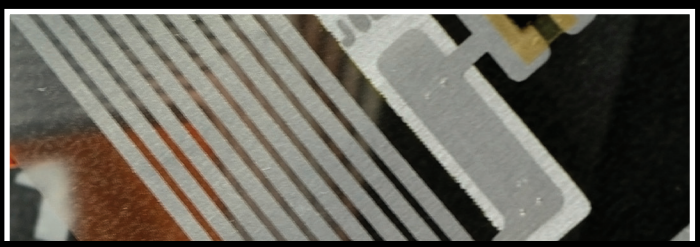
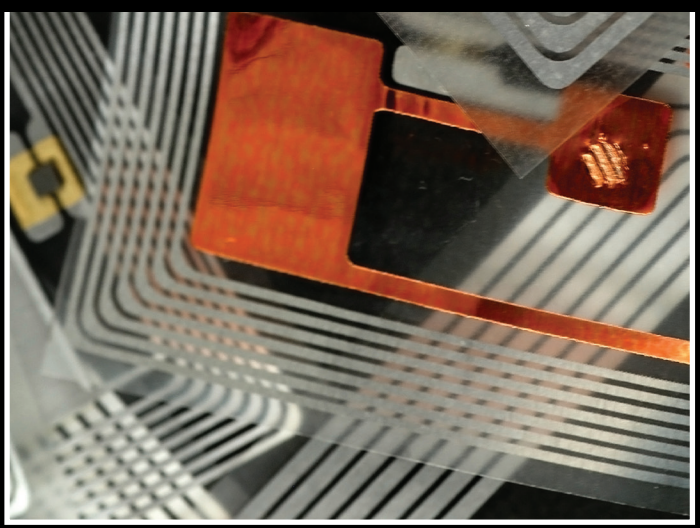


RFIDs, Near-Field Communications, and Mobile Payments

A GUIDE FOR LAWYERS



Sarah Jane Hughes, Editor
with Stephen T. Middlebrook
and Candace M. Jones

CYBERSPACE LAW COMMITTEE

AMERICAN BAR ASSOCIATION
Business Law Section

CHAPTER 19

An Economic Survey Analysis of the Legal Literature Pertaining to the Privacy Implications of Radio Frequency Identification Technology

Mike Jerbic*

I. Introduction

Radio frequency identification (RFID) technology is general technology increasing in use globally for the identification and tracking of people, animals, and things. Over the past decade, legal scholars and practitioners have published a substantial body of literature that discusses how use of the technology could threaten individual consumer privacy interests. In response to this literature and other events, former California Governor

*Mike Jerbic, an electrical engineer, economist, and a long-time member of the Cyberspace Law Committee, is principal consultant at Trusted Systems Consulting Group, a lecturer in Economics at San Jose State University, and a member of the Board of Directors of California Hydronics Corporation. Professor Jerbic is a past chair of The Open Group Security Forum and formerly worked at Hewlett Packard. His other publications include Mike Jerbic and Stephen S. Wu, *The Security Rule*, in A GUIDE TO HIPAA SECURITY AND THE LAW (ABA, 2007); Mike Jerbic et al., *Information Security Strategy: A Framework for Information-Centric Governance* (The Open Group Security Forum, 2007), www.opengroup.org (document W075); and Mattias Hallendorff and Mike Jerbic, *Framework for Control over Electronic Chattel Paper— Compliance with UCC §9-105*, 61 BUS. LAW. 721 (Feb. 2006).

