The existence of such relationship between employer and employee imposes a duty upon the employee not to use or disclose the employer's confidential information to the employer's detriment.").

[150] RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 41(a); MILGRIM, *supra* note 141, §4.01.

Where no express agreement to keep the data secret exists, it is unlikely that a duty of confidentiality would be implied in the consumer/retailer relationship. Unlike the employer/employee relationship, which has traditionally been recognized to include an implied duty of confidentiality,[151] no such duty exists between a consumer and the seller.[152] Certainly, no such implied duty would be understood to exist between a consumer and the manufacturer. There is no expectation that the consumer will keep any information relating to the manufacturer privatė. In fact, the exact opposite expectation exists—that once the manufacturer's products have been sold, any information contained in the purchased product, or that can be reverse engineered from it, is in the public domain.[153] Even if the product is covered by patents or copyrights, the information is not secret, but just limited in its use by the strictures of patent and copyright law.

Therefore, it is not likely that a court would hold that merely by purchasing an item containing a tag, the consumer impliedly agrees to keep any and all information contained on that tag a secret. Further, since the consumer owns the tag, he or she should have a right to take the tag apart, inspect it, and even use whatever means are at his or her disposal to get access to the data contained on the tag.

By way of analogy, it is hard to imagine that a court would hold a computer owner liable for accessing a browser cookie[154] stored on his or her computer by a company when the computer owner accessed the company's web site. Even assuming that the company had taken reasonable steps to keep the cookie secret, such as by making it a hidden file or encrypting it, it still was located on someone else's computer.

iii. Reasonable Efforts to Keep RFID Data Secret

The amount of information contained on the tag is not directly relevant to whether the information is a trade secret. Thus, the EPC itself, and the compiled data on the chip, could be protected as a trade

[151] MILGRIM, *supra* note 141, § 3.02.

[152] MILGRIM, *supra* note 141, § 1.05 ("Thus, it is an almost undisputed proposition that when an article, the ''secret'' nature of which is fathomable upon scrutiny and inspection, is marketed, the ''secret'' is lost").

[153] *See, e.g.*, Darling v. Standard Alaska Prod. Co., 818 P.2d 677, 681-82 (Alaska 1991) (no trade secret protection where product publicly sold and displayed to parties that copied product); Futurecraft Corp. v. Clary Corp., 205 Cal. App. 2d 279, 289-90 (2d Dist. 1962) ("'Matters which are completely disclosed by the goods which one markets cannot be his secret'"(quoting RESTATEMENT (FIRST) OF TORTS, § 757, cmt. b)).

[154] *See generally* Jerry Kang, *Information Privacy In Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1227-29 (1998) (discussing the function of cookies).

secret, assuming all of the other requirements for trade secret status were met.

First, the manufacturer must use reasonable efforts to maintain the secrecy of the data contained on the tag.[155] What would be deemed reasonable? Limiting access to the data certainly is a necessary precondition to the existence of a trade secret in the data contained on the tag.[156] The average consumer would not have easy access to the information contained on the chip. Such limited access, by itself, is not likely to constitute reasonable efforts to maintain secrecy, however, if the data is easily accessible by someone with knowledge of how to access the data.[157] For example, if the tag is designed to transmit its data to any reader that requests the information, the information would be readily ascertainable and thus not subject to a reasonable effort to maintain its secrecy.

Additionally, the information must not be disseminated widely, and when disseminated, should be done in a manner calculated to keep it secret.[158] While the chips themselves will be widely disseminated, it is unlikely that the data contained on any particular chip would be provided to a wide audience. By its nature, the tag only tracks the particular item to which it is attached, and only provides that information when a reader instructs it to transmit the data. However, if the chip transmits its data whenever it is requested to do so, this certainly would seem to go beyond the limitations imposed under trade secret law to protect such information.

What a court would likely require is that the tag not be accessible by unauthorized readers, at a minimum. This means that the tag should only communicate with approved readers. Further, the data contained in the tag should be protected by some sort of technology limiting access, such as encryption of the data.

There is a more fundamental question: does trade secret law as currently developed even reach information of the nature contained in

[155] RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. f. (1995) ("[T]he requirement of secrecy is satisfied if it would be difficult or costly for others who could exploit the information to acquire it without resort to the wrongful conduct proscribed under § 40."); UNIF. TRADE SECRETS ACT § 1, 14 U.L.A. 538 (1990).

[156] UNIF. TRADE SECRETS ACT § 1, 14 U.L.A. 539, cmt. (1990) ("[R]easonable efforts to maintain secrecy have been held to include advising employees of the existence of a trade secret, limiting access to a trade secret on "need to know basis", and controlling plant access.").

[157] *See, e.g.*, Amoco Production Co. v. Laird, 622 N.E.2d 912, 916-20 (Ind. 1993) (holding that the location of potential oilfields was a trade secret even though information about such location was in the public domain, because it was not readily ascertainable, instead requiring a substantial investment of time, expense, or effort to discover the information).

[158] RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. f (1995).

an RFID tag? Cases analyzing trade secrets are dealing with information created, or at least acquired, by the party claiming trade secret status for the information.[159] So, for example, a customer list, or secret formula, protected as a trade secret is usually generated by its owner. Thus, in the usual case the records are created by the owner or his or her employees or agents and kept in the owner's records or on the owner's computer systems.

With an RFID tag, by contrast, it is the consumer that both creates the record and maintains it, arguably on the consumer's own property (the RFID tag). The item owner can convincingly argue that it is his or her own secret information, and not that of the manufacturer, unlike a customer list. The record is not generated or maintained by the manufacturer, but by the consumer. Even if the manufacturer were only required to prove possession of the trade secret,[160] it would be difficult to show possession of information contained on a tag owned by the consumer, containing information unknown to the manufacturer. In fact, unless otherwise agreed, the item owner can even prevent the manufacturer from ever accessing the tag and associated database,[161] and can destroy the database without any liability.

If the item owner is the creator of the trade secret, and thus its owner, then it is up to the item owner to determine the proper use of, and access to, the database on the tag. Under trade secret law, at least, the item owner would have the right to permit third parties to have access to the data at their discretion. Further, it would be the item owner, in the first instance, that would have the right to assert a claim for misappropriation, given that it is their trade secret that is being taken. The manufacturer would likely not even have standing to sue.[162]

This does not mean that the manufacturer is without an argument. Certainly, the parties could have negotiated a contract

[159] DTM Research, L.L.C. v. AT & T Corp., 245 F.3d 327, 332 (4th Cir. 2001) ("As a consequence, one "owns" a trade secret when one knows of it, as long as it remains a secret."); MILGRIM, *supra* note 141, § 15.01[1][a][iv] (must be owner, or exercising rights granted by owner, to have standing to sue for trade secret infringement).

[160] *DTM Research*, 245 F.3d at 332.

[161] Whether the manufacturer would be liable for unauthorized access is debatable, of course. *See, e.g.*, Intel Corp. v. Hamidi, 30 Cal. 4th 1342, 1350-53 (2003) (emails sent to corporations employees did not amount to trespass to chattels because of a lack of actual harm); *see also* Maureen A. O'Rourke, *Property Rights And Competition On The Internet: In Search Of An Appropriate Analogy*, 16 BERKELEY TECH. L.J. 561 (2001); Dan L. Burk, *The Trouble With Trespass*, 4 J. SMALL & EMERGING BUS. L. 27 (2000).

[162] MILGRIM, *supra* note 141, § 15.01[1].

regarding use and ownership of the data. Further, it is not likely that the manufacturer would be suing the consumer for misappropriation, but rather a third party competitor, and such a competitor would have accessed the data without the manufacturer's consent. One does not have to be the owner of property to be able to assert a claim for trespass; merely having possession of property entitles the person to sue for trespass against someone whose claim is junior to the claimant.[163] Where the manufacturer has put in place reasonable measures to protect the secret nature of the information, a good argument can be made that the manufacturer has a greater interest than a competitor in the information, and therefore a right to sue for misappropriation of that information by a competitor. Where the item owner has not consented to the use of the information by the competitor, a claim for misappropriation should be able to be made out.

Of course, the situation is different where the consumer has granted permission to the competitor to access the data. Where the true owner of the property uses it, the possessor can make no claim. Thus the manufacturer would have no right—at least not under trade secret law—to prevent access to the data.

iv. Misappropriation of Trade Secrets

Trade secret law does not create a right in the information itself.[164] Instead, the UTSA, as well as the Restatements, makes the misappropriation of trade secrets illegal.[165] Generally, a

[163] RESTATEMENT (SECOND) OF TORTS §§ 157-58 (1965); *DTM Research*, 245 F.3d at 332.

