Chapter XI. Privacy and Data Security

In its discussion of credit information systems, the National Commission on Consumer Finance noted the issues surrounding privacy and the control of information systems, including specifically the need to consider carefully the tradeoffs often involved in protecting privacy. The concern at the time was the growing use of computers, and the Commission noted that "protection against the invasion of privacy in the computer age must be achieved by balancing the need to preserve privacy against the desire to maximize benefits of efficiency inherent in the new technology."[1] In the internet age, it is clear that the benefits of new technology go far beyond greater efficiency in accomplishing old, familiar tasks, and include the creation of entirely new ways of satisfying consumer desires. Perhaps more so in financial services than in many other markets, thee important benefits depend on the free flow of information. The Commission concluded that "There must be no barrier to the prompt flow of adequate credit information into and out of the data base. *Any laws or action or inaction by industry that impede these flows also lower the availability of credit and raise its price to consumers."*[2] The Taskforce believes that conclusion is just as valid today as it was when the Commission reached in in 1972.

This chapter considers the related issues of financial privacy and data security. We begin in Section I with a discussion of two fundamental economic factors that should shape approaches to privacy regulation, information asymmetry and the costs of conducting transactions. Section II considers the current disclosure-based approach to privacy regulation and argues that it is doomed to failure. In Section III, we lay out an approach to privacy regulation based on the consequences of information use and misuse, which considers both the benefits of information sharing and the potential costs, to privacy and otherwise. Section IV turns to information security and discusses a framework for analysis of information security issues.

I. Foundational Considerations

Many have argued that privacy is a matter of controlling the flow of information about an individual. Individuals want to choose what information they reveal, and to whom. On the other hand, providers of financial services in particular have a legitimate need for information about a consumer that the consumer might prefer not to reveal. This is the problem of information asymmetry: individual consumers may know more about the risks they pose than do providers of financial services. A second foundational issue is the costs of exercising control, which we consider in the topic of transaction cost economics.

A. Information asymmetry

A common concern in discussions about the cost of information is the problem of information asymmetry – one party to the potential transaction knows more about the deal than the other. Because information is costly, different parties, and different consumers, will have

[1] NCCF Report at 212.
[2] Id. at 213.

different amounts of information. The costs and benefits of acquiring information differ, so information disparities are inevitable.

In certain circumstances, information asymmetries can create problems in otherwise competitive markets. The best-known case is the market for "lemons."[3] Akerlof's conceptual example is the market for used cars. Sellers know whether the car they offer is high quality, and worth a high price, or low quality and therefore worth less. Buyers, however, cannot observe whether the product is high quality or low, but they are assumed to know the average quality of cars on the market. Market price will therefore reflect the average quality of traded goods. Sellers can profit by offering low quality goods at the high-quality price, which will reduce the average quality, reduce the market price, and reduce sellers' ability to offer high quality goods profitably. In the extreme, only low-quality goods are offered.

Fortunately, there is little or no evidence that any market has actually been destroyed by lemons market phenomenon. Nevertheless, some studies show that consumer inability to determine quality ex ante has detectable effects. For example, a recent study of the used car market found that trading for eight-year-old cars was delayed on average by about four months compared to what it would have been if quality had been fully observable.[4]

One factor limiting the emergence of lemons markets is the existence of quality assuring price premiums. Sellers who cheat by misrepresenting low quality goods as high quality will lose future sales. If there is a sufficient price premium for high quality, the potential loss of that premium by cheating motivates sellers to continue supplying high quality, because it is more profitable to do so in the long run.[5] In addition, as discussed in Chapter 7, investments in advertising and developing a good reputation create a bond that the firm will lose in the event of poor performance.[6]

Asymmetric information is important in credit markets, but it goes by a different name: adverse selection. Information is asymmetric because consumers have information about their likely ability and willingness to repay a loan that potential lenders cannot easily determine and may not be able to determine at all. The construction worker who seeks a loan to cover an income shortfall because of reduced hours likely knows whether the reduction was the result of bad weather or the employer's financial difficulties. The consumer with unexpected medical

---

[3] George A. Akerlof, "The Market for 'Lemons': Quality Uncertainty and the Market Mechanism." 84 *The Quarterly Journal of Economics* 488–500 (1970).

[4] Jonathan R. Peterson & Henry S. Schneider, *Adverse Selection in the Used-Car Market: Evidence from Purchase and Repair Patterns in the Consumer Expenditure Survey*, 45 RAND J. ECON. 140, 143 (2014). The effect for Hondas and Toyotas was smaller, around one month, than the effect for the American cars studied, the worst of which was about five months. *See id.* at 152 (Figure 3).

[5] See Klein and Leffler, supra note __, who develop such a model.

[6] See Chapter 7, text accompanying notes 15-23.

expenses inevitably knows more about the prognosis and the likely future consequences for income and expenses than does a potential lender.[7]

Of course, lenders can and do build sophisticated risk management models designed to predict the likelihood that a consumer will be both willing and able to repay a loan. By their nature, however, these tools are based on the performance of groups of individuals with a given set of characteristics. There remains variation within the group, where individuals have information about their own circumstances that creditors lack.

At a given interest rate, consumers who are more likely to default are also more willing to borrow at that interest rate. Moreover, the higher the interest rate, the greater the default risk of the consumers who are still willing to borrow. Lenders can observe the overall default rate in their portfolio, but they lack complete information on the risk that any individual borrower poses. If the default rate is higher than expected, lenders will raise their rates to cover the risk. Unfortunately, a rate increase tends to drive out low risk borrowers, who are unwilling to pay the higher rate, and the default risk of the remaining customers increases. In the simple lemons model, low-quality goods drive out high-quality goods. In credit markets, high-risk borrowers drive out low-risk borrowers, potentially until only high-risk borrowers remain.[8]

Even if it does not destroy markets entirely, adverse selection creates real costs for consumers. In particular, the interest rate charged must be high enough to cover the average risk in the pool of borrowers. If lenders cannot distinguish based on risk, all will pay the same rate. Low risk borrowers are paying more for credit than their default risk would require, and high-risk borrowers are paying less than they should. Thus, low-risk borrowers effectively subsidize the higher risk borrowers.

One lender response to limit adverse selection is limiting the amount of credit extended. Because all consumers have limits on their ability to repay, larger loans involve a larger risk of default. Limiting loan size can therefore reduce the risk of default. Limiting loan size also limits the lender's potential losses in the event of default. The result, however, is that consumers cannot get as much credit as they want at prevailing interest rates, even though they are willing to pay for it. Moreover, some borrowers are denied credit, even though they are willing to pay for it.[9]

The response of credit markets to the coronavirus pandemic demonstrates exactly this problem. Lenders who allow borrowers to defer payments cannot report those payments as late to the credit reporting agencies. Deferrals have been given on over 100 million accounts. The result is that it is more difficult for lenders to identify risks, leaving no alternative but to cut back

---

[7] For a formal model of credit granting decisions with imperfect information, see Joseph E. Stiglitz and Andrew Weiss, Credit Rationing in Markets with Imperfect Information, 71 American Economic Review 393-410 (1981).

[8] This discussion assumes that all consumers are offered the same price. As discussed below, risk-based pricing avoids this problem by differentiating consumers based on risk.

[9] Thomas A. Durkin, Gregory E. Elliehausen, Michael E. Staten, and Todd J. Zywicki, Consumer Credit and the American Economy, Oxford University Press 2014, at 242.

on credit extensions. In early April 2020, one third of banks reported that they had increased their minimum credit score requirements for credit cards. Mailed offerings of new credit cards and personal loans, and loan originations for credit cards, auto loans, and personal loans declined sharply through March, April, and May.[10] With less ability to identify risk, the likely result is less credit for broad portions of the population.