Arnold Schwarzenegger signed Senate Bill 31 on September 30, 2008.[1] This law outlaws the skimming of personal information from RFID tags embedded in identity documents, such as passports, without the data subject's knowledge or consent. It provides for imprisonment for up to one year, a fine of not more than $1,500, or both.[2]

Although the legal literature focuses on privacy rights and law theory, intellectual property theory, and other matters related to law, it occasionally also analyzes involved actors' economic interests to justify government intervention (or nonintervention) in the use of RFID technology. This essay surveys the legal literature from about 2004 through 2008 and looks at the economic arguments made and risks identified in various legislative proposals and recommendations related to the private sector use of RFID technology. The essay concentrates its analysis in these dimensions:

- Market (private) interests, power, and failure
- Privacy risk analysis broken down into expected value of loss and possible or speculative value of loss
- Alternatives to state coercion in managing privacy concerns: private sector norms, architectures, and markets
- Suggestions for future work that provides the highest return for a marginal research investment

This essay is written for those who have an interest in affecting public policy around this issue. Although the policy-making process may not require economic analysis, legislators and advocates of any position would improve their argumentative position through consideration of the economic implications of their proposals and positions. Incentives matter and modifying the law changes incentives for all affected parties.

II. How the Economics of Private Information are Different from Ideas and Knowledge Generally

Thomas Jefferson commented on the possession and use of information:

1. S.B. 31, 2007-2008 Leg., Reg. Sess. (Cal. 2008).
2. S.B. 31, 2007-2008 Leg., Reg. Sess. (Cal. 2008).

> If nature has made any one thing less susceptible than all others of exclusive property, it is the action of the thinking power called an idea, which an individual may exclusively possess as long as he keeps it to himself; but the moment it is divulged, it forces itself into the possession of every one, and the receiver cannot dispossess himself of it. Its peculiar character, too, is that no one possesses the less, because every other possesses the whole of it. He who receives an idea from me, receives instruction himself without lessening mine; as he who lights his taper at mine, receives light without darkening me. That ideas should freely spread from one to another over the globe, for the moral and mutual instruction of man, and improvement of his condition, seems to have been peculiarly and benevolently designed by nature, when she made them, like fire, expansible over all space, without lessening their density in any point, and like the air in which we breathe, move, and have our physical being, incapable of confinement or exclusive appropriation. Inventions then cannot, in nature, be a subject of property.[3]

Economists describe information of all kinds such as ideas, knowledge, and records, as nonrival, nonexcludable goods which, after initial production, maximizes social welfare when used and reused as much as possible to produce marketable goods and services. Economists model information production as having a fixed cost to produce but no additional, incremental costs on each subsequent reuse. Guided by Adam Smith's "invisible hand,"[4] profit seekers aggregating, transforming, and repurposing information for private gain not only make themselves better off, but make all of us better off as well.

Reusing, aggregating, transforming, and repurposing personal and "private" information, however, can place costs upon the *subject of that*

3. Letter from Thomas Jefferson to Isaac McPherson (Aug. 13, 1813), *in* 13 The Writings of Thomas Jefferson, at 333-35 (Andrew A. Lipscomb & Albert Ellery Bergh eds., 1905), *available at* http://press-pubs.uchicago.edu/founders/documents/a1_8_8s12.html.
4. Adam Smith, An Inquiry into the Nature and Causes of the Wealth of Nations, at 363-64 (1776), *available at* http://www2.hn.psu.edu/faculty/jmanis/adam-smith/Wealth-Nations.pdf.

information who subsequently may bear embarrassment, loss of reputation, intrusion into his or her personal space, criminal misuse, and other consequences. Incrementally using private information without internalizing these costs incentivizes profit seekers to overuse and over-reuse private information for private gain at the expense of an overall reduction in total welfare. This is the economic problem, or market failure, that government intervention through privacy policy, law, and regulation tries to solve. The severity of the real empirical problem and the effectiveness of the solutions to that problem are other matters. Regulatory solutions are tradeoffs that not only have the anticipated benefits, but costs as well.

III. How Contactless Data Exchange May Affect Privacy Differently than Other Identification Technologies

Regulating the use of private information is common around the globe. What makes contactless data exchange something new to regulate or otherwise control? What is specific to this technology that worries privacy advocates and policymakers over and above other forms of collecting sensitive private information? Briefly, contactless data exchange technology as expressed through the example of radio frequency identification (RFID) has these features and consequences not previously seen.

