Choice or Consequences: Protecting Privacy in Commercial Information

J. Howard Beales, III† *& Timothy J. Muris*††

INTRODUCTION

We are frequently asked how, during our recent tenure at the Federal Trade Commission, we came to create the National Do Not Call Registry, one of the most popular government actions ever undertaken. The answer lies in our search for an approach to regulate the exchange of consumer information in commercial transactions. Information exchange is the currency of the modern economy. The growth of the internet, and the resulting new possibilities for collecting, storing, and exchanging information, have sparked a renewed interest in privacy and the ability of consumers to control the use of information about them.

We argue that information exchange is valuable and that regulators should be cautious about restricting it. The traditional approach to privacy regulation, based on the so-called fair information practices (FIPs), is inadequate. Instead, we argue, government should base commercial privacy regulations and policies on the potential consequences for consumers of information use and misuse. This approach focuses attention on the relevant questions of benefits and costs, and offers a superior foundation for regulation. It was this approach that suggested there would be large consumer benefits from Do Not Call. Finally, we apply this approach to privacy to the growing problem of breaches of information security. Companies with sensitive information about consumers that, in the wrong hands, could harm consumers should be expected to protect that information in ways that are reasonable and appropriate given the sensitivity of the information.

I. THE VALUE OF INFORMATION EXCHANGE

A multi-billion dollar industry with dozens of firms compiles and resells information.[1] These companies collect and collate different

---

† Associate Professor, Strategic Management and Public Policy, George Washington University. Director, Bureau of Consumer Protection, FTC, 2001–2004.

†† Foundation Professor, George Mason University School of Law. Chairman, FTC, 2001–2004.

1 A wide variety of information products exist, offering substantial benefits. These products include tools to reduce the risk of fraud, facilitate credit-granting decisions, and locate indi-

items of information about an individual from various sources and resell it. The revenues of the risk management sector of the business are about $5 billion,[2] and the market for pre-employment background screening services is approximately $2 billion.[3]

The heart of building a database is a matching algorithm.[4] Systems must distinguish consumers with very similar identifying information, and recognize an individual wbose identifying information changes significantly, such as those who have moved or changed their names after marriage or divorce. The systems must accommodate records that may be missing parts of the identifying information, and they must recognize that any individual piece of incoming information may be a mistake.[5] Consequently, no one piece of identifying information is used to perform the match. Rather, matching is done based on multiple data points using an algorithm that tests the extent to which the various elements contain data that are consistent for that individual.

Matching systems confront an inherent tradeoff between inclusion (associating probable matches) and exclusion (keeping records separate when an exact match does not exist). Insisting on a more exact match reduces the chances that an incoming record will be associated mistakenly with the wrong individual. But it increases the chances that the information about an individual will be incomplete because some valid information cannot be matched to the individual with absolute certainty.[6] Either potential error can create costs for both users of the data and the consumers who are the subject of the information. Absent a unique, error-free, and universally available

---

viduals. Information tools also offer easier access to public records, thus helping to monitor official conduct, protect our most vulnerable citizens from criminals and sexual predators, monitor land use and development, and determine whether licensed professionals are who they claim to be.

2 According to LexisNexis, the risk management sector includes identity authentication, fraud prevention, and credit and security risk products. Reed Elsevier, *Reed Elsevier Announces the Acquisition of Seisint, Inc. for $775 Million* (July 14, 2004), online at http://www.reed-elsevier.com/index.cfm?Articleid=965 (visited Jan 12, 2008).

3 KPMG Corporate Finance, Background Screening *1 (Fall 2003), online at http://web.archive.org/web/20060706171129/http://www.kpmgcorporatefinance.com/us/pdf/bkgd_screen.pdf (visited Jan 12, 2008).

4 The data-matching process used in credit reporting is discussed in detail in FTC, *Report to Congress under Sections 318 and 319 of the Fair and Accurate Credit Transactions Act of 2003* 36–46 (2004), online at http://www.ftc.gov/reports/facta/041209factarpt.pdf (visited Jan 12, 2008).

5 Studies of unemployment insurance records, for example, suggest that the error rates in entering social security numbers range from 0.5 to 4 percent. Id at 39. Unlike credit card numbers, social security numbers do not include a "checksum" digit, which can be derived mathematically from the other digits in the number. Thus, a computer can check to ensure the credit card number is internally consistent, which substantially reduces the chances of undetected typographical errors.

6 The consequences of either incompleteness or inaccuracy depend on the particular item of information involved. Either type of error about a recent bankruptcy filing, for example, is more serious than if the information is about a recent account that was paid on time.

identifier, however, the tradeoff is unavoidable. An important element of competition among information providers is their systems' ability to provide the most complete, precise, and accurate data possible to their customers.

Information is compiled from both public and private sources. Public records include those for property ownership, marriage, divorce, birth, death, change of address, occupational licenses, and UCC and SEC filings. Other information, such as from telephone books, professional registries, and the like is also available. There is also an active commerce in nonpublic information, especially contact information such as names and addresses revealed in business transactions. Companies also compile information concerning products purchased, magazine subscriptions, travel records, types of accounts, fraudulent transactions, and payment history.[7]

Once compiled, information is used for many purposes.[8] Information intermediaries help locate individuals, providing information about their last known address, prior addresses, places of employment, and the like. For background checks, the intermediaries also facilitate searches of public records, revealing liens, bankruptcies, personal assets, and even criminal records.

Information products also reduce the risk of fraud in account applications or in remote transactions such as online or telephone purchases. Approaches to fraud control can be as simple as checking an identity against a list of prior cases of fraud or determining whether an address is a campground rather than a personal residence. More sophisticated approaches check for consistency in the ways identifying information is used in various transactions, or use available information to estimate the probability that a proposed transaction is fraudulent. Other fraud control tools rely on pooled data to search for anomalous patterns across applications or over time, such as numerous applications with different names but a common home telephone number. Although the evidence is anecdotal, these tools appear highly effective in reducing the incidence of fraud.[9]

---

[7] Identity Theft: Recent Developments Involving the Security of Sensitive Consumer Information, hearing before the Senate Committee on Banking, Housing, and Urban Affairs, 4 (Mar 10, 2005) (statement of the FTC), online at http://ftc.gov/os/testimony/050310idtheft.pdf (visited Jan 12, 2008).

[8] Many uses of information are restricted under various federal statutes. Under § 604 of the Fair Credit Reporting Act (FCRA), Pub L No 91-508, 84 Stat 1128, codified in relevant part at 15 USCA § 1681b (2007), for example, information that constitutes a "consumer report" can be used only for a narrowly drawn list of permissible purposes.

[9] A major national credit card issuer with approximately forty-five million accounts, growing by about ten thousand accounts a day, realized a 13 percent decrease in application fraud losses and annual savings of $18 million by implementing a basic identity authentication tool.

Of course, the accumulated information about consumers is used for marketing, perhaps the most controversial use of commercial data. Like the other uses of commercial data, marketing has real social value, enabling companies to offer consumers choices that better satisfy their preferences. Unlike the other uses, however, it directly involves the consumer, who must process a torrent of junk mail, both electronic and physical, and deal with unwanted calls from telemarketers.

It is not obvious, however, that better information about consumer behavior increases the amount of marketing. It clearly leads to more targeted marketing—there is a higher probability that the consumer will find the message relevant if information about past behavior helps to predict preferences. If targeting were perfect, consumers would receive only offers that were actually of interest. Imperfect, but better, targeting would increase the fraction of offers that the consumer finds interesting. By eliminating offers of no interest, it would tend to reduce the amount of marketing received.[10] Indeed, much of the annoyance of spam stems from that fact that, because it is so cheap to send, there is very little targeting.[11] Regardless of past behavior, virtually every consumer with an email account has likely received offers to enlarge or contract various body parts, as well as offers to assist in smuggling large sums of money out of a foreign country.

II. APPROACHES TO PRIVACY REGULATION

Since their origination in 1973,[12] the FIPs have been highly influential in privacy debates. The heart of FIPs is to require notice and choice. That is, consumers should receive notice of the information that is collected about them, and they should have a choice about how that information is used, particularly with respect to secondary uses.[13]

Similarly, a national wireless telecommunications provider reduced its fraud losses per handset by 55 percent and decreased the time it took to confirm fraud records by 66 percent. FTC, Panel on the Costs and Benefits of the Collection and Use of Consumer Information for Credit Transactions 11–12 (June 18, 2003) (testimony of Laura DeSoto, Senior Vice President, Credit Services, Experian).