A different, and better, solution to the adverse selection problem is to reduce the information asymmetry that is the cause of the problem. That is the role of credit reporting agencies. By pooling information about past payment history, credit bureaus enable lenders to better separate potential borrowers based on the default risk they pose.

As credit reporting grew, it fostered the development of formal risk scoring systems, such as the familiar FICO score. Many creditors develop their own risk assessment models to take into account the particular characteristics of their products or customers. A 2004 study identified 70 different generic scoring systems that were available at the time, with more than 100 different scoring models.[11] Risk assessment models based on credit bureau data have been shown to outperform assessments based on application data in the context of credit card applications.[12] Some studies indicate that the delinquency risk when decisions are based on scoring algorithms from credit report data are 20 to 30 percent lower than the risk of delinquency when the lender uses "judgment" to decide which consumers deserve a loan.[13]

In turn, credit reporting and automated scoring systems enabled the emergence of risk-based pricing. Rather than charging all borrowers the same interest rate, risk-based pricing separates borrowers based on the likelihood of default. Borrowers who are better risks get lower rates than they would have to pay if all are charged the same rate. Higher risk borrowers are able to borrow, albeit at higher rates, when they likely would have been denied credit or received less credit under a one-price model.[14]

Risk-based pricing and the expanded reporting and automated risk assessment systems that made it possible have been an important enabling factor in the substantial expansion in credit discussed in an earlier chapter. It has also expanded access to credit for many consumers. In 1970, only 2 percent of households in the lowest income quintile had a bank type credit card. By 2001, 38 percent of the lowest income quintile had at least one bank type card, a level of

---

[10] AnnaMaria Andriotis, 'Flying Blind Into a Credit Storm': Widespread Deferrals Mean Banks Can't Tell Who's Creditworthy, The Wall Street Journal, July 8, 2020.

[11] Gary G. Chandler, Generic and Customized Scoring Models: A Comparison, in *Credit Scoring for Risk Managers: The Handbook for Lenders*, Elizabeth Mays, Ed., (Mason, OH: Thomson/Southwestern, 2004).

[12] Gary G. Chandler and Lee E. Parker, Predictive Value of Credit Bureau Reports, 11 *Journal of Retail Banking* 47 (1989).

[13] Peter McCorkell, "The Impact of Credit Scoring and Automated Underwriting on Credit Availability," in Thomas A. Durkin and Michael E. Staten, eds., *The Impact of Public Policy on Consumer Credit (*2002).

[14] For an extended discussion of the benefits of sorting consumers by risk, see Michael Staten, Risk-Based Pricing in Consumer Lending, 11 J.L. Econ. & Pol'y 33 (2015).

ownership that persisted until the beginning of the financial crisis.[15] Moreover, risk-based pricing "led to a broader array of loan products available to all risk and income groups."[16]

Risk-based pricing obviously results in different prices for different consumers. That is both equitable and efficient, because it maximizes consumer welfare as judged by consumers. A fundamental principle of economic efficiency is that those who create costs must pay them. If not, they will create excessive costs that impair economic performance. It is both equitable and efficient that teenage males pay higher auto insurance premiums than teenage females or older men – they are higher-risk drivers.

The same principles apply in credit markets. Some consumers manage their financial obligations responsibly and pay their bills on time. Others borrow more than they can afford, and in the end, default. Because default rates differ, it costs more to provide loans to some consumers than to others. In efficient markets, prices will reflect those cost differences, which also create incentives for higher risk borrowers to improve their financial performance. This arrangement is beneficial for both lower-risk and higher-risk borrowers. Low-risk borrowers get credit on better terms than they would pay if the lender is constrained to offer a single price and clearly benefit. There is no reason that good credit risks should be expected to subsidize the choices made by those who are less likely to repay their debts.

The benefits to responsible, lower-risk borrowers were substantial as risk-based pricing emerged. The percentage of outstanding balances on credit cards with an APR greater than 18 percent fell from 70 percent in 1990 to 44 percent just four years later.[17] The lowest-risk customers enjoyed discounts of 8 percentage points on their APR.[18]

Higher-risk consumers also benefitted, from greater access to credit. A study of a subprime auto finance company that adopted risk-based pricing found that, for the lower-risk subprime borrowers, required down payments changed little, and loan size and car quality both increased.[19] Down payment requirements increased, however, for the highest risk group, resulting in smaller loans and lower default rates.[20]

---

[15]See Durkin, Elliehausen, Staten, and Zywicki, Consumer Credit and the American Economy, Table 7.4, at 303. For all cards, 42.9 percent of those in the lowest income quintile had at least one card. Kathleen W. Johnson, Recent Developments in the Credit Card Market and the Financial Obligations Ratio, Federal Reserve Bulletin, Autumn 2005, at 475. As discussed in Chapter 10, the CARD Act has reduced card ownership among higher risk groups.

[16] See Wendy Edelberg, Risk-Based Pricing of Interest Rates on Consumer Loans, 53 *Journal of Monetary Economics* 2283 (2006).

[17] See Staten, supra note __, at 43.

[18] Mark J. Furletti, Credit Card Pricing Developments and Their Disclosure (January 2003). Federal Reserve Bank of Philla Payment Cards Center Discussion Paper No. 03-02 (2003), Available at SSRN: [HYPERLINK "https://ssrn.com/abstract=572585" \t "_blank"] or [HYPERLINK "https://dx.doi.org/10.2139/ssrn.572585" \t "_blank"]

[19] Liran Einav et al., The Impact of Credit Scoring on Consumer Lending, 44 RAND J. ECON. 249 (2013)

[20] org/articles.php?doi=10.1257/mac.4.3.153. 33 William Adams et al., Liquidity Constraints and Imperfect Information in Subprime Lending, 99 AM. ECON. REV. 49 (2009).

Credit reporting is fundamentally an information system. It depends on the ability to share sensitive financial information without the consumer's consent, because allowing consumers a choice would significantly undermine the system's ability to assess risk. To be sure, credit reporting information is sensitive, and it should be protected. Since 1970, requirements have been in place under the Fair Credit Reporting Act requiring use of "reasonable procedures to assure maximum possible accuracy," and to restrict use of credit information to a specified list of permissible purposes. This is a fundamental privacy protection statute, but with a very different approach than what is currently in vogue.

The Fair Credit Reporting Act has allowed expansion of credit reporting with very little regulation of the content of a report. Any information with a demonstrated relationship to the likelihood of repayment is relevant and should be permitted. More and better information can enhance risk assessment and enable more efficient credit markets to the benefit of all consumers. "Flying blind" is not a solution.

B. Transaction Cost Economics

If privacy is seen as a matter of controlling the flow of information about an individual, the costs of exercising control are a key consideration. Transactions costs are important even when markets are perfectly competitive and consumers are fully informed, because the cost of engaging in a transaction may be too large to justify the transaction in the first place. If rearranging an investment portfolio would produce gains of a one percent higher return, but the costs of the rearrangement amount to 1.1 percent, engaging in the necessary transactions is simply not worth the cost.

Any transaction involves costs: Consumers must decide to pay attention to the decision, evaluate their alternatives, make a decision, and execute that decision. Transactions costs also include the costs of negotiating a deal in many instances. Some transactions costs are direct and explicit, as with the commission paid to a real estate agent or the fee for trading in a brokerage account. But all transactions have costs, which may preclude transactions that would make both parties better off if there were no transactions costs.