[164] RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. c (1995)

[165] UNIF. TRADE SECRETS ACT §§ 2, 3, 14 U.L.A. 619-34 (1995); RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40 (1995); RESTATEMENT OF TORTS § 757 cmt. b (1939);

> Misappropriation is defined under the UTSA as:
>
> (i) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or
>
> (ii) disclosure or use of a trade secret of another without express or implied consent by a person who
>
> > (A) used improper means to acquire knowledge of the trade secret; or
> >
> > (B) at the time of disclosure or use, knew or had reason to know that his knowledge of the trade secret was
> >
> > > (I) derived from or through a person who had utilized improper means to acquire it;
> > >
> > > (II) acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or
> > >
> > > (III) derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or

misappropriation occurs when someone uses improper means to obtain the secret information.[166] Thus, while someone may be liable for copyright infringement even if the copying is innocent, she would only be liable for trade secret infringement if she obtained or disclosed secret information in an improper manner. If the person independently discovers the information, or obtains the information by examining publicly available products and information, she will incur no liability under trade secret law.[167]

As stated by the Supreme Court, "[t]he public at large remain[s] free to discover and exploit the trade secret through reverse engineering of products in the public domain or by independent creation."[168] Its owner has no proprietary interest in the information as such, but only to the extent the information is a secret.[169] This raises the question of whether accessing information contained on hardware that you own would be improper. Obviously, the consumer could expressly agree to not access the information. But absent such agreement, would the consumer incur any liability by accessing the information? The key fact is likely that the manufacturer has freely distributed the tag with the item. As noted in the Restatement (Third) of Unfair Competition, "[i]ndependent discovery and analysis of publicly available products or information are not improper means of acquisition."[170] Since it is legal to purchase a competitor's product and reverse engineer it to determine any trade secret information,[171] the manufacturer would not have a claim against the consumer. The Restatement provides the following example:

> *A* sells a drug compounded from a secret formula. *B*, a competing drug manufacturer, purchases a quantity of *A*'s drug on the open market and learns the formula through scientific analysis. *B* then

> (C) before a material change of his [or her] position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake.

UNIF. TRADE SECRETS ACT § 1, 14 U.L.A. 537 (1995).

[166] UNIF. TRADE SECRETS ACT §§ 2, 3, 14 U.L.A. 619-34 (1995); RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40 (1995); RESTATEMENT OF TORTS § 757 cmt. b (1939).

[167] RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 43 (1995).

[168] *See, e.g.*, Bonito Boats, Inc. v. Thunder Craft Boats, Inc., 489 U.S. 141, 155 (1989).

[169] RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 43 cmt. a (1995) ("The owner of a trade secret does not have an exclusive right to possession or use of the secret information. Protection is available only against a wrongful acquisition, use, or disclosure of the trade secret."); *DTM Research*, 245 F.3d at 332 ("The 'proprietary aspect' of a trade secret flows, not from the knowledge itself, but from its secrecy.").

[170] RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 43 (1995).

[171] *Id.* § 43 cmt. b.

> begins to market a similar product. *B* has not acquired *A*'s trade secret by improper means.[172]

However, has a competitor that accesses the data on a tag owned by the consumer used improper means? First, what if the consumer is unaware of the access? As discussed above, the manufacturer would have to have used reasonable means to protect the information. For example, what if the manufacturer sets up the tag so that it does not broadcast indiscriminately, but only when certain readers, or certain codes, are sent to the tag? That would seem to be a reasonable means. One court has gone so far as to hold that merely flying over a competitor's factory, built in a remote area, amounted to improper means.[173] However, since the competitor is free to purchase the publicly available item and reverse engineer the tag, accessing other tags using that information would not seem to violate trade secret law. It is black letter law that reverse engineering a product freely available in the market place does not violate trade secret law.[174]

Even so, there are cases where a court has held that the method of obtaining the information claimed to be secret creates liability, even if the information itself was subject to being reverse engineered. For example, the Fifth Circuit Court of Appeals held that firmware contained on a chip embedded on microprocessor cards used in telephone switching systems could be a trade secret, even when the cards were sold to third parties and potentially subject to being reverse engineered.[175] The plaintiff, DSC Communications Corp. ("DSC"), manufactured telephone switching systems.[176] As part of an upgrade to the dialing plan required by the Federal Communications Commission, DSC had to upgrade its operating software, which further required DSC's customers to upgrade the microprocessor cards used in the switching systems.[177] The defendant, DGI Technologies, Inc. ("DGI"), sold competing cards for DSC switching systems.[178] In order to be able to make its cards compatible with DSC's upgraded operating system, it needed access to the firmware on the new DSC microprocessor cards.[179]

[172] *Id.* § 43 cmt. b, illus. 1.

[173] E.I. duPont deNemours & Company v. Christopher, 431 F.2d 1012 (5th Cir.1970), *cert. denied*, 400 U.S. 1024 (1971).

[174] Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 476 (1974).

[175] Alcatel USA, Inc. v. DGI Techs., Inc., 166 F.3d 772, 784-85 (5th Cir. 1999).

[176] *Id.* at 777.

[177] *Id.* at 778.

[178] *Id.*

[179] *Id.* at 779.

In order to obtain a copy of the firmware, DGI had to obtain a copy of DSC's software, which then allowed DGI to obtain the information about the firmware DGI needed. DGI obtained the software by having an employee at one of its (and DSC's) customers allow DGI to test its card in a DSC switch.[180] DGI argued that because it was not under any contractual obligation to DSC, and the employee willingly let DGI test out its card, DGI had not used improper means to obtain access to the information contained in DSC's firmware, and had merely engaged in legally permissible reverse engineering.[181] However, the court rejected this argument, holding that there was sufficient evidence to support the lower court's finding that obtaining the software in this way amounted to a misappropriation. In particular, the court felt that DGI used its relationship with the employee, who was susceptible to being hoodwinked, into granting access to the operating software without fully understanding DGI's purpose.[182] As a result, DGI was then able to use "the knowledge it gained from the purloined software to interpret the trade secrets contained in DSC's firmware."[183] Thus, the court focused on the means used to access the information, without fully analyzing whether the firmware was truly secret. What was determinative was that DGI used improper means, which are generally "'means which fall below the generally accepted standards of commercial morality and reasonable conduct.'"[184]

Thus, it is possible that a court would hold that accessing the data on the tag without the permission of the manufacturer amounts to misappropriation of trade secrets. The key issue will be the means employed. If the tag freely broadcasts its contents as soon as it passes close to a reader, this would likely not be improper means. However, if the competitor had to circumvent a password and decrypt the data, perhaps this would be seen to violate generally accepted standards of commercial conduct.

6. Unfair Competition Law

It is generally accepted that there is a right to compete, and that no liability should arise merely from causing harm to someone's

[180] *Id.* at 784-85.

[181] *Id.*

[182] *Id.* at 785.

[183] *Id.*

[184] *Id.* (quoting *duPont*, 431 F.2d at 1016).

business by competing with them.[185] Absent some specific law limiting rights in an intangible asset, such as trademarks or trade secrets, a competitor normally would not incur liability merely by aggressively pursuing a competitor's business.[186] Nevertheless, the Restatement (Third) of Unfair Competition does allow for claims to be brought based on a more generalized theory of "unfair competition."[187]

The Restatement states that such liability is based upon "other acts or practices of the actor determined to be actionable as an unfair method of competition, taking into account the nature of the conduct and its likely effect on both the person seeking relief and the public."[188] The key is that the kinds of conduct that would be actionable depend on their nature and their effect on competition. The comments to this section of the Restatement note that such practices must hinder competition, negatively affecting the efficient working of the marketplace.[189] However, Professor McCarthy, in his treatise on Trademarks and Unfair Competition Law, states that "[c]ourts have little success in defining unfair competition in the abstract, and often resort to statements such as '[t]he controlling question . . . is whether the acts complained of are fair or unfair.'"[190]

A claim of unfair competition does not directly create a property right in the data;[191] instead, it attempts to redress forms of competition that are "too hard." Since no fixed standard exists for determining what constitutes unfair competition, it is difficult to say for certain whether a competitor accessing data on a tag will be considered just a form of robust competition,[192] or an act that falls below minimum commercial standards of fair play, although the former is the most likely outcome.