10 Better targeting would reduce the marginal cost of acquiring a new customer, which would mean that sellers would seek to acquire more customers. This expansion in the amount of marketing would tend to increase the number of solicitations received. On the other hand, the increased productivity of marketing means that it takes fewer solicitations to generate a customer, which would reduce the number of solicitations received. Which factor would predominate is not obvious a priori.

11 See FTC, *Email Address Harvesting: How Spammers Reap What You Sow* 1 (Nov 2002), online at http://library.findlaw.com/2003/Aug/8/132973.pdf (visited Jan 12, 2008).

12 Report of the Secretary's Advisory Committee on Automated Personal Data Systems, US Department of Health, Education, and Welfare, *Records, Computers, and the Rights of Citizens* (1973), online at http://www.epic.org/privacy/hew1973report (visited Jan 12, 2008).

13 Other FIPs include access and correction (the notion that consumers should be able to examine and correct information about them). In some contexts (like credit reporting), these

In the context in which they were originally developed—assessing the privacy implications of government agencies matching data about a consumer derived from various sources—these principles are potentially quite useful. If consumers knew that data given to one agency would be matched to data from another agency and they had a choice about whether to provide the data or allow the match, then it is very difficult to see how a privacy problem could exist.

The converse, however, does not follow. That is, the absence of a privacy problem when consumers understand and have a choice about the information collection or use does not imply that a privacy problem exists whenever consumers are ignorant of the information use or lack a choice about it. No reasonable person would think that a privacy problem exists when information is shared with numerous parties to clear a check in settlement of a transaction or to conclude a transaction at an ATM. Yet, most consumers are unaware that such information sharing even exists, let alone have knowledge of which specific parties might receive the information, and consumers have given no consent beyond the fact that they initiated the transaction.[14] Indeed, attempting to apply FIPs to real-world privacy issues creates significant quandaries, as we discuss next.

A. The Irrelevance of FIPs

Both of the foundational principles of FIPs—notice and choice—are highly appealing in theory. In the abstract, who can oppose them? FIPs pose insuperable difficulties in practice, however. Most fundamentally, FIPs neglect the very real costs of processing information and making a decision. Everyone who has received a financial privacy notice (and has actually perused it) is aware that the notices are often long, complex, and filled with legal jargon. Few consumers actually take the time to read them, understand them, and make a conscious choice about whether to opt out of information sharing that is not a matter of statutory right for the financial institution.[15]

---

approaches are helpful, but in others they can create problems. Consider, for example, a database of identities that have been used to commit frauds. The only person with a real interest in examining and correcting such a database is the thief who used that identity once and would like to use it again. Similarly, the fact that one person's name has at some point been used with another person's social security number looks like an error to each of them, but knowing that fact helps creditors reduce the risk of fraudulent applications, thereby protecting both. FIPs also require that information holders protect the information, a notion that we explore at some length below.

[14] The most that even diligent readers of financial privacy disclosures might learn is that information "may" be shared to process a transaction. Plainly, such an incantation does not cure any privacy problem that would otherwise exist.

[15] See Susan E. Henrichsen, *What Privacy Notice?*, Presentation at Interagency Public Workshop on Financial Privacy Notices, slide 3 (Office of the Attorney General, California, Dec 4, 2001) (reporting that according to a May 2001 American Bankers Association survey, 41 per-

Judging by behavior in the marketplace, most consumers have better things to do with their time than read privacy notices. The point is not that transaction costs are particularly high, because it does not take long to process a privacy notice. Rather, processing privacy notices is a cost that most consumers apparently do not believe is worth incurring. The perceived benefits are simply too low. Simpler notices are always possible, but any notice that provides meaningful information about the actual uses of information in the modern economy will necessarily impose costs on consumers who must read and process the information.[16]

The reality that decisions about information sharing are not worth thinking about for the vast majority of consumers contradicts the fundamental premise of the notice approach to privacy. To be an effective approach, some significant number of consumers must not only read privacy notices for the businesses with whom they currently deal, they must also consider the privacy practices of alternative service providers and choose the provider whose practices best match their privacy preferences. There is no reason to think this is currently happening, or will ever happen.

The FIPs principle of choice fares no better. For consumers, the costs of exercising choice regarding information sharing involve more than the small investment of time to read the notice and implement the choice. To exercise choice, a consumer first must *decide* to do so. Because consumers literally have (at least) hundreds of ways that they can use their time, to care about choices regarding their information they must overcome both the costs of decisionmaking and the opportunity cost of not using their time elsewhere.[17] The costs involved in deciding to choose may pose a more fundamental barrier to FIPs than the mere time costs involved.

The tendency of consumers to avoid decisionmaking costs by avoiding a choice has been observed in a number of different contexts and given rise to debate about the proper choice of default rules. For example, Austria, Belgium, France, Hungary, Poland, Portugal, and Sweden have presumed consent (opt out) as the default rule for organ

---

cent of consumers did not recall receiving the notice, 22 percent had received but not read the notice, and 36 percent had read the notice).

[16] The situation is no different with respect to internet privacy notices. Although the vast majority of websites have privacy policies, there is little evidence that consumers actually click on them, let alone read them. In a survey by the Privacy Leadership Initiative, a group of corporate and trade association executives, only 3 percent of consumers read websites' privacy policies carefully, and 64 percent only glanced at—or never read—websites' privacy policies. Privacy Leadership Initiative (PLI), *Privacy Notices Research: Final Results* (Dec 2001), online at https://www.bbbonline.org/UnderstandingPrivacy/library/datasum.pdf (visited Jan 12, 2008).

[17] In many contexts, consumers can use the market to substitute money for time, hiring an agent to perform a task that would otherwise require their own time. It is difficult to imagine a practical market substitute for reading privacy notices and exercising choice, however.

donation, whereas Denmark, the Netherlands, the UK, and Germany have explicit consent (opt in) as the default.[18] Across European countries, the opt-out countries have drastically higher proportions of the population in the potential organ donor pool: a difference of at least 60 percentage points. Richard Posner has attributed the stickiness of default rules in the organ donation context to the cost of decisionmaking:

> One possible reason the weak default rule appears to have a significant effect is public ignorance. The probability that one's organs will be harvested for use in transplantation must be very slight—so slight that it doesn't pay to think much about whether one wants to participate in such a program. When the consequences of making a "correct" decision are slight, ignorance is rational, and therefore one expects default rules to have their greatest effect on behavior when people are ignorant of the rule and therefore do not try to take advantage of the opportunity to opt out of it.[19]

Thus, consumers rationally avoid investing in information necessary to make certain decisions, such as donating organs, when their decision is very unlikely to have a significant impact on them. The same is true with respect to privacy. Consumers also maintain rational ignorance about how much and what kind of information sharing occurs. It simply does not pay for most consumers to think and make decisions about policies on the use of their information, given that the issue is of such little consequence practically to them.[20]

In our economy, there are vital uses of information sharing that depend on the fact that consumers cannot choose whether to participate. One such example is credit reporting. Unlike many other countries, credit reporting in the US is "full file" or "comprehensive" reporting, including both positive and negative information about consumers.[21]

---

18 See Eric Johnson and Daniel Goldstein, *Do Defaults Save Lives?*, Science 1338, 1339 (Nov 21, 2003). Under the European Union's Privacy Directive, all EU members have an opt-in default rule for information sharing. Consumers are presumed willing to share their organs, but not their information.

19 Richard Posner, *Organ Sales—Posner's Comment*, The Becker-Posner Blog (Jan 1, 2006), online at http://www.becker-posner-blog.com/archives/2006/01/organ_salesposn.html (visited Jan 12, 2008).

20 Of course, some consumers care intensely about privacy issues and are willing to bear the decisionmaking costs of processing and deciding about privacy notices. Default rules should be designed to impose those costs on consumers who think they are worth paying. An opt-out default rule means that consumers who do not think that decisionmaking costs are worthwhile do not need to bear those costs. Consumers who care intensely, however, will face the costs of making a decision. In contrast, an opt-in default rule frees those who care the most about the issue to avoid the decision costs, because the default will accord with their preferences.