Many legal institutions essentially seek to reduce transactions costs. Despite the costs of administering and enforcing contracts, contract law that enables parties to make enforceable promises is much less costly than alternative means of assuring that a promise is kept. Although various market mechanisms create incentives for complying with contractual obligations,[21] in many instances contracts are not self-enforcing. When disputes arise between commercial parties, private contract enforcement generally provides adequate remedies. In consumer markets, however, the high costs of private enforcement may result in no effective remedy for practices that cause a small harm to a large number of individuals. In such cases, there is a critical role for government action to enforce consumer rights.

[21] See Benjamin Klein. and Keith B. Leffler, "The Role of Market Forces in Assuring Contractual Performance," 89 *Journal of Political Economy* 615-641 (1981).

Much of contract law is designed to reduce transactions costs. For example, the law specifies default contract terms in certain circumstances. If these defaults are what most parties would prefer, they reduce transactions costs, because there is no need to negotiate over those terms. If they prefer otherwise, however, the parties can negotiate a different arrangement.[22]

In contracts, the parties are in contact with each other. Transactions costs are therefore likely to be relatively low in general, because the parties can negotiate.[23] In contrast, in other situations, transactions costs are quite high. There is, for example, no way for the parties who may eventually be involved in an auto accident to negotiate the terms of engagement when they meet at an intersection. Nor is there a practical way for consumers to negotiate the details of safe product design, whether it is for automobiles or toasters. Instead, tort law imposes duties on drivers regarding how they should behave and on manufacturers to avoid producing defective products.

The choice between contract and tort approaches to a particular problem is one in which transactions costs, relative to what is at stake, are crucial. If transactions costs are low, compared to the choice at issue, contract law is an appropriate approach, because it leaves the parties free to negotiate the arrangement that is best for them. When transactions costs are high, compared to the choice at issue, tort law and the imposition of legal duties is a more appropriate approach. The stakes are high in an automobile accident case, but the transactions costs of negotiations to minimize the costs of accidents are even higher.

Substantive consumer protection requirements, such as restrictions on default remedies, are tort-like requirements imposing specific duties on sellers or lenders. They are appropriate where transactions costs significantly impair the ability to negotiate a contract. Because they do not allow alternative approaches, such requirements must be used with care to ensure that they create benefits that consumers value in excess of the potential costs of the restriction.

II. The Current Approach to Privacy Regulation

A. The Limitations of the Fair Information Practices[24]

When Congress adopted the privacy provisions of the Gramm Leach Bliley Act (GLBA), it adopted an approach to privacy that grew out of the Fair Information Practices ("FIPs) adopted in 1973[25] and is fundamentally rooted in disclosure. The starting point of FIPs is notice – consumers should be told what information is being collected about them and how it is being used. A second principle is choice; consumers should be able to control how information is

---

[22] This arrangement also imposes the transactions costs on the parties who benefit from them.

[23] With standard form contracts, "negotiation" takes the form of shopping elsewhere.

[24] For a fuller discussion of the limitations of the Fair Information Practices, see J. Howard Beales, III & Timothy J. Muris, Choice or Consequences: Protecting Privacy in Commercial Information, 75 U. CHI. L. REV. 109 (2008).

[25] 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 [HYPERLINK "http://www.epic.org/privacy/hew1973report"].

used. Third, the access and correction principle states that consumers should be able to see information about them and correct any inaccuracies. Fourth, those who have consumer information must take steps to secure that information and protect it from unauthorized disclosure. Fifth, the onward transfer principle maintains that information should only be used for the purpose for which it was originally collected; additional information uses would require additional authorization from the consumer. There are other principles, but these are the most important ones.

Under GLBA, financial institutions must adopt privacy policies addressing their practices regarding information use and provide those policies to consumers. In theory, consumers will read the policies of their institution, compare them to the policies of competing financial services providers, and choose the institution with the privacy practices that best match their own privacy preferences. Consumers have a limited right to "opt out" of certain information sharing, primarily third-party marketing, but important information sharing for purposes such as credit reporting and fraud control is explicitly permitted without consent.

The FIPs approach as implemented in GLBA is at its heart a property rights approach to personal information. It regards personal information as the consumer's "property," although U.S. law has never considered it as such. It is a peculiar form of property, to say the least. You may regard you ZIP code as "yours," but it also likely belongs to tens of thousands of others. Nevertheless, under the property rights approach, consumers can theoretically control how this particular property is used.

From an economic perspective, information about interactions between consumers and companies is jointly produced, and not the result of either party's efforts alone. This is most apparent in a real estate transaction, where both parties know all of the relevant details of the transaction, and each has legitimate needs to use the information in various ways (not the least of which is filing taxes). There is no apparent reason why the information should "belong" to either the buyer or the seller alone, and no clear basis for deciding which should have control under a property rights approach.

There are substantial limits to the FIPs as an approach to privacy regulation. The concept of notice is simple enough, but the costs of actually using notices are out of all proportion to what might be at stake. A study of online privacy policies estimated that simply to read privacy policies on the websites a typical user encounters would take 244 hours – more than 10 days of around the clock reading. The estimated opportunity cost was $781 billion.[26] For most consumers, the issue is not worth thinking about, let alone the costs of considering the notices and making a decision. Moreover, a significant body of research finds that "consumers are comfortable with the type of data sharing involved in the day-to-day functioning of an ad-

[26] Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & POL'Y 543, 544 (2008). Simplification is not an answer. Even in the highly unlikely event that we could reduce the time needed to read a privacy policy by half, five days of round the clock reading remains grossly disproportionate to what is at stake.

supported online world."[27] As a result, the default rule prevails. If the default is that information can be shared unless consumers opt out, the usual rule on internet sites, most consumers will allow sharing. If the default is opt in, however, most consumers will still do nothing, but sharing will not be allowed. Decisions about organ donation are analogous. Most consumers do not devote attention to considering the issue, and a study of European countries with different default rules for organ donations finds that the default rule prevails.[28] In short, transactions costs leave the default rule in place, because few are willing to engage in the costs of making a decision.

As GLBA recognizes, choice must also be limited for certain information sharing. Credit reporting depends on the fact that consumers cannot choose not to have their financial performance reported. If they could choose, consumers with poor repayment histories would choose not to have their information shared, and the system would lose its ability to distinguish consumers based on risk – the asymmetric information problem would re-emerge. Similarly, the property recordation system, which enables potential lenders to determine whether there are liens or other claims against a particular property, depends on the absence of choice.

Allowing consumer access to the information can also be problematic, particularly if companies respond to requests for data without demanding sufficient identity verification. One researcher tested an experimental attack, with the co-author victim's consent, using only publicly available information about the victim to request access under the EU's General Data Protection Regulation's (GDPR) right of access. Requests were sent to 150 organizations with whom the victim might have had a relationship, but without knowing whether a relationship actually existed. No documents were falsified, but some legitimate documents were submitted with key information hidden. In the sample, 72 percent of the organizations handled the request, and approximately two thirds of them responded in a way that confirmed that a relationship existed with the victim, including an online dating service. Of those who had information, approximately one quarter provided information without verifying identity. An additional 15 percent requested easily falsifiable forms of identification, such as a signed statement swearing to be the subject. In all, there were 60 distinct instances in which information was obtained. The information included online dating profiles, previous addresses, detailed purchase histories, a complete record of all rail journeys over several years, all hotel stays with a particular chain, and a complete social security number. Various organizations provided portions of the victim's credit card information, so that at the end of the experiment the attacker knew 10 digits of the account number, the expiration data, the issuing bank, and the victim's postal code. A threat intelligence firm provided a list of previously breached user names and passwords, which

[27] James C. Cooper, and Joshua D. Wright, The Missing Role of Economics in FTC Privacy Policy (January 5, 2017). Cambridge Handbook of Consumer Privacy, Jules Polonetsky, Evan Selinger & Omer Tene, eds., Cambridge University Press (2017), Available at SSRN: [HYPERLINK "https://ssrn.com/abstract=2894438" \t "_blank"]

[28] Eric J. Johnson & Daniel Goldstein, *Do Defaults Save Lives?*, 302 SCI. 1338 (2003)

worked on at least 10 online accounts, including an online banking service.[29] Clearly, access rights can create significant risks to consumers.