[185] *See, e.g.*, RESTATEMENT (THIRD) UNFAIR COMPETITION § 1 (1995).

[186] *Id.* See, also, ConFold Pacific, Inc. v. Polaris Industries, Inc. 433 F.3d 952, 959 (7th Cir. 2006) ("In general, if information is not a trade secret and is not protected by patent, copyright, or some other body of law that creates a broader intellectual property right than trade secrecy does, anyone is free to use the information without liability.").

[187] RESTATEMENT (THIRD) UNFAIR COMPETITION §1 (1995).

[188] *Id.*

[189] *Id.* at §1 cmt. g.

[190] J. THOMAS MCCARTHY, MCCARTHY ON TRADEMARKS AND UNFAIR COMPETITION LAW § 1:8; *see also* RESTATEMENT (THIRD) UNFAIR COMPETITION § 1 cmt. g (1995).

[191] *Id.* ("Unfair competition is not an objective 'thing' and has no objective reality. It is merely an intellectual concept convenient to describe a process which goes on in courts of law.").

[192] *See, e.g.*, M & M Rental Tools, Inc. v. Milchem, Inc., 612 P.2d 241, 246 (N.M. Ct. App. 1980) (taking other sales person's call not unfair where motive was not solely to harm competitor).

7. Tort of Misappropriation

The Restatement recognizes a tort of appropriation of trade values, which, in addition to liability for appropriation of trade secrets or violation of the right of publicity, also provides liability where the "appropriation is actionable by the other under federal or state statutes or international agreements, or is actionable as a breach of contract, or as an infringement of common law copyright as preserved under federal copyright law."[193] According to the official comments to this provision, the common law tort of appropriation is a limited tort that only provides a cause of action where an intangible trade value is clearly defined by some other law. "In the absence of such additional interests, the common law has resisted the recognition of general rights against the appropriation of information and other intangible trade values."[194] Since there is no specific recognition of rights in databases in the U.S., or automatically generated data in particular, it is not likely that a court would rely on this section to grant relief to a manufacturer.

The related tort of "misappropriation" grew out of the Supreme Court case, *International News Service v. Associated Press*.[195] The case centered around the use of hot news, gathered by the Associated Press and published in early editions of its members' east coast newspapers. International News Service then took that information, and republished it on the west coast, sometimes even before the Associated Press's members had a chance to publish the news in their own papers.[196] The Court found this to be a form of unfair competition, where one competitor took advantage of the time, effort and expense of another, allowing it to "reap where it has not sown," which the Court held should not be tolerated by the courts.[197]

Use of data created by another, in a manner that permits the competitor to free ride on the efforts of the manufacturer, would appear to fall squarely within the misappropriation doctrine described

[193] RESTATEMENT (THIRD) UNFAIR COMPETITION § 38(c) (1995).

[194] *Id.* at § 38 cmt. b.

[195] Int'l. News Serv. v. Associated Press, 248 U.S. 215 (1918).

[196] *Id.* at 238-39.

[197] *Id.* at 239-40:

> Stripped of all disguises, the process amounts to an unauthorized interference with the normal operation of complainant's legitimate business precisely at the point where the profit is to be reaped, in order to divert a material portion of the profit from those who have earned it to those who have not; with special advantage to defendant in the competition because of the fact that it is not burdened with any part of the expense of gathering the news.

by the Supreme Court. However, although the tort is broadly defined in the *International News* case, the doctrine is not likely to be applied to the use by a competitor of data contained on a tag owned by a consumer. First, the Restatement (Third) of Unfair Competition rejects the reasoning of the *International News* case, because of the potentially negative impact such a tort would have on competition generally.[198] Thus, any court applying the reasoning of the Restatement would likely not find there to be a tort of misappropriation.[199]

Second, courts have generally limited the doctrine to the facts of the original *International News* case,[200] refusing to extend it to other competitive situations.[201] The misappropriation tort's remaining viability is generally limited to "hot news" situations, where the information's timeliness is its value, the defendant is free riding on that information, and allowing copying would reduce the incentive to create the information.[202] Although an argument can be made that the copying of data off a tag is a form of free riding, which if unchecked would create a disincentive to track data, the data on the tag would not be time sensitive, at least in the hot news sense. Since the data can reside on a tag for an unspecified period of time, only being

[198] RESTATEMENT (THIRD) UNFAIR COMPETITION § 38 cmt. b (1995) ("The better approach, and the one most likely to achieve an appropriate balance between the competing interests, does not recognize a residual common law tort of misappropriation.").

[199] *See* Ginsburg, *supra* note 72, at 158 ("Most notably, the recent Restatement (Third) of the Law of Unfair Competition restates much of the misappropriation doctrine out of existence.").

[200] *See, e.g.*, Cheney Bros. v. Doris Silk Corp., 35 F.2d 279, 280 (2d Cir. 1929), *cert. denied*, 281 U.S. 728 (1930); Nat'l. Basketball Ass'n v. Motorola, Inc., 105 F.3d 841, 852 n.7 (2nd Cir 1997) (quoting Judge Learned Hand from the *Cheney Bros.* decision); RESTATEMENT (THIRD) UNFAIR COMPETITION § 38 cmt. c (1995) ("The limited extent to which the INS rationale has been incorporated into the common law of the states indicates that the decision is properly viewed as a response to unusual circumstances rather than as a statement of generally applicable principles of common law.").

[201] *See, e.g.*, *Nat'l Basketball Ass'n*, 105 F.3d at 853-54 (transmission of near real time sports scores of NBA games without permission of the NBA is not unlawful misappropriation of that information).

[202] *Id.* at 852. As described by the Second Circuit, the elements of the tort are:

> (i) the plaintiff generates or collects information at some cost or expense; (ii) the value of the information is highly time-sensitive; (iii) the defendant's use of the information constitutes free-riding on the plaintiff's costly efforts to generate or collect it; (iv) the defendant's use of the information is in direct competition with a product or service offered by the plaintiff; (v) the ability of other parties to free-ride on the efforts of the plaintiff would so reduce the incentive to produce the product or service that its existence or quality could be substantially threatened.

Id. (citations omitted). *Accord* ConFold Pacific, Inc. v. Polaris Indus., Inc. 433 F.3d 952, 960 (7th Cir. 2006).

accessed when near a reader, the manufacturer would be hard pressed to claim that a competitor's use of that data falls under the hot news doctrine.

Third, it is likely that a claim of misappropriation is preempted by copyright law.[203] The stored data comprises a compilation, a work subject to copyright law, although likely not copyrightable as noted above. Where a claim is made that an intangible property right has been misappropriated, and such claimed property right falls within the scope of copyright law, the courts have consistently held that the Copyright Act preempts the state common law tort of misappropriation.[204] Even where courts have entertained the possibility that a misappropriation claim based on copying information is not preempted by the Copyright Act,[205] the courts state that a "hot news" misappropriation claim only survives because the information's timeliness provides the extra element necessary to avoid preemption when compared to copyright infringement.[206] Thus a claim for "misappropriating" the data on a tag is likely to be preempted by the copyright statute.[207]

[203] 17 U.S.C. § 301 (2000) (preemption section of the Copyright Act).

[204] *Nat'l Basketball Ass'n*, 105 F.3d at 851 ("The broad misappropriation doctrine relied upon by the district court is, therefore, the equivalent of exclusive rights in copyright law."); *Alcatel*, 166 F.3d at 785-89; *accord ConFold Pacific*, 433 F.3d at 960 (state misappropriation claim preempted by federal patent law).

[205] *Alcatel*, 166 F.3d at 787 ("If, however, one or more qualitatively different elements are required to constitute the state-created cause of action being asserted, then the right granted under state law does not lie "within the general scope of copyright," and preemption does not occur.").

[206] *Nat'l Basketball Ass'n*, 105 F.3d at 852-53. In fact, the Second Circuit stated that three elements would have to be proven for a misappropriation's claim to avoid preemtion:

> We therefore find the extra elements—those in addition to the elements of copyright infringement—that allow a "hotnews" claim to survive preemption are: (i) the time-sensitive value of factual information, (ii) the free-riding by a defendant, and (iii) the threat to the very existence of the product or service provided by the plaintiff.

Id. at 853.