21 See generally John M. Barron and Michael Staten, *The Value of Comprehensive Credit Reports: Lessons from the U.S. Experience* (2000), online at http://privacyalliance.org/resources/

The expansion of credit reporting, along with improvements in credit scoring, has facilitated substantial expansion in the availability of credit to American consumers,[22] as well as the democratization of credit.[23] Credit grantors can make more expeditious decisions, often without a personal visit to a loan officer, enabling the phenomenon of "instant credit" and offering significant benefits to consumers as a group.

Comprehensive credit reporting, however, depends on the absence of consumer choice. Creditors report, on a voluntary basis, consumers' payment histories. If consumers could choose not to have some of their information reported,[24] the credit reporting system likely would experience significant adverse selection—consumers with poor payment histories would choose not to have that information reported.[25] Such information loss, however, would significantly compro-

---

staten.pdf (visited Jan 12, 2008) (discussing the benefits of the US system of comprehensive credit reporting, and offering the US system as a model for credit reporting systems in other countries that currently do not fully realize the benefits of comprehensive credit reporting due to varying limitations from country to country on lenders' access to personal credit history for the purpose of assessing risk).

22 In 1970, when the Fair Credit Reporting Act was enacted, outstanding consumer credit in constant dollars was $556 billion. Fair Credit Reporting Act, hearing before the House Committee on Financial Services (July 9, 2003) (statement of the FTC), online at http://www.ftc.gov/os/2003/07/fcratest.html (visited Jan 12, 2008). In 2002, it was $7 trillion. Fred H. Cate, et al, *Financial Privacy, Consumer Prosperity, and the Public Good: Maintaining the Balance* ii (AEI-Brookings Joint Center for Regulatory Studies, Mar 2003).

23 The percentage of families in the lowest income quintile with a credit card has increased from 2 percent in 1970 to 38 percent in 2001. The Information Policy Institute, *The Fair Credit Reporting Act: Access, Efficiency & Opportunity—The Economic Importance of Fair Credit Reauthorization* ("IPI Report") 5 (June 2003).

24 Recently, some states have enacted so-called "freeze" laws, allowing consumers to block access to their credit reports. Generally, these statutes include exceptions that effectively limit their applicability to when the consumer is applying for a new account. Freezes, for example, do not block access to credit reports for purposes of risk management or pricing a note or obligation in a transaction. Moreover, various hurdles have made requesting a freeze difficult, and only about 50,000 consumers have so requested. See Brian Krebs, *States Offer Consumers New Tool to Thwart Identity Theft: Consumers Largely Unaware of Credit Freeze*, washingtonpost.com (May 9, 2007), online at http://www.washingtonpost.com/wp-dyn/content/article/2007/05/09/AR2007050900427.html (visited Jan 12, 2008). More importantly for our argument, they do not allow consumers choice about what information is included in their credit file.

25 Although creditors could demand access to a credit report as a condition of granting credit, they could no longer distinguish between the consumer who has no report because he has no prior experience with credit and the very different consumer who has a bad credit history but has blocked reporting of any information. Both consumers would have no file. Or, a deadbeat with choice might maintain one account in good standing and repeatedly open and default on other accounts without allowing reporting. The result would have elements of a "lemons" market. See George A. Akerloff, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, 84 Q J Econ 488, 490–92 (1970) (demonstrating that asymmetrical information can lead to market conditions wherein poor-quality products drive out high-quality products). Choice would undermine the mechanism that allows lenders to differentiate consumers based on risk. A likely response of lenders would be to rely more heavily on their own experience with a consumer, thus tying consumers more tightly to a particular lender and reducing willingness to lend to strangers.

mise the value of the system, leading to some combination of increased defaults and reduced credit availability.[26]

Property recordation is another example in which giving consumers choice regarding use of their information in the system would seriously undermine an important institution. Although the recording acts governing property recordation vary from state to state, they share two separate, but interdependent, purposes. The first is to protect purchasers who acquire interests in real property. The second purpose, critical to achievement of the first, is enabling prospective purchasers—and lenders—to determine the existence of prior claims that might affect their interests. Thus, claims against property are a matter of public record, accessible to all.[27] If consumers could exclude liens against their property, or if they could limit access to the records, these important purposes would be thwarted.

We could, of course, narrow the range of places in which consumers are allowed choice to avoid the difficulties discussed above. But, if we accept FIPs as the basis for privacy regulation, there is no principled basis for limiting choice consistent with FIPs. A privacy regime that gives consumers a choice—except when it doesn't—is not a basis for a sound legal approach at all.

The core difficulty with the FIPs approach to privacy is its attempt to approach privacy as a question of property. Information about a consumer is seen as "belonging" to the consumer, who therefore is entitled to control how and where that information is disseminated. In fact, however, the consumer and the other party to a transaction generally jointly produce commercial information. There is no obvious way to assign property rights, particularly exclusive property rights, to either party. In a real estate transaction, for example, or an auction on eBay, both the buyer and seller know all of the pertinent details of the transaction and may benefit from using that information for a variety of other purposes. Which party should be given control? US law does not treat commercial information in the possession of sellers as something over which consumers can exercise exclusive control—it is not the consumer's property.[28]

---

26 See generally *IPI Report* (cited in note 23) (analyzing the many benefits of comprehensive credit reporting).

27 Richard R. Powell and Michael Allan Wolf, ed, 14 *Powell on Real Property* § 82.01[3] at 82-12 (Matthew Bender 2007).

28 See *Dwyer v American Express Co*, 652 NE2d 1351, 1354 (Ill App 1995) (dismissing the plaintiff consumer's challenge to American Express's practice of renting lists compiled from information contained in its own records, because by using the American Express card, the consumer voluntarily gave the information to American Express, which simply compiled and analyzed that information); *Shibley v Time, Inc*, 341 NE2d 337, 339–40 (Ohio App 1975) (upholding the defendant's practice of selling subscription lists to direct mail advertisers when subscribers'

Of course, under the Coase theorem, allocation of a property right to information would not matter in a world of zero transaction costs. As our discussion of notice makes clear, however, the transaction costs of even considering uses of personal information appear to loom large relative to the benefits, let alone the costs of negotiating to rearrange rights. Because transaction costs will essentially preclude transactions, we need to know the efficient use of the information before we can assign property rights. Yet, the attraction of the FIPs approach to privacy is that, at first blush, it seems to avoid precisely that question. Unfortunately, it does not.

B. Privacy Regulation Based on Consequences

Given these limitations of FIPs, a different approach to privacy in the commercial sphere is necessary. We believe the focus should be on the consequences of information use and misuse. There is little basis for concern among most consumers or policymakers about information sharing per se. There is legitimate concern, however, that some recipient of the information will use it to create adverse consequences for the consumer. Those consequences may involve physical harm, as when stalkers obtain information about their victims or child predators seek information online. They may be economic consequences, as when one's identity is stolen or when credit or insurance is denied based on incomplete or inaccurate information. Or there may be unwanted intrusions, such as the telemarketing call that disrupts the dinner hour or the spam that clogs our inboxes.

Focusing on consequences calls attention to the relevant issues immediately—what is the impact of a particular information use on consumers? This approach also conforms to the way that most consumers think about privacy issues. Although concerned about privacy, the majority of consumers are privacy pragmatists,[29] willing to provide information in exchange for specific benefits. When the impact is

---

profiles were used only to determine what type of advertisement was to be sent). Moreover, consumers' preferences regarding a seller's use of transaction information for other purposes may differ. See *Shibley v Time, Inc*, 321 NE2d 791, 797 (Ohio Ct Com Pl 1974) (noting that large portions of the class may have preferred receiving the unsolicited mail and supported the sale of mailing lists).

[29] According to the March 2003 Westin/Harris Interactive poll, 64 percent of adults polled are "privacy pragmatists" who are often willing to permit the use of their personal information if they are given a rationale and tangible benefits for such use and if they sense that safeguards are in place to prevent the misuse of their information. See Humphrey Taylor, *Most People Are "Privacy Pragmatists" Who, While Concerned about Privacy, Will Sometimes Trade It Off for Other Benefits*, The Harris Poll No 17 (Mar 19, 2003), online at http://www.harrisinteractive.com/harris_poll/index.asp?PID=365 (visited Jan 12, 2008). In a notice and choice system, however, most of these consumers are unlikely to take the time and effort in individual transactions to understand the benefits and costs of a specific sharing of information.

clearly positive, as when information sharing facilitates the completion of an ATM transaction that the consumer wishes to engage in, there is no reason to think that a privacy problem exists. Similarly, when information sharing is used to reduce the risk of fraudulent transactions, consumers benefit, and it is difficult to see why the government should be concerned about the privacy interests of those who wish to engage in anonymous fraud.