Of course, those who possess consumer information can be encouraged, or required, to obtain better identifying information before granting access. That, however, may require the collection of more information about the consumer in order to assure accurate identification. The fraud control tools discussed later in this chapter, for example, generally require detailed information about the consumer to determine the risk of a transaction, whether it is a financial transaction or a transaction granting access to a particular person.

Depending on its scope, the right to correct information can also pose risks. For example, a database of information used in previous cases of known frauds reduces the risk that a person whose information was used is victimized again. The person with the greatest interest in "correcting" the information is the thief who used it and would like to use it again. Similarly, a database of names and social security number combinations that have been used in previous instances of identity theft may be quite useful in preventing additional frauds. If one person's name was previously used in connection with a different person's social security number, however, from the point of view of either person, that record is a mistake. "Correcting" the information, however, undermines the value of the database in reducing fraud.

B. Ambiguity about Consent

The premise of FIPs is that the consumer gives consent for certain uses of information. Often, however, the nature and scope of consent may be ambiguous. That has been the case in many of the Federal Trade Commission's (FTC) enforcement actions involving negative option plans, where consumers may not be aware they are signing up for a recurring transaction that will continue until cancelled. It was concerns about the adequacy of consent that led the FTC to require telemarketers to obtain the last four digits of the consumer's account number directly from the consumer when they already had the account number and the offer included a negative option feature.

The scope of consent was a source of concern in the early information aggregator models, which obtained access to the consumer's financial information by obtaining the account credentials such as username and password. That "consent" could lead to far broader access to an account than the consumer intended, with potential for adverse consequences. The development of an applications programming interface that gives more nuanced assess to the needed information has greatly reduced this potential problem.

There is an inherent tradeoff between the quality and clarity of consent on the one hand, and convenience on the other. If each transaction in a series is separately authorized, there is less room to question that consent was given. But authorizing a repeated billing for a series of transactions, even when the details of those transactions are not yet specified, is far more

[29] James Pavur and Casey Knerr, GDPArrrrr: Using Privacy Laws to Steal Identities, Blackhat USA 2019 Whitepaper, available at [HYPERLINK "https://i.blackhat.com/USA-19/Thursday/us-19-Pavur-GDPArrrrr-Using-Privacy-Laws-To-Steal-Identities-wp.pdf"].

convenient. Auto-shipped merchandise from Amazon or other retailers is far simpler and for many greatly preferable to placing each order separately. Certainly, few want to enter all of their credit card information every time they visit Amazon, although doing so reduces any possible ambiguity about consent. Even when the details of future transactions are unknown, as with a dry cleaner who picks up and delivers the laundry and processes the charges through a card on file, the convenience of not having a separate bill to deal with outweighs any uncertainty about what they have agreed to for many consumers.

Potential ambiguities about whether consent was given are likely to grow with the spread of radio-frequency identification (RFID) enabled devices connected to the internet, the so-called internet of things ("IoT"). Some have estimated there will be 31 billion IoT devices by the end of 2020.[30] A "smart" refrigerator that can prepare a shopping list when stocks run low would be a great convenience, without raising consent issues. But it would be even more convenient if the appliance could order needed goods and they would appear on your doorstep.[31] Clearly, a consumer must agree to this arrangement. It is not clear, however, that there is a practical way to grant consent for each individual transaction, leaving some ambiguity about whether any individual transaction was actually authorized.

C. Recent General Privacy Regulation and its Effects

Two privacy laws based on the property rights approach have recently taken effect. The European Union's General Data Protection Regulation ("GDPR") effective on May 25, 2018, has been in place long enough for some early assessments of its impact to have emerged. More recently the California Consumer Privacy Act ("CCPA") took effect on January 1, 2020, and enforcement began on July 1, 2020. Compliance with the GDPR was a major undertaking for companies that operate in the EU, as it is for the far more numerous U.S. companies that must comply with the CCPA. Although there are important differences, the two laws have fundamental similarities in their approach.

Of course, the GDPR requires notice of what information is collected and how it will be used. Data cannot be used for purposes that were not included in the original notice without obtaining additional consent. The notice must also include notice of the consumer's ("data subject") rights under the GDPR. With certain exceptions, controllers must obtain affirmative, informed and freely given consent to use personal data. This is, in essence, an opt-in requirement. Probably the most important exception is that if the consumer requests a specific action, such as placing an order, the controller can use the information to the extent necessary to complete that request. However given, consent for further use of the data can be withdrawn at any time. Consumers also have the specific right to object to the use of information for profiling, for direct marketing, or for research purposes. The GDPR includes data minimization requirements; data can only be used to the extent it is "necessary." Data subjects have the right

[30] [HYPERLINK "https://securitytoday.com/articles/2020/01/13/the-iot-rundown-for-2020.aspx" \l ":~:text=In%202018%E2%80%94there%20were%207,of%2031%20billion%20IoT%20devices"]

[31] Avi Itzkovitch, The Internet of Things and the Mytical Smart Fridge, UX Magazine, Sept. 18, 2013, available at [HYPERLINK "https://uxmag.com/articles/the-internet-of-things-and-the-mythical-smart-fridge"].

to examine and correct the information a data controller holds about them. They also have the right to have information about them deleted and the right to data portability.

The CCPA has similar notice requirements, but with differences in the specific information required as well as the requirements for how motive is delivered. Consent under the CCPA, however, differs significantly. Affirmative informed consent is not generally required, but consumers have the right to opt out of the sale of information to third parties, with certain exceptions. Websites must include a clear and conspicuous "Do Not Sell my Personal Information" link on the home page. A consumer who opts out cannot be asked to reauthorize information use for 12 months. Opting out of the sale of information is the consumer's only option; there is no specific right to object to certain uses. CCPA's right of access and right to deletion is similar to the GDPR, but the CCPA provides broader grounds for a business to refuse to delete data. Unlike GDPR, CCPA has no right to correct or complete data. Data portability requirements are similar in the two regimes.

Because the GDPR became effective in 2018, studies of its impact have begun to emerge. Early studies find significant adverse effects. A study of venture capital financing of EU-based businesses found significant declines after GDPR took effect. Between May 2018 and April 2019, overall venture funding for EU tech firms fell $14.1 million per month per member state. The number of deals fell 26 percent, and the average amount raised per deal fell 34 percent. Effects were greater for "new" ventures (those three years old or less) and for businesses that were "more data-related."[32] A study based on data from Adobe Analytics, the number-four provider of data analytic services, found that recorded page views fell 9.7% and visits fell 9.9% after GDPR took effect. Among e-commerce sites, orders fell 5.6% and revenue fell 8.3%, or $8,000 per week for the median site.[33] The authors suggest that at least part of this decline was because of less effective marketing, because many visits follow clicking on a display ad or an email link. A study using data from an intermediary that collects consumer search queries and purchases across most major online travel agencies found a 12.5% decline in the number of consumers observed. In the context of auction markets for online search advertising, where advertisers bid for words included in the consumer's search to trigger their advertisement, the revenue loss was offset by the fact that the remaining consumers had higher value to advertisers, because their tracking history was longer.[34]

To date, all of the observed effects of GDPR are short run effects. Over time, firms will surely learn how best to live with the new regulatory regime, in ways that will likely attenuate its

---

[32] Jia, Jian and Jin, Ginger Zhe and Wagman, Liad, The Short-Run Effects of GDPR on Technology Venture Investment (November 8, 2019). Available at SSRN: [HYPERLINK "https://ssrn.com/abstract=3278912" \t "_blank"] or [HYPERLINK "https://dx.doi.org/10.2139/ssrn.3278912" \t "_blank"].