A. The kind of data available.

RFID tags can contain anything. When embedded in an ID card, they can contain any manner of personal information. When attached to a product, they can identify product manufacturer, product number, and serial number for an unlimited number of products. In other words, RFID tags have the potential to uniquely identify every person and thing on the Earth. In the supply chain, they have been called "barcodes on steroids."[5]

5. The Honorable Patrick Leahy, United States Senate, The Dawn of Micro Monitoring: Its Promise, and its Challenges to Privacy and Security, Address Before the Conference on Video Surveillance: Legal And Technological Challenges, Georgetown Univ. Law Ctr.

B. Data collection at a distance and without consent of the consumer.

RFID tags contain information that a radio transmitter/receiver "reader" can read and harvest at a distance ranging from a few inches to about 30 feet, without the knowledge or consent of the data subject. Using radio, the "reader" does not even need a line of sight to read the "tag." Deriving their power from the radio frequency transmissions from the reader, high-volume, low-cost RFID tags also operate free from local power sources. Without emitting any constant signal, which might alert the consumer, and without any power source to wear out, these tags can operate indefinitely and without any consumer awareness.

Although RFID tags considered in this analysis are the inexpensive "read only" and "passive" variety, they can contain a block of any information the tag producer wishes to encode. This might include personally identifiable individual, access, and authorization information for ID card use; product identification information for anticounterfeiting; inventory tracking that management integrated into products or their packaging; and health record information encoded into chips implanted into patients. The tag's producer knows what's on the tag. Consumers do not, making them unaware of what information is being collected about them.

Because the tags can be small, about the size of a grain of rice, consumers may be ignorant of their presence and use in products. Clothing may have an RFID tag nearly invisibly integrated into a label or piece of fabric, for example. A consumer wearing a tagged article of clothing and carrying an RFID identification card or passport could, after an initial scan with both the clothing and passport, be later identified solely by identifying the clothing article alone, raising an issue of whether scanning her clothing violates her privacy rights.

(Mar. 23, 2004), *available at* http://www.fas.org/sgp/congress/2004/s032304.html. Senator Leahy appears to have coined the phrase "barcodes on steroids."

C. Data aggregation to build profiles.

Data collected from RFIDs can be aggregated to build consumer profiles, again without the consumer's knowledge. Privacy advocates worry that tags identifying products can be read in conjunction with consumer ID information to build profiles of that consumer, which could reveal that Consumer X buys brand Y, reads books Z, associates with other consumers A, B, and C, etc. Profiles built would have a market value to both private and public organizations.

D. Data repurposing, reuse, and resale

As data are aggregated and profiles built, even if consumers consent to an initial use of information, data can be used for purposes not conceived at the time of consent. In addition, profiles compiled from data collected may be valuable for new purposes, and profile holders may sell profiles or other aggregated information to willing buyers, including public-sector buyers. Although data reuse and resale is nothing new, RFID technology may reduce the cost of individual data collection and aggregation, and may improve the specificity and quality of the data to the point where new privacy threats emerge that previously were economically unfeasible.

"Contactless data exchange," or "RFID," is not one but a collection of information devices that spans a spectrum of low-cost, low-function devices to high-cost, high-function devices and systems. The low-cost, rice-size, passive RFID chips represent the high-volume, low-cost part of the market. Beyond its uses for inventory management, this technology has been integrated into credit and debit cards, employee identification cards, automobile keys, and other applications where a low-cost, contactless electronic identifier improves productivity, performance, and security.

At the high-cost, high-function end of the spectrum, services such as GM's OnStar—a tracking and emergency response system—and the FasTrak highway and bridge toll transponder also are within the scope of "contactless data exchange technology." All these technologies share the potential that data may be collected without the data subject's knowledge

or permission, aggregated to build profiles, and subsequently repurposed, reused, or resold.