The consequences-based approach to privacy led directly to the Do Not Call Registry. It was clear that many consumers considered telemarketing calls an unwarranted intrusion on their privacy. As in any economic analysis, the question of the significance of the intrusion is one that consumers are uniquely able to judge. For many consumers, the costs are clearly significant.[30] Others, however, do not object, and may find the offerings interesting. Moreover, telemarketing, like other forms of marketing, offers significant benefits to consumers as a whole. The question is how to balance these competing concerns in a workable regulatory policy.

FIPs offer no solution. The vast majority of consumers have chosen to have their phone number published, with the clear understanding and expectation that people who do not otherwise know their number will call them. Nor will FIPs protect consumers with unlisted or unpublished numbers from random digit dialing. No information about the consumer is used in any meaningful sense to complete the call. The privacy problem arises not because information was shared, with or without consumers' permission, but because the call itself interrupted their right to be let alone.

The Do Not Call Registry resolved this dilemma with the creation of an enforceable right for consumers to avoid most telemarketing calls if they find such calls annoying.[31] The transaction costs of exercising choice appear tiny relative to the perceived benefits; more

---

30 The rulemaking record contained thousands of comments from individual consumers, often with extremely colorful descriptions of the unwanted practices of telemarketers. See FTC, *Telemarketing Sales Rule, 16 C.F.R. Part 310*, online at http://www.ftc.gov/bcp/rulemaking/tsr/tsrrulemaking/index.shtm (visited Jan 12, 2008) (linking to public comments). For the final rule, see FTC, *Telemarketing Sales Rule*, 68 Fed Reg 4580 (2003) (amending 16 CFR Part 310).

31 See *Mainstream Marketing Services, Inc v FTC*, 358 F3d 1228, 1237–38 (10th Cir 2004) (upholding the constitutionality of the national Do Not Call Registry and its fees against a challenge by telemarketing companies and a trade association alleging that the Do Not Call Registry violated the challengers' First Amendment free speech rights). The court explained that

> [o]ne important aspect of residential privacy is protection of the unwilling listener .... [A] special benefit of the privacy all citizens enjoy within their own walls, which the State may legislate to protect, is an ability to avoid intrusions. Thus, we have repeatedly held that individuals are not required to welcome unwanted speech into their own homes and that the government may protect this freedom.

Id, quoting *Frisby v Schultz*, 487 US 474, 484–85 (1988).

than 140 million telephone numbers are currently included in the Registry. The right created, however, concerns the telephone call itself, not the information that led to the call to a particular individual.[32] The Do Not Call Registry is a far more efficient solution to the real privacy problem—the call, rather than the information sharing that led to the call.[33] Focusing on how to avoid the undesirable consequences of information use produces a better solution.

III. INFORMATION SECURITY

Willie Sutton robbed banks because that was where the money was.[34] In today's information economy, sensitive information is the target of thieves for the same reason. Compromised information, particularly social security numbers, can create identity theft. Indeed, for many consumers, concerns over privacy are primarily about keeping their information secure from theft. Thus, information security is a natural component of an approach to privacy based on the consequences of information use and misuse. We consider first the nature and extent of the identity theft problem, and then the approach that the FTC has developed to try to reduce data breaches.

A. Data Security and Identity Theft

1. Data breaches.

Since California's law requiring notice to consumers who were the victims of compromised information became effective in 2003, the number of reported breaches and compromised records has grown substantially. A public database of data loss incidents maintained by

---

32 Ayres and Funk have argued that do not call lists are an all or nothing choice and that a mechanism to allow consumers to name a price at which they would be willing to accept calls would be an improvement. Ian Ayres and Matthew Funk, *Marketing Privacy*, 20 Yale J Reg 77, 106 (2003) (noting that potential recipients of marketing calls might prefer options between the extremes of all calls or no calls). In fact, however, the rule allows consumers to authorize any seller to call them, even if they are listed on the Do Not Call Registry. Some sellers have offered, for example, contests or drawings that allow consumers the chance to win a prize in exchange for express written authorization for telemarketing calls from that seller. The rule also permits consumers to allow most calls but request that specific companies not call them.

33 Of course, the Do Not Call Registry gives consumers a choice about receiving telemarketing calls. This choice is very different from the choice that FIPs contemplates, however. The choice pertains to the calls, not the information. It need be exercised only once every five years, rather than every time information is provided. Moreover, a FIPs choice that permits information sharing is difficult to reverse once the information has been shared and the consequences are known. A Do Not Call choice is easy to change.

34 See Willie Sutton and Edward Linn, *Where the Money Was* 119–21 (Viking 1976) (defining the so-called "Sutton Principle" and admitting that Sutton actually never uttered the oft-quoted line).

Attrition.org[35] includes 11 in 2003, rising sharply to 346 in 2006, with 282 incidents in the first ten months of 2007.[36] The reported number of records compromised has increased as well, from 6.4 million in 2003 to more than 86.2 million in 2007.[37] The reliability and comprehensiveness of these reports is uncertain. Recent statistics are certainly more comprehensive than those for earlier years, both because the California law has increased publicity surrounding breaches and the resulting public interest has provoked more attention to the issue. Moreover, the breaches differ greatly in their severity, ranging from compromised records that include both medical information and social security numbers, to records involving only credit card numbers, to records with only name and address or email addresses.[38]

A recent report analyzes where breaches occur, finding that 39 percent involved the private sector, 35 percent the public sector, 16 percent higher education, and 9 percent medical centers. Theft was the most common cause of breaches. Thefts of laptop computers alone accounted for 30 percent of the incidents, with other thefts accounting for an additional 16 percent. "Human/software incompetence" caused 29 percent of the incidents and outside hackers caused 19 percent. Insider malfeasance caused the remaining 8 percent.[39] Higher education was the primary target of outside hackers (52 percent of the hacker incidents); the public sector accounted for most incidents due to incompetence (44 percent); and the private sector and medical centers each accounted for 40 percent of incidents of laptop computer thefts.[40]

Two variables heavily influence the potential consequences of a given security breach. First, the sensitivity of the data is critical. Breaches of information with only name and address pose virtually no consequences for consumers. The information is widely and publicly available, and the additional fact that the name and address were as-

---

35 See Attrition.org, *DLDOS: Data Loss Database—Open Source*, online at http://attrition.org/dataloss/dldos.html (visited Jan 12, 2008).

36 See Etoliated Consumer/Citizen, *Statistics*, online at http://www.etiolated.org/statistics (visited Jan 12, 2008).

37 Id. The data are based on when the incident was reported, rather than when the breaches occurred. The 2007 statistics, for example, include 45.7 million records compromised at TJ Maxx over a period that apparently began in July 2005. See Larry Greenmeier, *Dubious Distinction: 45 Million Credit and Debit Card Records May Have Been Compromised*, Info Week 21 (Apr 2, 2007), online at http://www.informationweek.com/showArticle.jhtml;jsessionid=1TLIM4U3NUK3GQSNDLRCKH0CJUNN2JVN?articleID=198701551 (visited Jan 12, 2008).

38 See Attrition.org, *Data Loss Database—Open Source Key*, online at http://attrition.org/dataloss/dldoskey.html (visited Jan 12, 2008).

39 Beth Rosenberg, *Chronology of Data Breaches 2006: Analysis* (Privacy Rights Clearinghouse, Feb 1, 2007), online at http://www.privacyrights.org/ar/DataBreaches2006-Analysis.htm (visited Jan 12, 2008). The numbers do not add to 100 percent due to rounding.

40 Id.

sociated with a particular institution is unlikely to be sensitive in general.[41] Probably the most sensitive type of widely held information is social security numbers, which are crucial for opening new accounts in someone else's name.[42] Somewhat less sensitive is credit card or other types of account numbers. They may allow compromise of one particular account, but, as discussed below, this form of identity theft is generally less serious.

The second variable determining the risk of adverse consequences is the nature of the breach itself. Some reported incidents are essentially accidental—information is compromised, but it is not necessarily stolen. For example, in 2005, tapes from Citibank containing information on 3.9 million accounts were lost in transit to a credit bureau.[43] Of publicly reported breaches between mid-February and September 2005, 16 percent were accidental. Other breaches are incidental, as with a stolen computer containing sensitive data. The thief may or may not use, or even discover, the data. Such breaches were another 16 percent of the 2005 total.