[207] *Cf.* Ginsburg, *supra* note 72, at 164. ("Finally, misappropriation claims, to the extent they survive copyright preemption analysis, do not afford complete coverage of compiled information because they are, at most, limited to time-sensitive compilations. Static compilations, and even dynamic compilations that lack time-sensitivity, fall outside the claim's ambit.").

B. Ownership of Data as Derivative Work of Copyright in Software

One of the exclusive rights under section 106 of the Copyright Act is the right to make derivative works.[208] A derivative work is defined in the copyright statute as "a work based upon one or more preexisting works, such as a translation, musical arrangement, dramatization, fictionalization, motion picture version, sound recording, art reproduction, abridgment, condensation, or any other form in which a work may be recast, transformed, or adapted."[209] An important part of this definition is that a derivative work is based upon a preexisting work, and not merely created using such a work. Thus the definition limits the scope of a derivative work as one that recasts, transforms or adapts the earlier work. One test for derivative work status is whether the new work infringes upon the original work. If it does, then it is derivative.[210]

An example of a non-derivative work that relies upon an earlier copyrighted work would be a novel written on a computer using Microsoft Word. Clearly Word is a copyrighted software program,[211] and the novel was created using Word to write the new work. However, the novel is not a derivative work of Word, and so no permission is needed to write the novel, and it does not infringe Microsoft's copyrights.

In the same way, the item manufacturer cannot make a good argument that the data is a derivative work of the software on the chip, since it is not based upon, but only generated by, the software that tracks the data. As discussed above, either it is not owned by anyone, or the consumer is the owner (because the consumer is the author) of the data.

III. OWNERSHIP OF DATA THROUGH HARDWARE

Even if the manufacturer does not own the data directly—whether because the data is not subject to ownership by anyone, or because the manufacturer is not the creator of the data or otherwise directly owner of the intangible property—the manufacturer may be able to control the data because it owns the chip in the tag. Given that

[208] 17 U.S.C. § 106 (2000).

[209] *See* 17 U.S.C. § 101 (2000).

[210] M.H. Segan Ltd. P'ship v. Hasbro, Inc., 924 F. Supp. 512 (S.D.N.Y. 1996).

[211] *E.g.*, Microsoft Word v.X:Mac, Copyright Reg. No. TX-5-448-113 (registered Dec. 31, 2001).

the chip (and the antenna) is a piece of tangible, personal property, traditional rules regarding ownership of the chip would apply.

A. Who Owns the Hardware

1. Who Owns the Chip?

As described in the introduction, several advancements in technology now permit manufacturers to embed into their goods tracking technology that can be connected to the manufacturers' systems via wireless networking—RFID, in short. As mentioned, automobile manufacturers such as Lotus already build into their products microprocessors with sufficient memory to track the automobile's vital statistics, as in the aforementioned example of the Lotus Elise. This permits the automobile manufacturer, through its dealers, to better maintain and repair the car.

Before the sale to the consumer, the manufacturer owns the tag, or in the case of a Lotus Elise, the engine control unit. This is true because the manufacturer owned the components that went into making the car, and after the assembly process would own the entire car and its now-assembled components—that is, the manufacturer would hold title to the car. Given that the manufacturer intends to transfer possession of the car to the consumer, questions arise as to whether transfer of title to the car requires that title to all of the components be transferred as well.

2. UCC Article 2 Sales

In every United States jurisdiction, the sale of personal property is governed by Article 2 of the Uniform Commercial Code (U.C.C.). Since automobiles are personal property, the rules about ownership are governed by Article 2. According to section 2-401, title to the car would pass to the consumer when the seller completes delivery of the goods, unless otherwise agreed by the parties.[212] Thus, in the example, title to the car would transfer at the time of delivery of possession of the car to the consumer at the dealership, even if the certificate of title was to be delivered at a later date.[213]

Because the consumer has taken title to the car, such consumer would expect to own all of the tangible components making up the car. That is, after he or she pays for the car, that person would not

[212] U.C.C. § 2-401(2) (2005).

[213] *Id.* § 2-401(2)(b).

expect to own the engine, but only lease the computer in the engine. The same is not true, of course, of the copyrightable programs that run on the embedded computers. Under copyright law, those belong to the author of such works, or to the author's assignees, unless specifically assigned to the consumer by a signed, written agreement, and such assignments are rare. Nevertheless, the consumer is no less the owner of the computer merely because the tangible computer contains intangible copyrighted software. The consumer may even own the copy of the program installed in the car's computer.[214]

Section 2-401 states that title transfers upon physical delivery unless the parties otherwise agree. What if the manufacturer includes a provision in the sales documents that attempts to transfer title to the car, but retain title to the tag? Article 2 makes it clear that any attempt by the seller to retain title, in the case of a sale of the goods, is treated merely as the retention of a security interest under Article 9, and not a retention of title.[215] Thus, if the transaction is deemed to be a sale, then title to the entire car transfers to the consumer, and at best the manufacturer retains a security interest in the tag.

Thus, in this example, the consumer is the owner of the tag, and its embedded chip. This means also that the consumer owns the physical media on which the data is stored.

B. Title to Intangible Data by Title to Tangible Chip

An interesting interplay exists between rights in tangible and intangible property: Does ownership of tangible property entitle you to ownership of intangible property created by that tangible

[214] *See, e.g.*, Softman Products Co., LLC v. Adobe Sys., Inc., 171 F. Supp. 2d 1075, 1083-87 (C.D. Cal. 2001) (unbundling and sale of separate CDs containing Adobe software which was originally sold as a collection not infringement under the first sale doctrine); NIMMER, *supra* note 70, § 8:12[1][d][i] ("In short, the first sale defense would seem as operational in the software setting as it is in comparable circumstances to the millions of videotapes, books, and other physical media that have been sold."); Mark A. Lemley, *Intellectual Property And Shrinkwrap Licenses*, 68 S. CAL. L. REV. 1239, 1259-63 (1995). *Contra*, Adobe Sys., Inc. v. Stargate Software Inc., 216 F. Supp. 2d 1051, 1058-59 (N.D. Cal. 2002); Adobe Sys., Inc. v. One Stop Micro, Inc., 84 F. Supp. 2d 1086, 1092 (N.D. Cal. 2000).

[215] U.C.C. § 2-401(1) (2005). Interestingly, Article 9 specifically states that goods includes "a computer program embedded in goods and any supporting information provided in connection with a transaction relating to the program if (i) the program is associated with the goods in such a manner that it customarily is considered part of the goods, or (ii) by becoming the owner of the goods, a person acquires a right to use the program in connection with the goods." U.C.C. § 9-102(a)(44) (2005).

property?[216] Because the consumer owns the chip, one might expect that the same consumer owns the data contained on the chip.

Title to chattels not previously owned typically is created by taking possession. For example, wild animals are not owned by anyone while they are in the wild, but a person becomes the owner of such animals by possessing them. This rule, discussed in the seminal first year property law case of *Pierson v. Post*, discusses the point. In that case, the land was "wasteland," not owned by anyone.[217] However, the *Pierson* court noted that had the hunters been on land owned by someone, the outcome likely would have been different. The example given was of ducks in a duck pond—where the pond is someone's property, then title to the ducks remains in the real property owner, *ratione soli*.[218]

Likewise, ownership of the chip and the tangible storage medium could give ownership of the data to the consumer, at least where no specific intellectual property law, such as copyright, determines ownership. By owning the physical item, the consumer would own the data contained on that chip, particularly where it is the actions of the consumer that generate the data.

Cases discussing ownership of emails created by employees yield much the same result—because the employer owns the system, the employer owns whatever is contained on that system.[219] Of course, there is an important distinction—the nature of the relationship between the employer and employee, as opposed to that

[216] Under copyright law, for example, mere ownership of a copy of a work does not grant any rights to the copyright in the work:

> Ownership of a copyright, or of any of the exclusive rights under a copyright, is distinct from ownership of any material object in which the work is embodied. Transfer of ownership of any material object, including the copy or phonorecord in which the work is first fixed, does not of itself convey any rights in the copyrighted work embodied in the object; nor, in the absence of an agreement, does transfer of ownership of a copyright or of any exclusive rights under a copyright convey property rights in any material object.

17 U.S.C. § 202 (2000).

[217] *See, e.g.*, Pierson v. Post, 3 Cai. R. 175, 178 (1805):

> So also, encompassing and securing such animals with nets and toils, or otherwise intercepting them in such a manner as to deprive them of their natural liberty, and render escape impossible, may justly be deemed to give possession of them to those persons who, by their industry and labour, have used such means of apprehending them.