Just as in any other differentiated-product market, competition in contactless information exchange markets likely will produce products at various cost and value price points. Although the literature emphasized privacy threats from the lowest-cost, highest-volume RFID tag technology, only time will tell which technical price-information source may or may not turn out to be the most privacy-relevant one.

As a new technology ripening for commercial and government use and abuse, contactless data exchange appears to threaten individual privacy as traditionally appreciated and expected. The question surveyed now, and the subject for the rest of this essay, is "how has the literature assessed these threats as a matter of economic theory and incentive?"

IV. Private Market Forces, Power, and Failure

Underlying any market force theory is the notion that property rights in information are well defined and exchangeable. Lars Smith asks that very question in his paper, *RFID and Other Embedded Technologies: Who Owns the Data?,* and the answer is far from obvious.[6] A consumer's property rights in information about himself or its aggregation are unclear. Does the originator or collector of the information have ultimate control over who can read it as copyright law might imply? Might the reader owner(s) "own" the harvested data more than the entity that originally installed or placed the RFID tag into the object? Does the possessor of the device on which the information is stored own it as tangible property law might imply? Somehow is it a combination of both? Neither? What law dominates? Market exchanges of information rights leading to privacy rights depends on solving this problem.

One thing is certain, however. A consumer's right to control information about himself is not absolute, but one that depends on the situation. No one has a right to privacy to control incriminating evidence about himself

6. Lars S. Smith, *RFID and Other Embedded Technologies: Who Owns the Data?*, 22 Santa Clara Computer & High Tech. L.J. 695 (2006).

when, for example, law enforcement has a warrant to search for that evidence. Consumers generally have no rights to keep their actions private when conducted in a public place. Therefore, privacy is a question not of whether there's some protection, but how much and under what circumstances.

In spite of confusion over the definition and initial assignment of rights, the surveyed literature separated into two general categories of its interpretation of markets and market forces: (1) free market forces dominate and sustain efficient privacy, and (2) market failure forces dominate and prevent efficient privacy.

A. Free market forces dominate and sustain privacy

Consumers negotiate preferred levels of privacy with business, achieving an economically efficient and mutually agreeable level of well-being based on market opportunity, incentives, and equilibriums. Commentators including Brito[7] and Ulatowski[8] show how RFID applications can be created, tried out, and, if found sufficiently objectionable to consumers, die out without any government intervention.[9] Using the Nike and iPod Sport Kit as an example, Ulatowski discusses the commercial viability of a hypothetical RFID reader network that scans information from iPod Sport Kit customers passing by the readers during their routine exercise and concludes:

> Beyond simple hackers, this technology might be attractive to the corporate world. In fact, it would be quite easy, and possibly quite lucrative, "for a company to build their own tiny readers and deploy them in a large environment, selling the data stream to those who would track spouses or teens, or collect information about how many people wearing Nikes visit malls or movie theaters." Retailers are not likely to employ this technology, however, because they have little

7. Jerry Brito, *Relax, Don't Do It: Why RFID Privacy Concerns Are Exaggerated and Legislation Is Premature*, 2004 UCLA J.L. & Tech. 5 (2004).
8. Laura M. Ulatowski, *Privacy on the Internet and in Organizational Database: Recent Developments in RFID Technology: Weighing Utility Against Potential Privacy Concerns*, 3 ISJLP 623 (2008).
9. *See* Brito, *supra* note 7; Ulatowski, *supra* note 8.

> motivation to invade customers' privacy. The public backlash would probably be reason enough to dissuade retailers from employing such technology.[10]

Proponents of the "free market forces dominate" theory suggest government regulatory restraint, and if any intervention is needed, government should implement it only after the public need has been firmly established. Brito, in particular, writes: "Before we regulate, we should first confirm that privacy fears are not baseless and will not be constrained by market forces. Additionally, we should be more concerned by government use of RFID—something to which privacy advocates have paid little attention."[11]