Finally, many breaches are intentional, as someone deliberately steals the data itself, accounting for 68 percent of the 2005 breaches.[44] Intuitively, the risk of misuse is higher when the breach is intentional, if only because there will be no misuse in at least some of the accidental or incidental breaches. A recent GAO report supports that intuition. Examining the twenty-four largest data breaches reported between January 2000 and June 2005, GAO found evidence of existing account fraud in three cases and new account fraud in one, all intentional breaches. In two other intentional breaches, there was not sufficient evidence to determine whether fraudulent use had occurred. Of the nine accidental or incidental breaches examined, there was no evidence of fraudulent use of the information.[45]

---

41 Information about an association may be sensitive in particular cases. For example, the fact that an individual had a customer relationship with a psychiatric hospital would be sensitive.

42 An analysis of seventy breaches publicly announced between February 15, 2005 and September 30, 2005 found that 77 percent were "identity-level" breaches that involved social security numbers. See ID Analytics, *National Data Breach Analysis* 10 table 3 (Jan 2006), summary online at http://www.idanalytics.com/assets/pdf/national-data-breach-analysis-overview.pdf (visited Jan 12, 2008).

43 Tom Zeller, Jr., *U.P.S. Loses a Shipment of Citigroup Client Data*, NY Times C1 (June 7, 2005).

44 ID Analytics, *National Data Breach Analysis* at 10 table 3 (cited in note 42). The distributions are similar for the number of consumers affected. A single large breach (the CardSystems breach) accounted for approximately 90 percent of the intentionally breached consumers. Excluding this breach, 11.4 percent of the compromised consumers were accidental breaches, and 54.3 percent were intentional. Eleven percent were incidental. Id.

45 A total of fourteen breaches were intentional, involving either hacking (eleven breaches), deceptions to obtain access to the data (two breaches), or employee theft (one breach). Thus, fraud occurred in 29 percent of the intentional breaches, and may have occurred in

Even when intentional breaches compromise huge numbers of consumer records, the risk of actual harm to those consumers is vastly lower. The simple logistics of exploiting stolen information necessarily limit the risk of injury to individual consumers. Although it requires only five minutes to complete a credit application, it would take about fifty years for a single thief to exploit all of the stolen information on one million individuals.[46] Indeed, the ID Analytics study of an intentional breach of data that included social security numbers resulted in misuse in only 0.098 percent of the compromised identities.[47] If the methodology catches 10 percent of actual misuse, the risk to an individual whose information was stolen is under 1 percent.

2. Identity theft.

The first systematic analysis of the nature and extent of identity theft was a consumer survey conducted by the FTC in 2003.[48] The survey distinguished two different forms of identity theft—new account fraud, in which the thief opens new accounts or commits other offenses using the victim's identity, and existing account fraud, which compromises an existing account (usually a credit card).[49] Existing account fraud affects roughly two-thirds of the victims (an estimated 6.7 million victims, versus 3.23 million victims of new account fraud)

---

an additional 14 percent. Five breaches were incidental and four were accidental. One breach involved unrelated fraud charges against an employee with access to sensitive data, but there is no evidence that the data were compromised. See GAO, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* 26 table 1 (June 2007), online at http://www.gao.gov/new.items/d07737.pdf (visited Jan 12, 2008).

46 ID Analytics, *National Data Breach Analysis* at 10, 25 (cited in note 42). The study assumed that the thief works 6.5 hours per day, five days per week, and fifty weeks per year. Markets for stolen information exist to reduce these logistical barriers. Numerous "carding sites" traffic in stolen credit card data, for example. The Secret Service estimates that the two largest carding cites currently have over 20,000 member accounts. The President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan* 20 (2007), online at http://www.idtheft.gov/reports/StrategicPlan.pdf (visited Jan 12, 2008).

47 Id. Because the methodology only detects misuse that occurs among ID Analytics's subscribers, this figure is undoubtedly an understatement. Currently, the company evaluates almost 40 million transactions per month, and its risk scores are offered to card issuing banks through Visa USA. See ID Analytics, *Strength in Numbers* 2 (2006), online at http://web.archive.org/web/20061017120625/www.idanalytics.com/pdf/IDNetworkOverview.pdf.

48 Synovate, *Federal Trade Commission: Identity Theft Survey Report* ("*FTC 2003 Identity Theft Survey Report*") (Sept 2003), online at http://www.ftc.gov/os/2003/09/synovatereport.pdf (visited Jan 12, 2008).

49 Credit cards accounted for 67 percent of the misused existing accounts. Other accounts misused included checking or saving accounts (19 percent), telephone accounts (9 percent), internet accounts (3 percent), and insurance accounts (2 percent). Id at 33.

but less than one-third of the total losses ($14 billion, compared to $32.9 billion for new account fraud).[50]

Costs to the consumer victim, both out of pocket and the time and effort needed to resolve the matter, also differ significantly for new account and existing account fraud.[51] Compromises of existing credit card accounts are discovered more quickly (39 percent detect the problem in less than a week, versus 17 percent for new account frauds), resolved more quickly once discovered (57 percent of cases are resolved in less than a week, versus 25 percent for new account fraud), and are unlikely to linger (9 percent of victims took three or more months to resolve the issue, versus 39 percent for new account fraud).[52] Existing account fraud is unlikely to involve out-of-pocket losses (75 percent have no losses, versus 50 percent for new account frauds).[53] On average, victims of existing account fraud lost $160 out of pocket and spend fifteen hours to resolve the problem. In sharp contrast, victims of new account fraud lost $1,180 and spent sixty hours resolving the problem.[54] Undoubtedly, the differences in the costs to victims reflect the fact that credit card companies have sophisticated fraud detection systems to help prevent fraudulent use of credit cards.[55]

Not surprisingly, most victims of identity theft do not know who obtained the information about them. Only 34 percent of victims of new account fraud, and 18 percent of victims of a compromised credit card account, have this information.[56] Among those who knew (26 percent of all cases), 35 percent said the thief was a family member or other relative, and 18 percent said the thief was a friend, neighbor, or household

---

50 Id at 7. The incidence and cost figures are based on respondents who were victims of identity theft within the year prior to the survey. Other data are based on respondents victimized within the five years prior to the survey. The modal value of what the thief obtains with compromised existing accounts is $100–$499 (30 percent of victims). For new account fraud, the modal value is $5,000 or more (36 percent). Id at 41.

51 New account fraud also includes other misuses of identity that may have particularly serious consequences. For example, 4 percent of all victims (including existing account fraud victims) report that a crime was committed using their identity, 3 percent report that the thief obtained government documents, and 2 percent report that the thief filed tax returns in their name. Id at 37.

52 Id at 26. Moreover, 50 percent spent less than one hour to resolve the problem, versus only 15 percent for new account fraud. Id at 45.

53 Id at 43. Among victims of new account frauds, 16 percent experienced out-of-pocket losses of $1,000 or more, compared to only 3 percent of victims of credit card fraud.

54 Id at 7.

55 Credit card systems have reduced the fraud rate on general purpose credit cards in the United States from a high in 1992 of 15.7 cents per $100 of cash and spending to 4.7 cents in 2004, a 70 percent decline. Joe Majka and Sergio Pinon, *Credit Card Fraud in the U.S.*, The Nilson Report 8–9 (Mar 2005).

56 *FTC 2003 Identity Theft Survey Report* at 28 (cited in note 48).

employee.[57] Thus, the known offenders are frequently well known. Family members and relatives are apparently more likely to commit new account fraud rather than utilize existing credit card accounts (52 percent of new account victims who know the identity of the thief, versus 26 percent for existing credit cards).[58] The next-largest category of known thieves is employees of the company that had the information.[59]

Since the FTC survey, others have sought to replicate its methodology. Trends, however, are difficult to discern. Because sample sizes are relatively small (just over four thousand in the original FTC survey, and around five thousand in subsequent surveys), and the incidence of identity theft relatively low (4.6 percent in the past year in the FTC survey), finding statistically significant differences in incidence or cost is difficult. Javelin Strategy and Research has replicated the FTC methodology (with inconsequential differences) since 2005. Their 2007 report found that 3.74 percent of the US population had been victims of identity theft,[60] compared to 4.6 percent in the FTC survey. Total losses, however, were essentially unchanged ($49.3 billion, versus $53.8 billion in 2003, both in 2007 dollars).[61] New account fraud was also down (1.05 percent of the population, versus 1.5 percent in the FTC's 2003 survey).[62] Although the trend in identity theft appears to be downward, the decline is certainly not large, and may not be statistically significant.[63]

---

57 Id at 28, 29.

58 Id at 28.

59 This category accounts for 23 percent of all victims who know the identity of the thief (33 percent of new account victims; 13 percent of credit card fraud victims). Id at 29.