[218] *Pierson*, 3 Cai. R. at 179.

[219] *See* Smyth v. Pillsbury Co., 914 F. Supp. 97, 100-01 (E.D. Pa. 1996); McLaren v. Microsoft Corp., No. 05-97-00824-CV, 1999 WL 339015, at *4 (Tex. App. Dallas May 28, 1999) (rejecting employee's argument that messages stored in company email system were private).

between consumer and manufacturer. The employee is an agent of the employer and could be said to create all such information for the benefit of his or her principal, the employer. No such principal-agent relationship exists between a manufacturer and consumer.

In addition, if a thing is not of a type that can be owned, then mere ownership of the land (or chip) on which the thing exists does not create ownership in that thing. In the case of wild animals, the animal is not owned by the landowner until the landowner has possession. But the landowner has a better claim than a trespasser. Likewise, the landowner cannot be said to own the air on his or her land, as such air cannot be owned. Therefore, if the data cannot be owned, then possession and control would not seem to invest the consumer with ownership of the data.

However, with the chip there is a difference when compared to air—the data is fixed in a tangible medium, namely the magnetic data storage. Certainly, the consumer possesses that media. Since it is the bits of information that make up the data, such as the ferrous oxide on a cassette tape, perhaps consumer ownership of the media implies data ownership, as well.

The recent revisions to U.C.C. Article 2 specifically exclude "information" from the definition of goods.[220] The official comment to this section explains that this definition is meant "to exclude information not associated with goods," such as "an electronic transfer of information. . . ."[221] However, where the transaction involves both goods and information, the drafters decided to leave it to the courts to determine whether Article 2 applies to the transaction in whole, in part or not at all.[222] Therefore, no answer is provided

[220] U.C.C. § 2-103(1)(k) (2005). For a discussion of the difficult revision process for Article 2, *see generally* Linda J. Rusch, *A History and Perspective of Revised Article 2: The Never Ending Saga of a Search for Balance*, 52 SMU L. REV. 1683 (1999).

[221] U.C.C. § 2-103 cmt. 6 (2005) (citing Specht v. Netscape, 150 F. Supp. 2d 585 (S.D.N.Y. 2001), *aff'd*, 306 F.3d 17 (2d. Cir. 2002) as an example).

[222] *Id. See also* Linda J. Rusch, *Is The Saga Of The Uniform Commercial Code Article 2 Revisions Over? A Brief Look At What NCCUSL Finally Approved*, 6 DEL. L. REV. 41, 45 (2003):

> Drawing the line between what constituted a good that contains a computer program but is not a computer or computer peripheral (and hence a "smart good" that should be covered by Article 2) and a good that contains a computer program but is a computer or computer peripheral was finally acknowledged to be impossible in the spring of 2002 after numerous attempts to draw the line. . . .
>
> . . . .
>
> . . . When a transaction includes both the sale of goods and the transfer of rights in information, it is up to the courts to determine whether the transaction is entirely within or outside of this Article, or whether or to what extent this Article

under revised Article 2 as to whether ownership of a tangible good includes ownership of the information imbedded in that good.

Nor does the Uniform Computer Information Transactions Act ("UCITA"), the uniform law that came out of the attempts to revise Article 2 during the 1990s,[223] take a position on "smart goods." UCITA was intended to create a uniform law of computer information transactions,[224] which are defined as "an agreement or the performance of it to create, modify, transfer, or license computer information or informational rights in computer information."[225] The typical form of transaction covered by UCITA is a license for software and computer information.[226]

UCITA is only intended to cover transactions in computer information, although provision is made for "mixed transactions."[227] Where the transactions include both computer information and goods, UCITA generally applies to that part of the transaction that deals with information, and other law, such as Article 2, applies to the rest of the transaction.[228] However, where the goods sold include embedded computer programs which are "contained in and sold or leased as part of goods,"[229] then UCITA does not apply to the transaction.[230] The comments to this section go on to explain that "this Act excludes a copy of the computer program if the copy is embedded in, inseparable from, and sold or leased as an indistinguishable part of goods."[231] Examples of where UCITA would not apply are chips contained in toasters, and the programs that control the braking functions of an automobile.[232] Thus, instead of providing a solution to ownership and control of information contained on a tag, UCITA excludes the kind of transactions in which embedded tags would be at issue.

> should be applied to a portion of the transaction. While this Article may apply to a transaction including information, nothing in this Article alters, creates, or diminishes intellectual property rights.

Id.

[223] Rusch, *supra* note 220, at 1686-87.

[224] UNIF. COMPUTER INFO. TRANSACTIONS ACT § 103(a) (2001).

[225] *Id.* § 102(a)(11).

[226] UNIF. COMPUTER INFO. TRANSACTIONS ACT prefatory note.

[227] UNIF. COMPUTER INFO. TRANSACTIONS ACT § 103(b) (2001).

[228] *Id.* at § 103(b)(1) and cmt. 4.

[229] *Id.*

[230] *Id.* There are two exceptions: "(A) the goods are a computer or computer peripheral; or (B) giving the buyer or lessee of the goods access to or use of the program is ordinarily a material purpose of transactions in goods of the type sold or leased." *Id.* § 103(b)(1)(A)-(B).

[231] *Id.* at cmt. 4(b)(3).

[232] *Id.*

C. Bailment

The transfer of the chip to the consumer could be a bailment. A bailment is a transfer of possession of personal property from a bailor to a bailee, without transfer of title to such property to the bailee, and is based upon a delivery of the personal property to the bailee for a specific purpose.[233] One key element that distinguishes a bailment from a sale of personal property is that title does not transfer, but instead remains with the bailor. The bailee has an obligation to restore the property to the bailor, in the same or some altered form. If the bailee does not need to restore the same property, then the cases have held that the transaction is a sale.[234]

Two main definitions of bailment exist. The first is more restrictive, requiring there to be a contractual agreement to the bailment. As stated by Justice Story in his treatise on bailments, "a bailment is a delivery of a thing in trust for some special object or purpose, and upon a contract, express or implied, to conform to the object or purpose of the trust."[235] Professor Williston suggests a second, broader definition, stating that a bailment is "the rightful possession of good by one who is not the owner."[236] Although a question exists about whether a contract is necessary for a bailment,[237] a common element between these definitions is the need for a delivery of the personal property.[238]

In order to establish that a bailment exits, the bailee has to have actual, physical control of the property, and an intent to possess the property. The physical control element is likely not a stumbling block for the possession of the data on the chip, because the consumer will have control over the entire physical item, and thus physical control over the chip embedded in the item. As a result, this element of bailment is met.

[233] 8 C.J.S. *Bailments* § 2 (2005).

[234] *See, e.g.*, Wilson v. Brawn of California, Inc., 132 Cal. App. 4th 549, 558 (2005); 8 C.J.S. *Bailments* § 9 (2005).

[235] JOSEPH STORY, LAW OF BAILMENTS § 2 (Cambridge, Hilliard & Brown 1832); *see also* RAY A. BROWN, THE LAW OF PERSONAL PROPERTY § 10.1 (Walter B. Raushenbush ed., 1975)

[236] 9 S. WILLISTON, A TREATISE ON THE LAW OF CONTRACTS § 1030 (3d ed. 1967). *See also* BROWN, *supra* note 235, § 10.1.

[237] *See* BROWN, *supra* note 235, § 10.1. Justice Story discussed a similar point in a later edition of his book, criticizing the argument that not every bailment was supported by a contract. *See* STORY, *supra* note 235, § 2 n.2.

[238] *See also* 8 C.J.S. *Bailments* § 2 (2005). Justice Story noted that the term bailment comes from the French word *bailler*, "which signifies to deliver." STORY, *supra* note 235, § 2.

The second element requires intent to exercise control over the item.[239] Again, there is clearly an intent to possess the item, because the consumer purchased it. Thus, the consumer intends to exercise control over the item, which would logically include all of the constituent parts of the item. Of course, a problem with this is that the consumer intended to take title to the item, and this would weigh against the finding of a bailment because the consumer did not intend merely to take possession, but also to take title. Many bailment cases emphasize that both parties must intend that the bailee receive possession with an obligation to return it. For example, where a woman delivered a coat with a fur piece concealed inside, the court held that the defendant dance hall was not liable when the fur turned up missing, because the defendant had not intended to take possession of the fur.[240] Of course, this case hinged on the lack of delivery and acceptance of the fur, but is based upon the concept that a bailment arises out of a contract, and since there was no meeting of the minds, no bailment was created.