B. Market failure forces dominate and prevent privacy

This theory posits that some businesses will have sufficient market power to coerce consumers into exchanging their personal information or allowing information to be collected about them involuntarily. Alternatively, consumers unwilling to share their information will "be forced" to pay for that choice through higher retail prices. This theory rests on an assumption that major retailers have pricing power and will use it to gather, aggregate, and exploit personal information for private business use at the expense of the efficient public good privacy level. Eden[12] and Stein[13] share this general view. Eden, in particular, writes:

> There are two broad threats to privacy posed by this new technology. First, under our current privacy regime private companies are at liberty to gather, process, and share customer data without obtaining customer consent to specific data aggregation, archival, and sharing policies and procedures. This feature of our privacy regime is particularly vexing

10. Ulatowski, *supra* note 8, at 635.
11. Brito, *supra* note 7, at 5.
12. 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).
13. Serena G. Stein, *Where Will Consumers Find Privacy Protection from RFID?: A Case for Federal Legislation*, 2007 Duke L. & Tech. Rev. 3 (2007).

> given that we live in an era in which identity theft is particularly common and extremely hard to prevent; thus control over private data is extremely important. Second, the absence of meaningful regulation of new surveillance technologies, particularly RFID, is having a profound effect on the broader social norms that privacy protects. Private facts about consumer preference patterns are currently treated as cost-free commodities for corporate America: companies need not pay for the privilege of aggregating and using data, nor is consumer consent regarded as necessary because consumer surveillance has already been presented as a common practice that is usually in consumers' best interests.[14]

In light of dominant market failures leading to inefficiently low public privacy expectations, proponents of this theory advocate preemptive government intervention to prevent privacy abuses and erosion of public expectations.

Two groups emerge from this analysis. On the one hand, those who believe that private markets will determine an efficient balance of the social good of privacy, private economic growth, and welfare will have a hands-off, wait-and-see approach to regulation or other governmental intervention. On the other hand, those who foresee an as-yet-undemonstrated market failure demand immediate preventive government intervention.

V. Privacy Risks: Probable Loss Versus Possible Loss

RFID technology is new and its applications now and into the future are uncertain. Originally intended as a tool to reduce private sector losses in global supply chains and to improve security through "smart" identification cards, RFID no doubt will find new, innovative uses that have unintended consequences of both its planned and unplanned use. All new technologies have this fate and RFID is no different.

14. Eden, *supra* note 12 at 21.

Although the privacy literature is clear that there is no absolute right to privacy, an expectation of privacy is a social good that makes us all better off. A measure of privacy protects civil society; a bit more protects individuals from identity theft or misuse of information.

Government specifically protects the privacy of certain personal information such as health records through HIPAA[15] and financial information through the privacy provisions of the 1999 Gramm-Leach-Bliley Act.[16] Expectations of privacy exist in attorney-client privilege, and privately contracted confidentiality clauses are enforceable to enable commerce. *The question is not whether we should have privacy, but rather how much and under what circumstances.* Risks to privacy, as measured by the expected value of its loss, represent real social costs.

In analyzing privacy risks, the literature takes generally two approaches: (1) a probable approach to the loss of privacy and (2) a speculative, worst-case scenario, possible-loss approach. Although the probable-value approach is true risk management[17] in the economic and classical sense, the other, speculative approach is not. Policymakers reviewing the literature need to determine which discussion of risk is used and use the literature accordingly. This section describes the two approaches and gives an example to help out.

A. Probable privacy loss

Brito discusses likely RFID technology capability, especially at price levels that would enable pervasive use, concluding that in the private sector retailers already track consumer purchases, with consent through loyalty programs and otherwise, and attempts to track individuals' movements and locations through movement of their purchased goods is unreliable.[18]

---

15. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936.
16. Gramm-Leach-Bliley Financial Services Modernization Act of 1999, Pub. L. No. 106-102, 113 Stat. 1339.
17. *See* Open Group Risk Taxonomy Standard, Open Group document C081, 18-19 *available at* www.opengroup.org/bookstore/catalog/c081.htm (discussing the components of information risk).
18. *See* Brito, *supra* note 7 at 18, 21–23.