60 See Mary T. Monahan, *2007 Identity Fraud Survey Report: Identity Fraud Is Dropping, Continued Vigilance Necessary* 1 (Javelin Strategy & Research, Feb 2007), brochure online at http://www.javelinstrategy.com/uploads/701.R_2007IdentityFraudSurveyReport_Brochure.pdf (visited Jan 12, 2008). The sample size was 5,006 consumers.

61 Id at 60. Javelin's estimate of total losses reported in the text is based on a three year moving average of total loss estimates. The actual survey estimate for 2007 was $34.5 billion.

62 Id at 19. Javelin reports that the incidence of new account fraud in 2003 was 1.0 percent. The FTC report, however, which is the source of the figure, reports the incidence as 1.5 percent. There was no change in methodology that would account for the discrepancy.

63 It is clear, however, that trends based on complaints about identity theft are not reliable. For example, the FTC received 214,905 identity theft complaints in 2003 and 246,035 complaints in 2006. FTC, *Identity Theft Victim Complaint Data: January 1–December 31, 2006* 3 (Feb 7, 2007), online at http://www.ftc.gov/bcp/edu/microsites/idtheft/downloads/clearinghouse_2006.pdf (visited Jan 12, 2008); FTC, *National and State Trends in Fraud & Identity Theft: January–December 2003* 3 (Jan 22, 2004), online at http://www.consumer.gov/sentinel/pubs/Top10Fraud2003.pdf (visited Jan 12, 2008). Nothing in the results from random samples of consumers would suggest the 14 percent increase in identity theft that the complaint data imply. The complaints are far more likely driven by increased consumer awareness of the problem and of the FTC as a place to complain.

3. Incentives to protect sensitive information.

Businesses, of course, have incentives to protect sensitive information. In the aggregate, businesses bear approximately 90 percent of the total costs of identity theft.[64] Financial institutions in particular are likely to bear significant costs if compromised information allows a thief to commit fraud against existing accounts.[65] Consumer losses from credit card fraud are limited by law to $50,[66] and many credit card issuers generally waive even that limit.[67] Moreover, reissuing credit cards to avoid further fraud losses involves significant costs to the institution, creating incentives to avoid the problem in the first place. Institutions that open new accounts for an identity thief will bear all of the losses, and thus have incentives to try to verify an applicant's identity.

Others who possess sensitive data, however, often do not bear the full costs of compromised data. For example, retailers who retain credit card numbers are not liable for fraud losses if the network (for example, Visa or MasterCard) has approved the transaction,[68] even if the compromised data is used to make fraudulent purchases from the same retailer. More significantly, in all probability the information stolen from one retailer will be used to commit fraud somewhere else, avoiding any potential cost to the retailer who permitted the breach. A credit card number stolen from a bricks-and-mortar shoe retailer may be used to purchase a big-screen, high-definition TV from an online merchant, for example.[69] Both problems imply that retailers do

---

64 The FTC survey estimated that the total amount of fraud in 2003 was $47.6 billion. The loss to victims (included in the total loss) was $5.0 billion. *FTC 2003 Identity Theft Survey Report* at 7 (cited in note 48).

65 Thomas M. Lenard and Paul H. Rubin, *An Economic Analysis of Notification Requirements for Data Security Breaches*, Progress on Point 12.12 (The Progress & Freedom Foundation, July 2005), online at http://www.pff.org/issues-pubs/pops/pop12.12datasecurity.pdf (visited Jan 12, 2008).

66 15 USC § 1643(a)(1)(B) (2000).

67 FDIC Consumer News, *It Pays to Ask Questions before Paying for Credit Card Insurance* (Fall 2000), online at http://www.fdic.gov/CONSUMERS/consumer/news/cnfall00/diduknw.html (visited Jan 12, 2008).

68 See David S. Evans and Richard Schmalensee, *Paying with Plastic: The Digital Revolution in Buying and Borrowing* 119 (MIT 2d ed 2005) ("The merchant is typically guaranteed payment even if a cardholder never pays their bill or the card is stolen—so long as the merchant follows the authorization procedures agreed to (such as comparing signatures on the slip and the card)."). Losses are allocated to the merchant when the card is not present.

69 Fraud rates are vastly higher in online transactions than offline. In 2002, fraud losses in online transactions were some thirty times higher than fraud losses offline—2.1 percent of total credit card sales online, compared to only 0.07 percent offline. Despite a smaller transactions base, online losses accounted for one-third of total US credit card losses attributed to fraud in 2002. Celent Communications, via Lafferty Publications, as reported by Kalysis, *Statistics for General and Online Card Fraud*, US Credit Card Fraud Statistics, 2000–2007 (2007), online at

not have appropriate incentives to protect data they possess. For this reason, in part, the payment card industry has adopted security standards for merchants who accept payment cards.[70]

More generally, consumers also bear significant costs that companies in possession of sensitive information have no incentive to consider. Business losses are substantial, but as documented above, the costs to consumers, both out of pocket and in the time and effort to resolve the matter, are substantial as well. The usual market checks of reputation and repeat business are unlikely to offset these problems, if only because a substantial majority of identity theft victims do not know how (or where) the thief obtained the information. Absent proper market incentives, the potential exists for government intervention to improve consumer welfare.

B. The FTC's Information Security Program

At its root, identity theft is a criminal law enforcement problem. Civil remedies are unlikely to prevent or deter either the theft of information, or the subsequent fraudulent use of that information. Like Willie Sutton, information robbers will, at least on occasion, succeed, and when they do, there is no alternative to criminal prosecution. But when theft occurs because a company controlling valuable information has failed to take reasonable steps to protect it, civil law enforcement against the company may be appropriate as well.

As the FTC sought to refocus its privacy agenda around the consequences of information misuse, it increasingly brought cases involving information security issues. The most comprehensive statement of the FTC's view of security practices is its Safeguards Rule, promulgated under the Gramm-Leach-Bliley Act[71] (GLB Act) to assure that financial institutions protect sensitive data.[72] The rule covers a wide range of "financial institutions" subject to the FTC's jurisdiction,[73] and establishes a very flexible approach to information security.

---

http://kalysis.com/content/modules.php?op=modload&name=EasyContent&file=index&menu=410&page_id=109 (visited Jan 12, 2008).

70 See generally PCI Security Standards Council, *Payment Card Industry (PCI) Data Security Standard* (Sept 2006).

71 Pub L No 106-102, 113 Stat 1338 (1999), codified at 15 USCA § 6801–09 (2007).

72 See FTC, *Standards for Safeguarding Customer Information*, 67 Fed Reg 36484, 36485 (2002) (promulgating 16 CFR Part 314 (The Safeguards Rule)). Similar rules apply to financial institutions that are subject to other regulators such as the Federal Reserve or the Comptroller of the Currency.

73 The GLB definition of financial institutions is extremely broad. Accountants, mortgage brokers, and many other businesses that are not conventional "financial institutions" fall within the definition, because they offer services banks were permitted to offer prior to the GLB Act.

The Safeguards Rule views security as a process. Regulated companies must develop a security plan identifying the risks the company faces, implement reasonable steps to address these risks, and provide for reassessment and revision as the risks change. There are no requirements for particular security measures or technologies. Rather, each company's security plan must be appropriate for its own situation. Core elements of that program include designating a responsible individual; conducting a comprehensive risk assessment in all relevant areas of the business; designing reasonable safeguards to control these risks and regularly monitoring their effectiveness; adjusting the program as needed; and documenting the program in writing.

Most of the Commission's information security cases have been based on the prohibition on "unfair or deceptive acts or practices" in § 5 of the FTC Act.[74] The Commission's first cases were based on deception—a company had promised to keep sensitive information secure and failed to honor that promise.[75] Recognizing that perfect security is impossible, the complaints construe a promise to protect sensitive information as one to take steps that are "reasonable and appropriate under the circumstances."[76] In turn, what is reasonable and appropriate depends on the sensitivity of the information. Thus, the cases establish a sliding scale, with more sensitive information requiring more elaborate security precautions. To date, all of the cases were resolved with consent agreements; there have been no litigated cases involving information security issues.