[33] Goldberg, Samuel and Johnson, Garrett and Shriver, Scott, Regulating Privacy Online: The Early Impact of the GDPR on European Web Traffic & E-Commerce Outcomes (July 17, 2019). Available at SSRN: [HYPERLINK "https://ssrn.com/abstract=3421731" \t "_blank"] or [HYPERLINK "https://dx.doi.org/10.2139/ssrn.3421731" \t "_blank"].

[34] Guy Aridor, Yeon-Koo Che, and Tobias Salz. The Economic Consequences of Data Privacy Regulation: Empirical Evidence from GDPR, NBER Working Paper No. 26900 (March 2020).

adverse impacts. Although the long run effects may be reduced, their elimination is unlikely. If there were better ways to market than the pre-GDPR approaches, firms had every reason to adopt them. The significant adverse effects to date strongly caution against modeling U.S. privacy regulation on the GDPR, and there is little reason to believe the effects of the CCPA will be significantly better.

D. The Competitive Consequences of Privacy Regulation

Data are the essential raw material of the information economy. In an economy that is increasingly driven by machine learning and artificial intelligence, access to data is the sine qua non of competitive advantage. Whether it is humans or machines seeking to extract knowledge from data, the data itself are key.

The quality of the knowledge that can be extracted depends on several characteristics of the underlying data. It depends on the volume of data; more information is generally better. Data variety is also important; diverse information sources likely increase the knowledge that can be gained. The veracity of data is critical; inaccurate or unreliable data are not likely to yield useful insights.[35] Finally, in many applications the freshness of data is important; stale data may generate "insights" that are no longer correct.[36]

Because data are valuable, companies that have data have an incentive to maintain control. Data that allow better assessment of credit risk, for example, may also allow competitors to identify and target an institution's best customers. Credit reporting agencies [redacted] combat this incentive by requiring many institutions to contribute data as a condition for purchasing data or for purchasing data at a favorable price. Nonetheless, declining to share information has been an issue from time to time, as some furnishers have strategically withheld certain information.[37] Strategically withholding information generally impairs competition, and harms consumers.

Privacy concerns, real or imagined, offer another rationale for withholding valuable information to obtain competitive advantage. For example, Apple is planning changes to its iOS that will require additional consumer consent before apps can share the identifier for advertisers ("IDFA," also known as Mobile Ad ID or "MAID"), widely used in the advertising industry to identify a particular device for purposes of tracking browsing behavior and measuring advertising effectiveness. The change will reduce the competitive appeal of using advertising placed through Google, Facebook, and other non-Apple providers, who will have less information about the user to target advertising, and enhances the appeal of advertising purchase

[35] A persistent problem in machine learning is that algorithms developed using biased data sets will likely faithfully reproduce the biases in the original data.

[36] See Michael S. Gal and Oshrit Aviv, The Competitive Effects of the GDPR, Journal of Competition Law and Economics (forthcoming, 2020), [HYPERLINK "https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3548444"].

[37] For example, for a period of time Capital One was not reporting a customer's credit limit to credit reporting agencies, because it feared undercutting a proprietry risk management system that it saw as a business advtantage. See Lenders Faulted for Giving Incomplete Credit Picture, Los Angeles Times, July 30, 2003.

through Apple, which still has access to the data.[38] One industry participant thought there was "probably 30 percent truth in that they're doing it for privacy reasons, and it's 70 percent that they're doing it because it's what's good for Apple."[39]

Of course, companies can choose to compete based on their ability to satisfy consumers' privacy preferences, and doing so will benefit the company as well. That may be Apple's objective. Apple has also called for privacy regulation that would impair the ad-supported model of its key competitors far more than it would impact Apple's own subscription and sales-based model.[40] Regulatory requirements based on claimed privacy concerns, however, rather than privacy preferences revealed in the marketplace, are an attempt to secure from government advantages that consumers are unwilling to bestow.

Similarly, privacy regulatory requirements can create artificial competitive advantages. By far the largest players in the online advertising marketplace are Google and Facebook, in large part because users sign in to use their services. Sign-in enables these companies to collect substantial amounts of information. Third-party competitors use tracking cookies to obtain much of the same information by building networks of website publishers, which allow these firms to obtain information about browsing at all sites in the network (and, by cross matching the cookies, about browsing on other networks as well). An early study after the GDPR went into effect found that there were significant declines in the number of websites that smaller vendors could observe, but that Google's reach increased.[41] Both Google and Facebook had revenue growth greater than the European digital advertising market growth, implying increases in their market share.[42] Researchers have also found that GDPR increased concentration among the technology vendors who provide services to websites.[43]

These adverse effects on competition arise for a number of reasons. First, theoretical work indicates that the transactions costs of obtaining user consent disproportionately affect smaller and more specialized firms, thus favoring firms that are both larger and provide a broader

---

[38] John Koetsier, Apple Just Crippled IDFA, Sending an $80 Billion Industry Into Upheaval, Forbes, June 24, 2020.

[39] Nick Jordan, Founder of Narrative I/O, quoted in Reed Albergotti and Elizabeth Dwoskin, Apple makes a privacy change, and Facebook and advertising companies cry foul, The Washington Post, August 28, 2020.

[40] Ian Bogost, Apple's Empty Grandstanding About Privacy, The Atlantic, Jan. 31, 2019. [HYPERLINK "https://www.theatlantic.com/technology/archive/2019/01/apples-hypocritical-defense-data-privacy/581680/"].

[41] Bjoern Greif, Study: Google is the Biggest Beneficiary of the GDPR, Ghostery.com (October 10, 2018), available at [HYPERLINK "https://www.ghostery.com/blog/ghostery-news/study-google-is-the-biggest-beneficiary-of-the-gdpr/"].

[42] Nick Kostov and Sam Schechner, GDPR Has Been a Boon for Google and Facebook, The Wall Street Journal, June 17, 2019.

[43] Johnson, Garrett and Shriver, Scott and Goldberg, Samuel, Privacy & Market Concentration: Intended & Unintended Consequences of the GDPR (July 8, 2020). Available at SSRN: [HYPERLINK "https://ssrn.com/abstract=3477686" \t "_blank"] or [HYPERLINK "https://dx.doi.org/10.2139/ssrn.3477686" \t "_blank"]

array of services.[44] Second, users of data are potentially liable under the GDPR for violations by the firm that collected the data, and firms may be more willing to trust the compliance efforts of large companies such as Google and Facebook than they are smaller vendors.[45] Third, there have been allegations that Google used an unnecessarily strict interpretations of GDPR to impose restrictions on its vendors and users of its advertising systems. Google's consent tool, for example, limited publishers to a maximum of 12 ad tech vendors, where many had previously used more.[46] Finally, consumers may simply be more willing to grant consent to well known, consumer-facing companies, and less likely to agree to share with the behind-the-scenes advertising technology companies that are almost universally unknown to consumers.[47]

Of course, privacy concerns may be legitimate. When information aggregators began offering their services by obtaining the consumer's credentials and essentially "scraping" information from the website of the financial service provider, they were circumventing the bank's security measures to provide their service to consumers. These concerns have been largely resolved by the development of an Application Programming Interface (API), which give information aggregators sanctioned access to the bank's information with proper consumer authorization. Banks were legitimately concerned, but they also stood potentially to benefit from protecting detailed information about their customers. When privacy concerns are raised as a rationale for restricting information sharing, regulators should evaluate not only the potential privacy benefits of any restrictions, but also consider the potential for adverse competitive consequences, which will inevitably harm consumers.