Although the private sector possibly could invade consumer privacy with RFID technology, Brito argues that the profit motive checks and incentives make invasion unlikely.[19] The probable privacy loss in his analysis is far less than the possible loss discussed in other literature.

Ulatowski looks at privacy as a continuum, not as an absolute, and forms estimates of privacy risks within a cost-benefit framework and an evaluation of the likely threats. Ulatowski concludes:

> With RFID technology, "[t]he cost of the sacrifice of privacy is hard to quantify while the touted benefits seem hard for many people to overvalue." Maybe the government and private industry are right to tout the exceptional benefits to efficiency, privacy and security. Perhaps the threat to personal privacy is not as great as some privacy advocates fear. The most significant limitation to RFIDs' tracking capabilities is that the power level of the chip must be quite low so as not to interfere with other devices using radio frequency.
>
> One real privacy threat comes not from RFID devices themselves, but from hackers. In fact, hacking seems to be getting easier by the day. Plus, mobile phone vendors are looking into developing portable RFID readers coupled with cellular phones, making "RFID technology a user-driven activity in addition to one controlled by companies." If any teenage hacker with a cell phone can access personal information held on an RFID, it makes for quite an alarming proposition.[20]

B. Possible privacy loss

Eden, J. Smith, and Stein speculate on possible outcomes that are unproven and ignore the likelihood or probability of the event.[21] Eden's abstract puts it succinctly:

---

19. *See* Brito, *supra* note 7 at 37.
20. Ulatowski, *supra* note 7 at 647–48 (footnotes omitted).
21. *See* Eden, *supra* note 12 at 11–14; Jennifer E. Smith, Recent Development: *You Can Run, but You Can't Hide: Protecting Privacy from Radio Frequency Identification Technology*, 8 N.C. J. L. & Tech. 249, 262-265 (2007); Stein, *supra* note 13 at 6–7.

> RFID is a powerful new technology that has the potential to allow commercial retailers to undermine individual control over private information. . . . Although some potential privacy abuses could be addressed by modifying RFID technology, this iBrief argues that it would be wise to amend the Privacy Act of 1974 so that corporations would have a statutory obligation to preserve individual anonymity and respect the privacy preferences of consumers.[22]

In addition, Stein concludes that "[i]n the absence of enforceable regulations, society risks being subjected to an unprecedented level of Orwellian surveillance"[23] and J. Smith foresees that "[w]ithout regulation, RFID will be used to track both products and people."[24]

Because they're uncertain, technology's capabilities are often exaggerated, especially with respect to features not yet available at a mass consumption prices—or expected to be available in those price ranges in the near future. Speculative privacy loss not only depends on a general market failure theory, where consumers involuntarily hand over access to personal information, but also upon a widely deployed and available technical infrastructure to gather, process, transform, and exploit that information. These assumptions of market failure and an enabling and cost-effective ubiquitous infrastructure are common to analyses recommending preemptive governmental intervention to prevent unspecified yet dire outcomes. Politicians have amplified this approach: "[T]he RFID train is beginning to leave the station, and now is the right time to begin a national discussion about where, if at all, any lines will be drawn to protect privacy rights."[25]

Policymakers motivated by the public interest should evaluate carefully what social risks they are attempting to manage, the likelihood of the benefits

---

22. Eden, *supra* note 12 at 1.
23. Stein, *supra* note 13 at 3.
24. Smith, *supra* note 21 at 250.
25. Katherine Albrecht and Liz McIntyre, *RFID: The Big Brother Bar Code, 6* ALEC POL'Y FORUM *49 (*Winter 2004) (quoting Senator Patrick Leahy at the panel discussion on Video Surveillance: Legal and Technological Challenges at Georgetown University Law Center (Mar. 23, 2004)), *available at* http://www.spychips.com/alec-big-brother-barcode-article.html (last visited Oct. 8, 2012).

exceeding the cost of managing those risks, and the residual risk remaining in considering any law or regulation. When using the literature on RFID, including the essays in this ABA collection, policymakers should internalize the authors' perspectives on privacy, distinguish between likely and speculative risks, and assess the cost effectiveness of any proposed rule, regulation, or other policy intervention. In other words, the policymaker's perspective on privacy is key: is privacy an absolute, all-or-nothing proposition, or is it a continuum to be traded off against other competing social objectives?