Importantly, the Commission has sought to avoid a standard of strict liability for any breach. Clever thieves can defeat virtually any security system on at least some occasions. Commission statements about information security have repeatedly said that not all breaches are actionable.[77] Instead, the issue is whether the company was employing reasonable and appropriate security measures.

---

74 15 USCA § 45(a) (2007).

75 A practice is deceptive if it is likely to mislead a consumer, acting reasonably in the circumstances, about a material fact. See FTC, *The FTC Policy Statement on Deception* (Oct 14, 1983), online at http://www.ftc.gov/bcp/policystmt/ad-decept.htm (visited Jan 12, 2008); *Thompson Medical Co, Inc v FTC*, 791 F2d 189, 193–94 (DC Cir 1986).

76 See Complaint, *In the Matter of Guess?, Inc, and Guess.com, Inc* ("*Guess?* Complaint"), No C-4091, *3 (July 30, 2003), online at http://www.ftc.gov/os/2003/08/guesscomp.pdf (visited Jan 12, 2008) (alleging that Guess?, Inc, wrongfully exposed consumers' personal information by maintaining a website that was susceptible to commonly known hacking techniques); Complaint, *In the Matter of Microsoft Corp* ("*Microsoft* Complaint"), No C-4069, *2 (Dec 20, 2002), online at http://www.ftc.gov/os/caselist/0123240/microsoftcmp.pdf (visited Jan 12, 2008) (charging that Microsoft had deceived users of its online .NET Passport service when the company failed to maintain the security measures promised in its privacy policy).

77 See, for example, Identity Theft: Recent Developments Involving the Security of Sensitive Consumer Information, hearing before the Senate Committee on Banking, Housing, and Urban

The cases establish several basic principles. Even inadvertent breaches can constitute a violation. Eli Lilly, for example, inadvertently revealed the email addresses of all subscribers to its daily reminder service for Prozac users. The complaint alleged that this breach occurred because of the failure to provide adequate training and oversight, and the failure to implement appropriate checks and controls on the process of writing new software. Thus, it alleged, the company had "not taken steps appropriate under the circumstances" to keep its promise to protect sensitive information.[78]

The Commission has also brought cases when a proven breach of security has not yet occurred. In the Microsoft case, the FTC complaint alleged that the Passport system did not employ "sufficient measures reasonable and appropriate under the circumstances" to keep its promise to protect the information, including credit card numbers that were stored in Passport Wallet. Although there was no known actual breach, the complaint alleged that the company failed to implement procedures to prevent and detect unauthorized access, or to retain sufficient information to conduct security audits. Thus, even if breaches had occurred, they could not reliably be detected.[79]

Because the Commission views security as a process, an important component of information security is adapting to new and emerging threats. In *Guess?*, the complaint alleges that the company's website was vulnerable to a well known and easily prevented vulnerability known as an "SQL injection" attack.[80] Through this attack, a hacker could gain access to customer information, including credit card numbers and expiration dates. Even if the security system were state of the

---

Affairs 14 n 42 (Mar 10, 2005) (statement of the FTC) ("It is important to note, however, that there is no such thing as perfect security, and breaches can happen even when a company has taken every reasonable precaution."), online at http://www.ftc.gov/os/testimony/050310idtheft.pdf (visited Jan 12, 2008); Identity Theft, hearing before the House Financial Services Committee 15 (Apr 3, 2003) (statement of the FTC), online at http://www.ftc.gov/os/2003/04/bealesidthefttest.pdf (visited Jan 12, 2008):

> It is important to note that the Commission is not simply saying "gotcha" for security breaches. While a breach may indicate a problem with a company's security, breaches can happen even when a company takes all reasonable precautions. In such instances, the breach does not violate the laws that the FTC enforces. Instead, the Commission recognizes that security is an ongoing process of using reasonable and appropriate measures in light of the circumstances.

78 Complaint, *In the Matter of Eli Lilly and Co*, No C-4047, *3–4 (May 8, 2002), online at http://www.ftc.gov/os/2002/05/elilillycmp.htm (visited Jan 12, 2008) (alleging that the defendant had deceived customers in not maintaining the data privacy policies that were promised in the company privacy policy).

79 *Microsoft* Complaint at *2.

80 *Guess?* Complaint at *3.

art when first installed, the failure to adjust to avoid a new and well known vulnerability was alleged as a violation.[81]

Attempts to correct problems can also introduce new vulnerabilities if they are not carefully implemented. In the Tower Records case, for example, in redesigning the "checkout" portion of its website, the company failed to ascertain whether the user seeking information about an order was the person who placed the order.[82] Thus, users could obtain information about all purchases from Tower pertaining to any other online customer. As in Lilly, the complaint charged that the problem resulted from the failure to maintain reasonable and appropriate procedures to manage software revisions.[83]

More recently, the Commission has applied the same general principles even in the absence of a security promise, alleging that the failure to maintain reasonable security policies and practices is unfair.[84] *BJ's Wholesale Club*[85] was the first unfairness case. Like many retailers, BJ's transmitted and stored credit card information over its computer network without encryption. The network also included wireless access points that supported wireless devices used to help manage inventory. Unfortunately, these access points did not employ "readily available security measures to limit access." This failure allowed unauthorized wireless users to enter BJ's computer network, where credit card information was stored in files that could be accessed anonymously, using default user names and passwords supplied with the software. The complaint also alleged inadequate measures to detect and investigate unauthorized access, and that BJ's unnecessarily increased the risk by retaining information for which it no longer

---

81 Id. The same issue, and the same vulnerability, was involved in Decision and Order, *In the Matter of Petco Animal Supplies, Inc*, No C-4133, *3–4 (Mar 4, 2005), online at http://www.ftc.gov/os/caselist/0323221/050308do0323221.pdf (visited Jan 12, 2008) (alleging that Petco failed to take reasonable and appropriate precautions against SQL injection attacks, a well known and easy to correct vulnerability).

82 Complaint, *In the Matter of MTS, Inc*, No C-4110, *3–4 (May 28, 2004), online at http://www.ftc.gov/os/caselist/0323209/040602comp0323209.pdf (visited Jan 12, 2008).

83 Id.

84 See 15 USC § 45(n) (2000):

> The Commission shall have no authority under this section or section 57a of this title to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

85 Complaint, *In the Matter of BJ's Wholesale Club, Inc*, No C-4148, *3 (Sept 20, 2005), online at http://www.ftc.gov/os/caselist/0423160/092305comp0423160.pdf (visited Jan 12, 2008) (alleging that the "failure to employ reasonable and appropriate security measures to protect personal information and files caused . . . substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers").

had a business need. Many cards used at BJ's were counterfeited, and used to make "several million dollars in fraudulent purchases."[86]

Taking these deficiencies together, the complaint alleged, the "failure to employ reasonable and appropriate security measures" caused or was likely to cause substantial consumer injury, without offsetting benefits to consumers or competition, that consumers could not reasonably avoid. It was therefore an unfair practice in violation of § 5. Thus, the Commission's basic approach is the same under either an unfairness or a deception theory. The issue is whether a company has taken reasonable and appropriate security measures to protect sensitive information.[87]

Unfairness was also the basis for prosecuting CardSystem Solutions,[88] a credit card processor responsible for a breach that compromised an estimated 40 million credit card numbers.[89] CardSystem Solutions retained full data from the magnetic stripe on the back of the cards, thus enabling thieves to produce counterfeit cards that were indistinguishable from the genuine card in the approval process. As in other cases, the complaint alleged a series of poor security practices that, taken together, constituted a failure to maintain reasonable and appropriate security measures, and was therefore an unfair practice.

Last year, the Commission used an unfairness theory to prosecute ChoicePoint for a breach that compromised records of more than 163,000 consumers.[90] ChoicePoint, a so-called data broker, supplies sensitive identifying information, as well as credit reports about consumers, to some 50,000 business clients, who use the information for a wide variety of purposes. Although consumers may be harmed, they are not ChoicePoint's customers. Despite significant intellectual property reasons for preventing theft of its data, the company may not have very strong market incentives to examine whether its customers actually have a legitimate need for the information.

---

86 Id.

87 The Commission also brought a substantially similar case against DSW. Complaint, *In the Matter of DSW, Inc*, No C-4157, *3 (Mar 7, 2006), online at http://www.ftc.gov/os/caselist/0523096/0523096c4157DSWComplaint.pdf (visited Jan 12, 2008).