In significant part, the potential for anticompetitive consequences of privacy regulation stems from the distinction between "first parties," who collect information directly from consumers, and "third parties," with whom that information may be shared. First parties typically have broad permission to use the data as they see fit, but there may be numerous restrictions on sharing information with third parties.

There is no clear privacy difference between the two scenarios. Privacy problems would intensify, not disappear, if all information were collected by a single first party but never shared. Nor is it clear that sharing creates any new or unique privacy risks. When information is shared by granting access to a centralized data source, for example, there may not even be another copy of the information that could constitute another target for hackers. Instead, there is simply another access point in a network that likely has many such access points, with or without sharing. First parties and third parties alike may fail to take adequate steps to secure data,

---

[44] James David Campbell, Avi Goldfarb, and Catherine E. Tucker, *Privacy Regulation and Market Structure*, 24(1) JOURNAL OF ECONOMICS & MANAGEMENT STRATEGY 47 (2015).

[45] See Gal and Aviv, supra note __.

[46] [HYPERLINK "https://www.adexchanger.com/online-advertising/googles-gdpr-consent-tool-will-limit-publishers-to-12-ad-tech-vendors/"] (May 3, 2018). See also Jessica Davies, 'The Google Data Protection Regulation': CDPR is strafing ad sellers, Digiday (June 4 2018), available at [HYPERLINK "https://digiday.com/media/google-data-protection-regulation-gdpr-strafing-ad-sellers/"].

[47] For example, the first four members of the Network Advertising Initiative, an industry self-regulatory group, are 33Across, Acuity, Adara, and Add This, none of which are household names.

creating harm to consumers. Similarly, first parties or third parties may use information in ways that are harmful to consumers, but the concern is with the use, and not the fact of sharing. Regulatory burdens on sharing may simply increase the costs of obtaining the information needed to provide valuable services to consumers.

The economic question is the most efficient way to organize the information economy in a way that allows each company to obtain the information necessary for competitive success. If a use of information by a "first party" is a useful practice that benefits consumers, it does not become any less useful, or create any more of a risk to privacy, if the most efficient way to produce those benefits is to share the information with a "third party" who actually does the analysis. Instead, the goal should be to maximize the ability of the cooperating parties to exploit their competitive strengths and minimize costs to consumers. Restrictions on sharing create incentives for "first parties" to collect more information than they might otherwise, rather than obtaining the information from some other party who can collect it more efficiently. Such restrictions may degrade the quantity and quality of information available and increase the costs of obtaining necessary information.[48] Neither outcome is good for consumers.

Restrictions on information sharing may also reduce the amount of information collected, again with the potential for adverse consequences for consumers. Lenders have an obvious incentive to screen potential borrowers to assess risk and deny loans to borrowers who are too risky. An additional incentive to screen borrowers, however, is the possibility of profiting from other uses of the information, such as marketing related services. If lenders cannot use the data for such purposes, they may collect less data in the first place. As a result, lenders will be less able to assess risk. To prevent increasing losses, they will deny more loans initially. In essence, rather than gathering more information to assess marginal applicants, they may simply deny credit, because gathering information is less valuable if it cannot be used for other purposes.

As noted above, the federal Gramm Leach Bliley Act established an opt-out rule for information sharing – institutions can ~~could~~ share data unless consumers told them not to do so. In 2002, however, several local governments in the San Francisco Bay area adopted opt-in requirements, prohibiting further use of the data for marketing without the consumer's express consent. (California eventually adopted this approach statewide, effective in 2004.) With less incentive to gather information, denial rates for mortgage loan applications increased, for both purchases and refinancing, in jurisdictions that adopted opt-in requirements compared to those who did not. Moreover, as the financial crisis began to unfold in 2007 and 2008, foreclosure start rates were higher in counties with the opt-in requirement.[49]

III. Privacy Regulations Should Reduce Harms by Focusing on the Consequences of Information Use

[48] See Gal and Aviv, supra note __, for a discussion of the potential impacts of privacy regulation on industrial organization and the choice between internal collection and sharing.

[49] Jin-Hyuk Kim and Liad Wagman, Screening incentives and privacy protection in financial markets: a theoretical and empirical analysis, 46 RAND J. Econ. 1-22 (2015).

A. Regulation Based on Consequences

The first federal privacy statute was the Fair Credit Reporting Act, passed in 1970. It established a regulatory scheme to govern the credit reporting industry that has stood the test of time (albeit with numerous amendments along the way) and preserved and expanded an important information source for financial services firms.

Although the statute includes elements of the fair information practices, it takes a very different approach to privacy regulation than does the GDPR or the CCPA. Most prominently, it allows information sharing without the consumer's consent, which, as discussed above, is an essential element of the credit reporting system. Instead, it restricts the uses of credit reports to a narrow list of permissible purposes. Moreover, it directly addresses a principal source of adverse consequences of credit reporting for consumers, requiring "reasonable procedures to assure maximum possible accuracy." Allowing consumers access to their credit reports, providing notice when a credit report is the basis for an adverse action, and allowing consumers to dispute information in their report are other important elements to assure credit reporting information is accurate. But the focus is on the problem of assuring accuracy, not the process by which information is initially gathered.

The privacy policies that are the foundation of the current approach to privacy regulation are surely the epitome of information overload, discussed in Chapter 7. Rather than protecting consumers from possible problems, they rely on consumers to read and understand legalistic descriptions of the complex, technical information flows that are central to the information economy – and then take steps to protect themselves. It is, in essence, a contract-based approach to privacy, with the parties theoretically bargaining about what information practices are acceptable. Applied to automobiles, this approach would let manufacturers produce any car they wished, as long as they disclosed all of the technical specifications. This is not consumer protection, it is caveat emptor in the extreme.

Rather than relying on a contractual approach to privacy, an approach based on tort law would be more protective of both privacy and consumers. The risk of potential privacy problems such as data security breaches are relatively remote, which suggests that consumers may have little reason to consider them carefully. The problem is similar to products liability, in which consumers are unlikely to invest in information about the benefits and costs of a relatively remote risk of a serious product failure.[50] Imposing tort liability on product manufacturers is a more sensible solution.

Applied to privacy, a tort approach would impose substantive regulation on holders and/or users of information to prevent harm to consumers. A consequences-based approach to privacy regulation leads immediately to the relevant question: what is the impact of a particular use of information on consumers? The reason we care about commercial information use or sharing is that something bad might happen to consumers, and the goal should be to avoid those adverse consequences. There is little reason for concern when using information benefits

[50] See Richard Posner, Economic Analysis of Law, Section 6.6.

consumers, as it does when information is used to process a transaction or when information collected for a different purpose is used to reduce the risk of fraudulent transactions. There are legitimate concerns when information is used in ways that harm consumers, but the focus should be on controlling harmful uses of information, rather than trying to control the information itself. Regulation should seek to protect consumers, rather than protecting data.