VI. Alternatives to Law and Regulation

Although the vast majority of the literature concentrates on RFID technology, the probable and possible outcomes of its use, and the recommendations for its regulation, a minority strand presents alternatives to law and regulation to achieve the desired social outcome. In particular, Ronzani, citing the work of Larry Lessig as a backdrop and Lessig's four "modalities" of law, social norms, markets, and technical architecture, stresses the need to look beyond law to constrain behavior.[26] Social norms include not only unwritten rules within a community to govern or moderate behavior, but also voluntarily agreed to and enforceable codes of practice and standards of business conduct developed through private business associations. Markets, as already discussed in the literature, moderate behavior through voluntary exchange and prices, but the role of technical architecture—that is, technical features that constrain behavior or capability such as privacy-enhancing technology—is generally new to the discussion of RFID social policy. Ronzani discusses the problem as:

> The problem is that from a holistic perspective, we risk over-regulating with law if we do not consider the trade-off between the four modalities. As noted earlier, the claim in this paper is that if norms, market and architecture are considered, this will result in less need for laws.

26. Daniel Ronzani, *Modality Mix of RFID Regulation*, 3 J. Int'l Com. L. & Tech. 222 (2008) (referencing Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach, 113* Harv. L. Rev. 501 (1999)).

> This trade-off is possible and affordable because the technology-independent legislation enacted at [sic] European level is already sufficient to protect the stakeholders (with some limitations).[27]

Today, changes in law are the dominant solutions to the privacy "problem," incrementally favoring either the consumer or business, but not both. In the context of rapidly changing technology, law's inflexibility has the side effect of eliminating opportunity before it can ever have a chance of developing. Mechanisms and tools outside of law give policymakers options that are less politically polarizing and more flexible to adapt to changing views of the privacy problem as it emerges, enabling innovation and economic growth. The lowest-cost RFID technology, such as that designed for tracing things in the supply chain, much less the technology that tracks people through identification and authorization cards, are both still too expensive for ubiquitous deployment needed to create an "Orwellian" surveillance society. Ronzani argues that markets, norms, and the architecture itself will flexibly and affordably evolve to address privacy concerns while giving the innovators a chance to use the technology to its highest social value.[28]

VII. Missing from the Literature: Economics of Government's Impact on Contactless Data Exchange Technology and Privacy

As Brito points out: "We should be more concerned by government use of RFID— something to which privacy advocates have paid little attention."[29] Although privacy advocates may have paid little attention to government use, some conclusions nevertheless can be drawn from available information.

Governmental executive branches have many of the same functions and incentives as the private industry. The same benefits that contactless data exchange technology brings to the private sector also can improve operations

27. *Id.* at 223.
28. *Id.* at 222–223 and 230–231.
29. *See* Brito, *supra* note 7 at 5.

of the public sector,[30] and in many cases, governmental organizations innovate and lead the private sector in adopting new technology. RFID began as a government initiative. Both Axis and Allied forces are widely credited as being the first to use RFID technology in an application to identify allied aircraft during World War II.[31] Today the U.S. government embeds RFID chips into passports as well as RFID chips in its supply chains.[32] Government has been and will continue to be a heavy user of this technology, just like the private sector. The incentives and economics of that use should be similar, too.

Being such large users and—in many cases—early adopters, governments often develop or sponsor the initial technology and knowledge base. As very large users of the technology for public purposes, governments develop polices and standards for its use. For example, the U.S. government through its National Institute of Standards and Technology (NIST) has published NIST SP-800–98 "Guidelines for Securing Radio Frequency Identification (RFID) Systems," and this standard is available for public and private sector use.[33] Government, in functioning like an enterprise and research arm, can help develop for itself the best practices in the use of the technology that the rest of the world can reuse.