There are also cases where a bailee was not held liable for the theft of items stored in a trunk of a car, even where there was a bailment of the car. The defendant was not liable because he was unaware that the property was in the trunk, and so no bailment existed. Of course, a bailee will be liable for items he or she should expect to be in the property, such as luggage, but this hinges on what the bailee would reasonably be assumed to know about the contents of the property bailed.[241]

1. Bailment Versus Sale

Treating the transfer of the tag embedded in the item as a bailment has distinct advantages for the manufacturer. Because title has not transferred, the consumer is merely in lawful possession of the tag, rather than the owner of the tag. This would give the manufacturer a stronger argument that the consumer's use of the tag is limited by the contractual nature of the bailment. Assuming a bailment exists, the terms of that bailment are set by the agreement between the manufacturer and the consumer, and may include contractual terms limiting the consumer's rights to use the data.[242]

[239] Brown, *supra* note 235, § 10.3

[240] Samples v. Geary, 292 S.W. 1066 (Mo. Ct. App. 1927).

[241] BROWN, *supra* note 235, §120.3.

[242] *See infra* for a discussion of contractual rights to the data.

However, in order for this argument to succeed, the manufacturer must argue that the transfer of the tag amounted only to a bailment, and not a sale. This can only be true if the rule of UCC 2-401(1)—that an attempted retention of title in the goods delivered by the seller to the consumer is merely a security interest and not retention of title—does not apply. The manufacturer would argue that there are two transactions, one for the sale of goods, and the other for the bailment of the tag.

The UCC does not do away with the law of bailments.[243] If the manufacturer does not intend to part with title, it may be a bailment for hire, which is covered under Article 2A Leases,[244] or some other form of bailment, such as involuntary or gratuitous bailment. For any of these arguments to succeed, however, the manufacturer must intend to retain title, and most courts considering whether a party intended to retain title hold that the party must intend to receive back the exact same item.[245] If the party will receive either different property, or similar property but not the same item, then it is a sale and not a bailment. In some cases, the courts have allowed the bailee to make changes to the item and still have the relationship function as a bailment, but in those cases it is the same item being returned, albeit transformed from its original state when the bailee first received it.

This creates problems for the manufacturer, because the tag is attached to an item that has been sold, and the manufacturer does not intend to ever get the item back. Title has clearly transferred to the consumer for the item. In order for the manufacturer to create a bailment of the tag, it must establish two separate transactions: sale of the item, no return intended; and bailment of the tag, return intended. This is of course theoretically possible—there is nothing illegal about two parties entering into a contractual relationship where one party is both selling some goods, and leasing other goods. However, in order for that contractual setting to exist, the parties must both intend it. Even if the manufacturer attempts to establish such a relationship by using the correct terminology in the contract, a court is free to look

[243] *See, e.g.*, U.C.C. § 2A-103 cmt. k ("The provisions of this Article, if applicable, determine whether a lease agreement has legal consequences; otherwise the law of bailments and other applicable law determine the same.").

[244] U.C.C. § 2A-103 cmt. j ("At common law a lease of personal property is a bailment for hire. . . .").

[245] *In re* Porter, 202 B.R. 109, 115 (N.D. Ind. 1996); Payberg v. Harris, 931 P.2d 544, 545 (Colo. Ct. App. 1996).

past the form of the agreement to its actual substance.[246] And if the manufacturer in fact does not intend to get the tag back, a court will likely hold that title transferred, and that the putative bailment of the tag was really a sale.

In addition, if the manufacturer were able to show that two separate contractual arrangements were made regarding the item and the embedded tag, it would have to establish a working method of retrieving the tag. This in and of itself likely would cost so much that the system would be unsustainable.

2. Article 2A Lease of Chip

Take the other extreme: The consumer has leased the car. Under most car lease agreements, the manufacturer or its agent, the dealer, is the owner of the car. Assuming that the car will retain a significant portion of its value at the end of the lease, it will be respected as a true lease under Article 2, rather than being deemed to be a sale.[247] As a result, the consumer does not own the chip, let alone the software. The tag, the chip and the transmitter are all still the property of the dealer.

Does that mean that the dealer is the owner of the data? Again, although the dealer (treated the same as the manufacturer for this purpose) has made tracking the use and vital statistics of the car possible, it is the lessee's operation of the car that actually creates the database. Does the fact that the dealer still owns the car change the analysis?

An Article 2A lease is just a species of bailment—a bailment for hire.[248] In order for a transaction in goods to be a lease governed by Article 2A, it must meet the relevant definition: "a transfer of the right to possession and use of goods for a period in return for consideration, but a sale, including a sale on approval or a sale or return, retention or creation of a security interest, or license of

[246] *See, e.g.*, Atlas Industries, Inc. v. National Cash Register Co., 216 Kan. 213, 219-20 (1975) (although documents stated transaction was a lease, court ruled that substance of agreement was a sale of goods).

[247] U.C.C. § 2A-103 cmt. j. (2005).

[248] U.C.C. § 2A-103 (2005):

> At common law a lease of personal property is a bailment for hire. While there are several definitions of bailment for hire, all require a thing to be let and a price for the letting. Thus, in modern terms and as provided in this definition, a lease is created when the lessee agrees to furnish consideration for the right to the possession and use of goods over a specified period of time.

Id. (citing Charles W. Mooney, Jr., *Personal Property Leasing: A Challenge*, 36 BUS. LAW. 1605, 1607 (1981)).

information is not a lease."[249] As with bailments generally, the transaction is either a sale or a lease, but not both. The key limitation is that a lease is a right of possession over a specified period.[250] This distinguishes the lease from bailments generally, which have no time period.

As discussed above, title does not pass to the lessee under a lease.[251] If the substance of the transaction is intended as a lease the manufacturer would have a stronger claim to the data. At least the manufacturer could claim an interest in the data that flowed from ownership of the hardware. However, as seen above, mere ownership of the hardware would not make the manufacturer the author for copyright purposes, nor would the manufacturer be in direct possession of the information for trade secret purposes. Even so, a claim against a competitor would at least be bolstered, where the manufacturer could now claim some interest in the tag.

3. Obligations and Liability of Bailee

If the manufacturer can establish that a bailment was created, this would generally make the consumer liable for the loss or destruction of the tag. If the manufacturer does not hold the bailee liable for any loss or damage, then this would constitute evidence that title had passed. Three different levels of duty of care are imposed on a bailee under the common law, depending on the nature of the bailment. If the bailment is mutually beneficial to both bailor and bailee, then the bailee is bound to use ordinary diligence in the care of the item, and is liable when negligent in that care.[252] A bailment for hire, such as a lease of personal property, would be such a circumstance.[253] If the bailment is solely for the benefit of the bailor, then the bailee only has a slight duty of care, and is only liable for gross negligence.[254] Examples include the gratuitous bailee, who receives no compensation or other benefit from keeping the item. Keeping an item for the safekeeping of the bailor is an example.[255] Where the bailment is for the sole benefit of the bailee, then the bailee has a great duty of care, and is liable even for slight negligence.[256]

[249] *Id.* § 2A-103(1)(p).

[250] *Id.* § 2A-103 cmt. (j).

[251] *Id.*

[252] BROWN, *supra* note 235, § 11.2.

[253] *Id.* § 11.1.

[254] *Id.* § 11.4.

[255] 8 C.J.S. *Bailments* § 17 (2005).

[256] BROWN, *supra* note 235, § 11.3.

This is often characterized as a "loan" of goods, or friendly borrowing.[257]

While the bailee is never held to be the insurer of the goods,[258] so that some proof of negligence is necessary under any of these standards,[259] under the circumstances of the sale of an item an associated bailment of the tag would at most be considered a bailment for mutual benefit of the parties, and perhaps even a gratuitous bailment.

IV. "VIRTUAL" OWNERSHIP THROUGH ACCESS CONTROL

Although the data may not be owned directly by the manufacturer, the manufacturer may choose to limit access to the data through technological means. Two likely limits on accessing the data would be password control to access the chip, and encryption of the data on the chip.