88 Complaint, *In the Matter of CardSystems Solutions, Inc*, No C-4168, *2–3 (Sept 5, 2006), online at http://www.ftc.gov/os/caselist/0523148/0523148CardSystemscomplaint.pdf (visited Jan 12, 2008) (alleging that CardSystems was unreasonably vulnerable to attack by hackers, and that this vulnerability was unfair).

89 *Data Security Roundtable: The Threats to Data Security: What's Here, What's Ahead*, Am Banker 10 (Nov 23, 2005) (reporting the CardSystem breach as the largest data theft to date).

90 Stipulated Final Judgment and Order for Civil Penalties, Permanent Injunction, and Other Equitable Relief, *United States v ChoicePoint, Inc*, No 1 06-CV-0198, *14–16 (ND Ga Feb 15, 2006), online at http://www.ftc.gov/os/caselist/choicepoint/stipfinaljudgment.pdf (visited Jan 12, 2008) (ordering ChoicePoint to implement a variety of precautions in processing requests for credit reports).

ChoicePoint offers information products that many businesses use to verify that an applicant is who he or she claims to be—exactly the information an identity thief needs. Unfortunately, ChoicePoint signed up putative business clients without adequate verification—including its failure to utilize its own identity verification products. As a result, fraudulent businesses signed up as customers, often submitting their applications using public fax machines and reporting conflicting or incomplete information about their business need for the information. Along with several violations of the Fair Credit Reporting Act that resulted in a $10 million civil penalty, the Commission alleged that the failure to maintain adequate customer verification procedures was an unfair practice. Besides the usual order requirements, it also imposed $5 million in consumer redress to compensate individuals who were victims of identity theft.

To date, the Commission's use of unfairness to attack information security problems has been appropriate, but the theory is potentially far-reaching and subject to abuse.[91] An unfairness theory is sound when security deficiencies are clear, have resulted in intentional breaches that are highly likely to lead to fraudulent use of the information, and low-cost steps that would significantly reduce the risk are readily apparent.

Unfairness is essentially a cost-benefit test, but the Commission (and the court) lacks the expertise to fine-tune difficult choices about security tradeoffs and priorities, particularly given that they will almost inevitably be evaluating those choices with perfect hindsight. Companies must make security choices ex ante. Whatever choice they make, if a breach occurs, the Commission can almost always find an "expert" to say that the precise risk that materialized should have been addressed. Ex post, that expert is correct, but following that advice ex ante would inevitably have led to less attention to a different risk that did not occur, perhaps because of the steps that the company took to avoid it. Moreover, from the perspective of security as a process, companies must rely in significant part on the evidence of the threats they actually confront, which may differ from the threats facing others. Second guessing choices about allocating resources based on a company's own experience versus risks that others might face is particularly problematic.

Each security breach should teach lessons about potential vulnerabilities. Some of those lessons have been taught before, and companies that have not paid attention can, and should, be held account-

---

[91] See J. Howard Beales, *The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection*, 22 J Pub Policy & Marketing 192 (2003) (suggesting parameters for FTC use of the "unfairness authority").

able. Some breaches reveal entirely new risks that few, if any, anticipated. Liability for failure to anticipate such risks is inappropriate. Other breaches, perhaps most, reveal new information about the changing relative probabilities of various risks. Companies should respond to that information, but we cannot expect perfect foresight. Hindsight will always have information that was not available when the choice was made. Reasonable ex ante choices, even when they prove wrong, should not result in liability for breaches.

The unfairness cases so far have involved actual fraudulent use of stolen information. When intentional theft of information has occurred, the Commission need not prove actual fraud to prevail in an unfairness case, particularly if the interval between the breach and its detection is short enough that fraudulent use may not yet be observable. Cases involving accidental or incidental information loss, however, are far more problematic. The problems inherent in second guessing are every bit as real, but the (admittedly limited) evidence to date provides little reason to believe that such breaches are likely to cause substantial consumer injury.

Taken together, there are several noteworthy aspects of the Commission's information security cases. First, they have avoided the temptation to identify a single failure as the source of a violation. FTC complaints have noted, for example, the lack of encryption or unnecessary data retention as evidence of inadequate security procedures. They have not, however, challenged failure to encrypt or unnecessary data retention as § 5 violations. Doing so would likely lead many businesses to encrypt (or examine data retention schedules closely), whether they need to or not, and without regard to the sensitivity of the information.

Second, the orders entered to resolve the cases have avoided detailed regulatory requirements. In the fast-changing world of information technology and cyber attacks, specific regulatory requirements are likely to become obsolete quickly. Instead, orders have required a planning process to identify reasonably foreseeable risks and take reasonable steps to address those risks, supplemented by outside audits to assess the adequacy of the security program.

Third, the orders have not required notice to individual consumers whose information was compromised. In the more recent cases, pursuant to state laws, notice was already given (and may have brought the breach to the Commission's attention). But even in the earlier cases, notice was not required. Notice is potentially attractive because it enables consumers to try to protect themselves, but its value depends both on the likelihood that the information will be misused and on the availability of reasonable steps to reduce the risk of loss. If the circumstances of the breach indicate that information is,

in fact, being used for identity theft, or that misuse is highly likely, notice will be extremely valuable. Depending on the type of information compromised, consumers can take appropriate steps such as placing a fraud alert on their credit report to prevent the opening of new fraudulent accounts, or examining their report to clear up any fraudulent information.

In addition to consumers, or even in lieu of direct notification to consumers, in some cases other parties should receive notice (for example, credit reporting bureaus and credit card issuers). Because some consumers will inevitably fail to receive, act upon, or, perhaps, understand the notice sent to them, or because the costs of notice may outweigh the benefits to consumers, it could be useful for a business that suffers a breach to notify other relevant parties. For example, if only credit card numbers were compromised, notifying the credit card issuers so that they can monitor and close affected accounts if necessary may be an alternate solution to blanket notification of consumers. Because the credit card companies bear the financial risk of unauthorized transactions, they have incentives to be vigilant and have mechanisms in place to contact consumers about questionable transactions. Furthermore, consumers' options for self-help are no different than those the credit card companies would follow: monitor and close affected accounts. Thus, the cost of notice to consumers might outweigh any benefits given the ability of the credit card system to identify and stop injury.

In still other cases, notice to consumers or other parties may have little or no value. When a database has been compromised, it may be discovered that the perpetrator was only trying to prove that the system could be breached, as in the *Guess?* case, or it may be difficult to determine exactly which information, if any, has been stolen. Individualized notices to consumers would concern them for no particular reason, and would likely reduce the attention consumers would pay to other notices when action may actually be important. Moreover, if consumers place fraud alerts when the risk is low, the value of the fraud alert as a signal of a real risk of fraud might be reduced.

CONCLUSION

Economists have long recognized the costs of information and the constraints they impose. Continuing advances in computing and telecommunications have transformed the structure of those costs, making possible information collection and processing that simply was not feasible only a few years ago. In turn, increased collection and use of information about commercial transactions has fanned increased privacy concerns.

The information economy will continue to create enormous benefits for consumers. Information tools help to reduce the risk of fraudulent transactions, facilitate access to public records that the government has decided should be available to anyone, and enable such everyday conveniences as consolidated financial statements and widespread credit availability. Information sharing is essential to accomplish such mundane tasks as clearing a check or processing a credit card transaction at the lowest possible cost. Much of the information that enables these benefits is sensitive, and needs protection. But protections should be structured to preserve the existing benefits of the information economy, and to permit the emergence of new technologies and new services that have not yet been invented.

The Fair Information Practices, the basis of much analysis about privacy and privacy regulation, are inadequate guides for sound public policy. They ignore the very real costs of gathering information and making decisions when, for most consumers, very little is at stake. Such decisions, for most, are simply not worth worrying about. Applied literally, FIPs would seriously compromise important institutions such as credit reporting or property recordation. A far better approach to privacy protection is to focus on the consequences of information use and misuse for consumers. This approach directs attention to the relevant tradeoffs between benefits and costs of information use. It enables practical solutions to real-world privacy problems, such as the Do Not Call Registry and law enforcement to help preserve the security of sensitive information.

Protecting sensitive information is important, but there are other vital interests at stake. Wise choices about privacy protection can be made only after careful consideration of the particular uses of information, the problems they may pose for consumers, and the benefits those uses may offer to other consumers and the economy as a whole.