Just as its incentives for developing and using the technology are similar to those motivating private sector actors, the government's incentives to collect, aggregate, repurpose, and reuse information are similar to the private sector's as well. When government does not internalize all costs, including the social costs of privacy-eroding use, then the government's use is economically inefficient, reducing overall welfare, in the same manner as private sector overuse. The government, however, has powers and privileges beyond those of the private sector, and when government stands

30. For additional discussion of this phenomenon, see Roland Trope's essay "Maddening to Militaries and Museums" in Chapter 17 of this book, *infra.*

31. Rfid Journal, *The History of RFID Technology* 1, *available at* http://www.rfidjournal.com/article/articleview/1338/1/129/ (last visited Oct. 5, 2012).

32. For more discussion of this application, see chapters by Stephen Middlebrook and Roland Trope, *infra*.

33. National Institute of Standards Technology, Guidelines for Securing Radio Frequency Identification (RFID) Systems (2007), *available at* http://csrc.nist.gov/publications/nistpubs/800-98/SP800-98_RFID-2007.pdf (last visited Oct. 2, 2012).

sufficiently to benefit, history has shown it will use its powers and privileges. The consequences of using those powers and privileges sometimes distort incentives even further than the private sector can do on its own. Given how little research has been conducted in the analysis of government use of contactless data exchange and RFID, this is an area ready for more research.

VIII. Conclusion and Next Steps

Like any change in law and regulation, RFID law and regulation will transfer wealth, creating winners and losers. Although little in the literature quantifies the wealth at risk, policymakers, using economic theory, can anticipate and predict general flows of wealth implied by proposals in the RFID law literature, based on its assumptions about markets and the kind of risk analysis and assessment made.

This survey of private-sector use of RFID and its resulting risks to privacy expectations reveals that part of the literature foresees well-functioning markets moderating private-sector privacy abuses, estimates privacy loss based on a likely or probable loss scenario, and recommends a reactive legal intervention policy to address actual discovered problems. Another part of the literature foresees market failure, estimates speculative, worst-case scenario privacy losses, and recommends a preemptive legal intervention policy to prevent possible dire outcomes.

		Privacy Loss Risk Approach	
		Probable	Possible
Market Belief	Market Forces Dominate	•	
	Market Failure Dominates		•

Market assumptions and the approach to risk management will determine policy outcomes. Policymakers should consciously evaluate their economic belief about the market and their approach toward risk management before taking a position on RFID technology policy. Both under-regulating and over-regulating have net social deadweight economic losses, including

losses from economic opportunities preemptively and prematurely made illegal. Economic analysis shows that use and reuse of information generally improves total welfare, but external costs to the data subject can change that general conclusion.

Policymakers concerned about privacy erosion arising from the private sector use and overuse of new technology, including RFID, need a comprehensive framework for analyzing this class of problem and the implications of proposed solutions. This literature survey demonstrates that analyzing market assumptions and approaches to risk management are necessary, but they are hardly sufficient. The social costs and benefits of government's use of the technology is an opportunity for more research, and economic considerations that apply to policy generally but not specifically to contactless data exchange have not been addressed here.

The next step in this analysis would be to derive a framework that includes all other necessary and sufficient dimensions. Although such an undertaking is ambitious, it could be accomplished through a collaborative, multidisciplinary approach that includes legal, technical, and economic contributors. Such a framework would look at the constraints and incentives imposed by all modalities regulating actors' behavior, their immediate and foreseeable future consequences on wealth generation and distribution, and their external social side effects. The social impact of government's use of both public sector and private sector collected information could be analyzed, including the likelihood of policy effectiveness and lost opportunities of diverting regulatory resources to this technology to other uses of those resources. Whether regulating RFID use at all improves social welfare remains an open question.