Harms may be economic, as with identity theft or inaccurate information in credit reports. In some instances, harms may be physical, and relatively small disruptions to large numbers of consumers may constitute an actionable harm. Harms certainly include the recognized privacy torts of harm to reputation, intrusion on a private place, or spreading intimate details before the public, which all require conduct that "would be highly offensive to a reasonable person."[51]

Of course, some consumers may want privacy protection that goes beyond preventing concrete harms. In many instances, those concerns have not been articulated with any specificity, making policies to reduce the harm very difficult to develop. Moreover, specific concerns may vary widely from person to person, again making a regulatory response difficult. Some, for example, may simply consider certain uses of information "creepy," as with Target's algorithm used to identify pregnant women for marketing purposes based on their other purchases.[52] Others may greatly value the discounts for newly-relevant products that resulted from the use of the information. Because no company wants to offend its customers, Target adjusted its marketing practices to reduce consumer unease, but continued to use the algorithm. The ability to opt out of certain information uses or information sharing allows those with particularized privacy preferences to protect them, without imposing significant costs on those who do not share their concerns. It is therefore a valuable safeguard for those with possible intense, but idiosyncratic preferences.

Privacy harms do not depend on the consumer's state of residence. They are the same, wherever the consumer lives. There is therefore little benefit in allowing states to customize their privacy requirements. There are, however, significant costs, particularly for online commerce, if companies must comply with a patchwork of inconsistent requirements. Like the Fair Credit Reporting Act, the central provisions of a federal privacy law should be preemptive. That is especially so because sharing information about, for example, California consumers may allow the development of better tools for important functions that benefit consumers in Massachusetts as well.

---

[51] Restatement (Second) of Torts § 652B (1977) (intrusion upon seclusion); id. § 652D (publicity given to private life); id. § 652E (publicity placing person in false light).

[52] See Kashmir Hill, How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did, Forbes, Feb. 16, 2012. Available at [HYPERLINK "https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/" \l "1992aa3b6668"].

Data breach notification laws are a case in point. All 50 states have such laws, plus the District of Columbia, Guam, Puerto Rico, and the Virgin Islands.[53] States differ in what information is considered protected and in the entities who must give notice. "State laws differ not only in the types of data breaches they regulate, but also in who, what, when and how they require companies to notify their customers."[54] States also has differing "triggers" for when a breach must be disclosed, ranging from when unauthorized "acquisition" to unauthorized "access" to either one. The need to understand and apply these various requirements raises obvious compliance difficulties for a national organization, with little obvious benefit to consumers. Nor is the objective clearly specified. If the objective is to provide actionable information for consumers, the scope of breaches that require disclosure should be limited to ones where there is some step consumers should take to reduce their risk; in many cases, there are no such steps and notice serves little purpose. Broader disclosure runs the considerable risk that consumers will simply ignore all breach notifications, even when action is necessary. If the objective is public shaming of companies with inadequate security, far less costly public notice requirements could likely achieve the goal with lower compliance costs. In any event, there should be a uniform national standard that applies. To the extent that state laws have allowed experiments with different approaches, it is time for Congress to learn what can be learned from the experiments, and discard the experiments that failed.

Beginning in 2001, the FTC has used its authority to prohibit unfair or deceptive acts or practices to build a productive privacy protection program based on the consequences of information use and misuse. This approach led directly to the National Do Not Call Registry, and to the Commission's information security cases. The FCRA is an example of this approach, imposing duties on credit reporting agencies to limit the uses of information and to assure its accuracy. The resolution of privacy concerns about information aggregators through the development of an API is a non-regulatory example of the same principle: privacy requirements should seek to provide real protection from real problems, rather than relying on an obscure disclosure that some risk exists.

B. Benefits of Information Sharing

A substantive approach to privacy regulation must consider the costs and benefits of the uses of shared information. Some benefits are clear and straightforward; others are far more difficult to identify or quantify. For example, sharing information allows personalization and customization of websites to increase convenience and ease of use for consumers. That is an essential part of the business of information aggregators, which allow consumers to display information from a number of different financial service providers in a single display and format.

---

[53] [HYPERLINK "https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx"].

[54] Mark L. Krotoski, Lucy Wang, and Jennifer S. Rosen, The Need to Repair the Complex, Cumbersome, Costly Data Breach Notification Maze, Privacy & Security Law Report, 15 PVLR 271, 2/8/16, available at [HYPERLINK "https://www.morganlewis.com/~/media/files/publication/outside%20publication/article/bna-need-to-repair-data-breach-notification-maze-08feb16.ashx"].

One clear example of the benefits of information sharing is the credit reporting system, discussed above. The system enables better management of risk and extensions of credit to consumers who might otherwise be denied credit entirely.

Much of the internet content we all enjoy, and many valuable services such as email, cloud storage, and software, are "free" because they are supported by advertising. The revenue available from advertising in turn depends on information about the potential customer. A study of the effects of the EU's 2002 E-Privacy Directive found that reduced ability to target advertising reduced advertising effectiveness by 65%.[55] A study of auction markets for online advertising in the U.S. found that if a cookie was available with an impression, the price was roughly three times higher than if there was no cookie.[56] More recently, the UK's Competition and Marketing Authority on Online Platforms and Digital Advertising concluded that blocking third-party cookies would reduce short-run publisher revenue by 70 percent.[57]

Paradoxically, one crucial tool in the fight against fraud of all sorts and identity theft in particular is the ability to share sensitive information. Controlling identity theft requires that the company considering an extension of credit have access to more information about the real person than the thief. That allows the company to determine whether the transaction is likely legitimate or fraudulent.

Given the information available, any attempt to detect and prevent fraud confronts an inherent tradeoff between false positives and false negatives. False positives occur when a potential transaction is mistakenly identified as potentially fraudulent. Consumers are likely to be contacted for additional information, and their transaction may be delayed. False negatives occur when fraudulent transactions are mistakenly approved. Merchants or financial institutions suffer financial losses, and consumers may find themselves victims of identity theft. The only way to reduce both false positives and false negatives is to obtain more and better information, which is the key to better predictions of the risk of fraud.

A wide variety of information-based products help financial institutions and others identify, and in some cases quantify, the risk that a proposed transaction is fraudulent. The most straightforward such tool is fraud data bases, which identify information that has been used in past fraudulent transactions. The Postal Service, for example, maintains a list of addresses that have been used in previous mail fraud cases. Other databases allow identification of addresses that are campgrounds or telephone numbers that are in prisons.

More sophisticated tools look for consistency in the way information is used across different transactions. Often, these products use information that was collected for completely

---

[55] Avi Goldfarb and Catherine Tucker, "Privacy Regulation and Online Advertising," 57(1) Management Science (2011), 51-71.

[56] J. Howard Beales and Jeffrey A. Eisenach, "An Empirical Analysis of the Value of Information Sharing in the Market for Online Content," published online by Digital Advertising Alliance, available at http://www.aboutads.info/resource/fullvalueinfostudy.pdf, January, 2014.

[57] Competition & Marketing Authority, Final Report on Online Platforms and Digital Advertising, Appendix F, at paragraphs 115-120 (July 1, 2020).

different purposes. Magazine subscription lists, for example, can help to identify an unusual combination of a name and address that may indicate increased risk that an application is fraudulent. Data on other transactions can similarly be used to check for consistency. Essentially, these tools use information from multiple sources to triangulate on the likelihood that a consumer is in fact who he or she claims to be.