A. Technological Limits to Access

The EPCglobal Class 1 Generation 2 (gen 2) standard for RFID chips provides that a manufacturer may control access to the tag through a 32-bit encrypted password. Establishing encryption as part of the standard allows every chip the capability to restrict access to its data.[260] Thus the protocol developed by EPCglobal includes a method of limiting access to the data contained on the tag by password protecting the tag. The specification also contains protocols for encrypting the data being transmitted, including the EPC, by "cover-coding" the transmitted data.[261]

Assuming that these technological choices by EPCglobal are effective at preventing access to the tag, they may prove to be more useful in preventing the copying and use of the data than legal regimes such as copyright or trade secret law. These methods have the added benefit of preventing copying and use regardless of whether the underlying data is itself protected by any of the legal schemes described above.

However, as been made clear over the last decade, oftentimes such attempts to prevent access have met with limited success. For

[257] *Id.* at § 11.1, 11.3; *see also* 8 C.J.S. *Bailments* § 18.

[258] BROWN, *supra* note 235, § 11.1.

[259] *Id.* at § 11.3.

[260] CLASS-1 GENERATION-2 UHF RFID PROTOCOL FOR COMMUNICATION 36 (EPCglobal Jan. 2005).

[261] *Id.* at 44.

example, the encryption system on a DVD, the Content-Scrambling System (CSS), was cracked by a 15 year old Norwegian student named Jon Johansen (colloquially referred to as "DVD Jon"). One version of the program to descramble a DVD, DeCSS, can be written in only 7 lines of code.[262] DeCSS is a 40-bit cipher, which is generally considered to be a very weak level of encryption.[263] Yet the cipher included in the gen 2 protocol is only 32 bits. Even the first attempt at encryption for wireless 802.11b transmission, the Wireless Encryption Protocol (WEP), which can be set for 128-bit encryption, can be broken in minutes with the right software.[264] Therefore, it is likely, given the right tools, that someone will devise a way to quickly and easily circumvent the encryption systems built into the current gen 2 protocol.

Of course, with the development of more sophisticated tags, such as the fully active Class 4 tags anticipated by EPCglobal, the encryption systems will likely become more sophisticated, possibly even providing for the real time encryption of the data on the chip itself, and not just when sending the data to the reader. Also, stronger ciphers will be used to communicate with the readers, much like how the 802.11 encryption system has migrated from WEP to WPA and WPA2.

B. Legal Limits to Access

Instead of creating liability for the copying or accessing of the data, legal limits may also be placed on access to the data, where such access can include eavesdropping on the transmission of data, or causing the data to be transmitted by the tag. The U.S. government has taken steps to make accessing data and capturing transmissions and communications illegal.

[262] Declan McCullagh, *Descramble That DVD in 7 Lines*, WIRED, Mar. 7, 2001, *available at* http://www.wired.com/news/culture/0,1284,42259,00.html. *See also* Gallery of CSS Descramblers, http://www.cs.cmu.edu/~dst/DeCSS/Gallery/ (last visited Mar. 24, 2006) (extensive site discussing many permutations of DeCSS).

[263] *See, e.g.*, William A. Hodkowski, *The Future Of Internet Security: How New Technologies Will Shape The Internet And Affect The Law*, 13 SANTA CLARA COMPUTER & HIGH TECH. L.J. 217, 234 (1997) ("[B]ecause of modern technology, symmetric encryption using 40-bit keys offers virtually no protection against brute-force attacks.").

[264] Humphrey Cheung, *The Feds Can Own Your WLAN Too*, TOM'S NETWORKING, Mar. 31, 2005, http://www.tomsnetworking.com/Sections-article111-page2.php.

1. DMCA

The Digital Millennium Copyright Act (DMCA) was enacted in 1998 to deal with the burgeoning illegal digital duplication of copyrighted works.[265] In order to address the problem of protecting copyrights of digital works in the age of the Internet,[266] the federal government put into place three legal restrictions on the circumvention of technological measures to protect a copyrighted work, making it illegal: first, to circumvent a technological measure which controls access to a work;[267] second, to traffic in a technology, product, service or device that assists in circumventing the access control;[268] and third, to traffic in a technology, product, service or device that assists in circumventing a technology that effectively protects a right in a work under copyright.[269]

All three of these prohibitions are limited by their language to circumventing technological means controlling access to a work protected under copyright law. Thus, it is not illegal to circumvent an access control which is limiting access to a work not protected by copyright. This limitation clearly reduces the scope of § 1201(a)(1), the provision which prohibits circumvention of access controls. For example, it would not be illegal for the owner of the media to de-encrypt an encrypted copy of a Shakespeare play under this provision.

However, just because it is legally permissible to break the encryption on a work of Shakespeare does not imply that it is also legal to traffic in such decryption technology. Although the trafficking provisions of § 1201(a)(2) also include a reference to "a work protected under this title,"[270] selling such technology likely is still illegal.[271] This is because if the circumvention technology is "primarily designed" for accessing copyrighted works, then it is still

[265] 17 U.S.C. § 1201 (2000).

[266] *See generally* USPTO WORKING GROUP ON INTELLECTUAL PROPERTY RIGHTS, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE 7 (Sept. 1995), *available at* http://www.uspto.gov/web/offices/com/doc/ipnii/ ("The merger of computer and communications technology into an integrated information technology has made possible the development of the National Information Infrastructure which will generate both unprecedented challenges and important opportunities for the copyright marketplace.").

[267] 17 U.S.C. § 1201(a)(1) (2000).

[268] 17 U.S.C. § 1201(a)(2) (2000).

[269] 17 U.S.C. § 1201(b) (2000).

[270] 17 U.S.C. § 1201(a)(2)(A) (2000).

[271] *See* Jane C. Ginsburg, *Copyright Legislation For The "Digital Millennium"*, 23 Colum.-VLA J.L. & ARTS 137, 144-48 (1999).

illegal, even though it also can be used to access public domain works.[272]

The same result occurs with the § 1201(b) rules—if the technology is designed "primarily" to circumvent a technological protection of a right conferred by copyright (such as the right to copy, distribute, or publicly perform the work), then it does not matter if it can also be used to copy, distribute or publicly perform a public domain work.[273]

With respect to the data contained on the tag, as discussed above it is unlikely that the EPC or the data will be protected under copyright law. Thus, unlike the cases finding liability for "cracking" DVDs, where the technology was used almost exclusively to access copyrighted content, in the case of RFID it would not be illegal to circumvent the access controls in an RFID tag, such as the password control built into the gen 2 protocol.

Even so, it may still be illegal to traffic in the technology that permits access to such information. If the devices or technology distributed to access the data were of the same type used to access copyrighted works, then the distributor would run afoul of the anti-trafficking rules.[274] In fact, it is illegal even to manufacture, import, offer to the public, or provide such technology, let alone traffic in it.[275]

2. ECPA

Because the tag transmits radio signals to communicate with the reader, in order to retrieve the data a competitor would have to "eavesdrop" on that communication. As a result, a competitor accessing the data by intercepting an electronic communication or accessing information stored about such communication must be concerned about violating the Electronic Communications Privacy Act (ECPA).[276] The ECPA is a complex statute to understand, so

[272] *Id.*

[273] Ginsburg, *supra* note 271, at 152:

> If the circumvention device (etc.) is designed for or can be put to commercially significant fair use, then it is not a violation of § 1201(b) to sell the device or to offer the circumvention service. Here, as in the case of circumventions of access controls, however, the device itself probably cannot distinguish between circumventions for fair use purposes, and circumventions aimed simply at obtaining unauthorized copies.

[274] *Id.*

[275] *Id.*

[276] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, §§ 101-303, 100 Stat. 1848 (1986) (codified at 18 U.S.C. §§ 1367, 2510-2521, 2701-2710, 3121-3126

much so that the Fifth Circuit has noted that "[u]nderstanding the Act requires understanding and applying its many technical terms as defined by the Act, as well as engaging in painstaking, methodical analysis."[277]

The ECPA makes illegal two different acts relating to an electronic communication.[278] First, it is illegal under Title I of the ECPA to intentionally intercept an electronic communication.[279] Second, it is illegal under Title II of the ECPA to obtain access to a stored electronic communication without authorization,[280] Title II is commonly referred to as the Stored Communications Act,[281] which was added to the ECPA's amendments to the Wiretap Act to address issues relating to unlawful access to communications such as email.[282] Both of these restrictions create criminal[283] and civil liability.[284]

On the surface, it would seem that intercepting a communication from a tag to a reader, or accessing data stored on a tag, would fall under such legal restrictions. However, there are several arguments why such acts are not illegal under the ECPA when they relate to RFID tags.

First, in order for a transmission of data from a tag to a reader to fall under Titles I and II of the ECPA, it must be an "electronic communication" as defined in 18 U.S.C. section 2510. Electronic

(2000)) (hereinafter ECPA). Title I of the ECPA, §§ 101-111, regulates the interception of communications under the ECPA; Title II of the ECPA, §§ 201-202, governs accessing information stored on an electronic communication facility.

[277] Steve Jackson Games, Inc. v. U.S. Secret Service, 36 F.3d 457, 461 (5th Cir.1994).

[278] It is also illegal under the ECPA to install a pen register or trap and trace device to discover a telephone number dialed without a court order. 18 U.S.C. § 3121 (2000). "Basically, a pen register is a device or process which records the telephone numbers of outgoing calls; the trap and trace device captures the telephone numbers of incoming calls." *In re* Application for Pen Register and Trap/Trace Device with Cell Site Location Authority, 396 F. Supp. 2d 747, 749 (S.D. Tex. 2005) (citing 18 U.S.C. § 3127). However, since a tag is not a telephone, such restrictions are not relevant to this discussion.

[279] 18 U.S.C. § 2511(1)(a) (2000). This section further makes use, disclosure or other related activity with an intercepted electronic communication illegal. *Id.* § 2411(1)(b)-(e).

[280] 18 U.S.C. § 2701(a) (2000).

[281] United States v. Councilman, 418 F.3d 67, 81 (1st Cir. 2005).

[282] *Id.* at 80-81. *See also* Orin S. Kerr, *A User's Guide To The Stored Communications Act, And A Legislator's Guide To Amending It*, 72 GEO. WASH. L. REV. 1208 (2004).

[283] 18 U.S.C. § 2511(4) (2000) (criminal liability for intercepting an electronic communication); 18 U.S.C. § 2701(b) (2000) (criminal liability for illegal obtaining stored electronic communication).

[284] 18 U.S.C. § 2511(5) (2000) (civil liability for intercepting an electronic communication); 18 U.S.C. § 2707(a) (2000) (civil liability for illegal obtaining stored electronic communication).

communication is generally defined as "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, photoelectronic or photooptical system that affects interstate or foreign commerce."[285] While transferring data by radio communications is general covered by this definition, specifically excluded is "any communication from a tracking device (as defined in section 3117 of [Title 18])."[286] Section 3117 defines a tracking device as "an electronic or mechanical device which permits the tracking of the movement of a person or object."[287] In many earlier cases, tracking devices were often referred to as "beepers."[288] However, as noted in a recent federal district court opinion,

> Aside from its welcome brevity, the definition is striking for its breadth. Note that a device is covered even though it may not have been intended or designed to track movement; it is enough if the device merely "permits" tracking. Nor does the definition suggest that a covered device can have no function other than tracking movement.[289]

Given that an RFID tag was primarily designed for the purpose of tracking individual items, it would seem to clearly fall under the definition of a tracking device. Even though the active tags may also store information unrelated tracking the location of the tag, as noted by the district court, so long as the tag permits tracking, it is a tracking device.[290]

As a result, it is likely that the ECPA would not apply to a communication to or from a tag. So, for example, if a competitor were somehow to intercept and use the transmission of data from a tag to a reader, this would not violate Title I.[291] This is true even if the nature of the communication has nothing to do with tracking, because the exclusion covers any communication from a tracking device. This also means that accessing information on the tag would not violate the

[285] 18 U.S.C. § 2510(12) (2000).

[286] 18 U.S.C. § 2510(12)(C) (2000).

[287] 18 U.S.C. § 3117(b) (2000).

[288] United States v. Dunn, 480 U.S. 294, 296-97 (1987); United States v. Karo, 468 U.S. 705, 707 (1984); Michael v. United States, 454 U.S. 950, 950 (1981); Miroyan v. United States, 439 U.S. 1338, 1340 (1978).

[289] *In re* Application for Pen Register and Trap/Trace Device with Cell Site Location Authority, 396 F. Supp. 2d 747, 753-54 (S.D. Tex. 2005) (rejecting the government's argument that a tracking device is limited to "one-way radio 'homing' devices").

[290] *Id.* at 753.

[291] 18 U.S.C. § 2511(a)-(e) (2000).

Stored Communications Act, because you have to "obtain[], alter[], or prevent[] authorized access to a[n] . . . *electronic communication* while it is in electronic storage."[292]

Second, even if the communication between the reader and the tag would be an electronic communication, the data on the tag is not protected. The ECPA defines an electronic communication as "any *transfer* of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted. . . ."[293] While the data is stored on the chip, it is not a communication, it is just data. Thus, accessing the tag to obtain the data would not violate the Stored Communications Act because the data would not be a stored communication.[294] Nor is it likely that the data would be "in electronic storage" while on the tag, because only temporary storage of the transmission while in transit, or backup storage of an electronic communication, is included in that definition.[295]

C. Limited Statutory Responses to RFID and Other Embedded Technology

1. RFID Right to Know Legislation

There are legislative movements to require merchants attaching RFID tags to their products to provide notice to consumers. California and Utah proposed, but ultimately did not pass, such legislation.[296] C.A.S.P.I.A.N., a consumer advocacy group that is actively fighting the use of RFID tags on products, has proposed a federal law, entitled the "RFID Right to Know Act of 2003," which requires labeling of all products that contain tags.[297]

[292] 18 U.S.C. § 2701(a) (2000). Exclusion of a tag from the definition of electronic communication also precludes application of other parts of the Stored Communications Act regarding stored communications held by a "remote computing service," because to be such a service one must to provide "computer storage or processing services by means of an electronic communications system." 18 U.S.C. § 2711(2) (2000). Since an electronic communications system "means any service which provides to users thereof the ability to send or receive wire or electronic communications," 18 U.S.C. § 2510(15) (2000), this prevents application to RFID tags.

[293] 18 U.S.C. § 2510(12) (2000).

[294] 18 U.S.C. § 2701(a)(2) (2000).

[295] 18 U.S.C. § 2510(17) (2000). *See Councilman*, 418 F.3d at 79 ("We conclude that the term 'electronic communication' includes transient electronic storage that is intrinsic to the communication process for such communications.").

[296] Reuven, et al., *RFID, Electronic Eavesdropping and the Law*, RFID JOURNAL, Feb. 14, 2005, http://www.rfidjournal.com/article/articleview/1401/1/128/.

[297] RFID Right to Know Act of 2003, *available at* http://www.nocards.org/rfid/rfidbillsummary.shtml (last visited Mar. 25, 2006).

CONCLUSION

Determining the ownership of, or proprietary rights in, data contained on embedded tracking technology presents several difficult factual issues. First, while the merchant creates the unique identifier (the EPC), all of the other data tracked are generated by the actions of the consumer. Again, this is different from the typical claim where the party asserting an interest (the merchant) is responsible for the creation of the data, or at least its compilation. Second, because the data are generally compiled automatically by a system predetermined by the merchant, it is not likely that the merchant can establish a valid claim of copyright in a compilation of that data. Third, because the data is contained on a tag embedded in an item of personal property owned by a consumer, it is likely that the consumer owns the tag. As a result, the circumstance can be distinguished from situations where the party claiming proprietary rights in the data owns the hardware.

Even if neither copyright law nor property law gave rights to the merchant in the data, it may be that the merchant can control data through other means, such as claiming a trade secret interest in the data, at least to the extent that he or she has taken reasonable steps to limit access. However, this would create an unusual claim of trade secret rights, where the merchant is claiming an interest in data contained on a tag owned by a consumer, generated automatically by the tag. While the definition of trade secret may not exclude such a possibility, neither is it clearly supported by the cases considering trade secrets, or by the Restatement (Third) of Unfair Competition.

The merchant may be able to circumvent these legal hurdles through technological means, by using encryption and password protection systems for accessing the data. It may be that to the extent that a merchant can claim that such technological protections could be used to protect a copyrighted work, the Digital Millennium Copyright Act would prohibit competitors from accessing the information. However, this would require an application of the DMCA to protect information that is likely not itself copyrightable, because in theory the technology could protect a copyrighted work. This would require an extension of the DMCA and its anti-circumvention provisions beyond what the courts have currently been inclined to grant.

In sum, it is likely that a merchant will have little luck in claiming proprietary rights in the data contained in embedded tracking technology.

*   *   *