Some products use information about past frauds to convert observed inconsistencies into a quantitative index of the risk of fraud, similar to credit scoring models. Still other approaches pool information from applications to search for unusual patterns across applications that may indicate fraud. For example, multiple applications in a short period of time listing the same workplace and telephone number may indicate that something is amiss.

Generally, these tools are used as the basis for requesting additional identifying information, rather than simply refusing the transaction. Users must develop their own criteria to balance the risk of false positives and false negatives. False positives may be particularly costly to the entity using the tool, because they will often trigger the need to request and process additional information.

Fraud control tools are only one example of benefits from secondary uses of information originally collected for a different purpose. Credit reporting itself is a secondary use of information; financial institutions maintain records of payment histories for their own business reasons, not for purposes of credit reporting. Strict application of the notice and choice approach to privacy regulation, however, frowns upon secondary uses unless they were disclosed at the time the information was originally collected. In some instances, this may not be possible, because the secondary use may have been discovered later.

We all benefit from many secondary uses of information. Location information that is used to monitor traffic patterns is a clear and familiar example. Using the same information to measure the extent of compliance with lockdown orders during a pandemic is another, more recent example. It is difficult to see a significant risk of harm in these instances. Using location data to locate a particular individual in real time is far more problematic, but that use of information can be specifically restricted, as can government access to the data.

Secondary uses of data are likely to grow with the expansion of the internet of things. As more and more devices are connected to the internet and communicate data relevant to their function to various entities, it seems almost inevitable that clever entrepreneurs will discover other insights that can be gleaned from the data, in ways that are almost impossible to predict. Machine learning and artificial intelligence almost always benefit from additional data, regardless of the original purpose for which it was collected. The growing use of these technologies will inevitably spur continuing searches for useful data.

There are, of course, risks in sharing information as well. Foremost among them is the risk that data will be compromised and used in ways that facilitate frauds than harm consumers. The task of sensible privacy regulation is to identify the potential harms and determine which solutions can best reduce the harm without compromising important benefits of information sharing.

C. Information Security

One clear duty of those who hold consumer information is to protect it from data breaches. Financial regulators have adopted rules requiring information security pursuant to the Gramm Leach Bliley Act, and the Federal Trade Commission has a long series of cases contending that the failure to take security measures that are reasonable and appropriate in the circumstances is either a deceptive practice (if security claims are made) or an unfair practice.

Regulatory approaches to information security have been principles-based, rather than imposing specific requirements such as encryption or use of a particular technology. That approach is appropriate, because the security landscape is constantly evolving. The FTC's Safeguards Rule, for example, requires companies to assess the risks they face, take steps to reduce those risks that are reasonable and appropriate given both the size and sophistication of the business and the sensitivity of the information, monitor the environment both to identify new risks and assure the continued effectiveness of its program, and to adjust its security measures as necessary.

Information security choices necessarily involve tradeoffs, whether it is efforts to prevent fraudulent transactions or to protect stored information. If a fraud control system mistakenly declines a transaction, the costs fall on the consumer who initiated it. Those costs depend on the nature of the transaction. In an application, it may just be the need to provide additional information; in a credit card transaction, the consumer may be able to use a different card; in a debit card transaction the consumer may have no alternative but to abandon the attempted purchase. If a transaction is mistakenly approved, on the other hand, the costs most likely fall on the financial institution eventually, although sometimes significant costs may be imposed on consumers to restore their prior position, as in the case of identity theft. Users of fraud control systems must balance these potential costs.

As noted above, given the information available, there is no way to reduce the risk of both types of mistakes. Additional information, however, can enable better predictions, and simultaneously reduce both types of errors. Unnecessary restrictions on information sharing can make the task of obtaining additional information more difficult.

Another important tradeoff for consumers is between convenience and security. Convenience in a transaction is another way of saying transactions costs are low – there are not significant obstacles to engaging in the transaction. When a website stores a consumer's credit card information for use in future transactions, it reduces transactions costs for the consumer. It also creates, however, a potential security risk if the website is compromised. Entering a credit card number for each separate transaction is likely safer, but the gain in security may not be worth the loss of convenience.

An example of the tradeoff is the introduction of the EMV (Europay, Mastercard, and Visa) chip system in U.S. payment cards that began in 2015. Chips assign a transaction-specific identifier to each transaction, rather than using just the card number itself, thus substantially reduce the risk of counterfeit card transactions and therefore reducing the risk of fraud. On the other hand, payment systems impose transactions costs (often called "friction" in payment

discussions), including the time it takes to complete the transaction. The goal of the system is to minimize total costs, i.e., fraud losses plus friction costs, which is the security vs. convenience tradeoff discussed above.

When chipped cards were introduced in the UK and the EU (earlier than in the US), they required the customer to enter a PIN for an added layer of security, but the US rollout of the system did not require a PIN. The reason is the tradeoff between avoided fraud losses and frictions in the system. In Europe, telecommunications systems have historically been slower and more expensive than in the US, and as a result, a transaction might not be approved or rejected until after the fact. The US system, however, enabled essentially real-time authorization of the transaction. In Europe, the additional fraud losses prevented by the PIIN, at the cost of some increase in frictions, made the PIN worthwhile. In the US, the additional fraud that a PIN might prevent was smaller, because of real-time approval, and the added frictions of requiring a consumer to enter a PIN would effectively increase the total cost of the system.[58] This was an efficient market outcome, rather than a market failure.

Similarly, two factor authentication is more secure than a single password to protect an account, but it is also less convenient. Again, companies (and policy makers) must balance these costs to determine the appropriate balance. One interesting possibility for improving the tradeoff for both parties is sharing additional information. For example, if a financial institution had access to cell phone location information, it could potentially verify that the user's cell phone was at the same location as the proposed transaction. Such a system may provide almost as much additional security as texting an authorization code to the phone, without the need for the consumer to take additional steps.

The current approaches to data security are essentially a fortress approach: build additional walls and barriers to block unauthorized entry into data systems. Unfortunately, any fortress can be breached, and determined attackers have clear motives for attempting to do so. Because breaches are inevitable, systems to minimize the costs of breach are also critical. Credit card numbers, for example, are frequently compromised, but the costs to consumers are generally low, because robust fraud detection systems are in place. Indeed, many consumers find out that their account has been compromised when the issuer calls to verify a suspicious transaction.

The inevitability of breach also means that the regulatory focus must be on reasonable measures, rather than imposing strict liability for any breach. Companies should be held accountable for failure to take reasonable and appropriate security measures, but even the best security efforts may be breached. When breaches occur, companies should learn from their mistakes, and share that information with others, to secure the particular door to the fortress that was pried open.

D. Privacy and Credit Reporting

[58] See James Cooper & Todd Zywicki, A Chip off the Old Block or a New Direction for Payment Card Security: The Law and Economics of the U.S. Transition to EMV, 2018 MICH. St. L. REV. 869 (2018), for a fuller discussion.

As discussed above, credit reporting is vital to assuring credit availability to as many consumers as possible on the best possible terms. We address two important privacy-related issues with credit reporting. First, we consider accuracy in credit reporting, because inaccuracies can create significant consumer harms. Second, we consider the use of alternative data, which can help expand credit access.

1. Accuracy in Credit Reporting

There are clear market incentives for credit reporting agencies to strive for accuracy. Accurate data are far more likely to offer reliable predictions of risk, which is why the market for credit reports exists in the first place. The FTC has noted that there are "market incentives to maintain and improve the accuracy and completeness."[59] Similarly, researchers at the Federal Reserve Board have said that "research and creditor experience has consistently indicated that credit reporting company information … generally provides an effective measure of the relative risk posed by prospective borrowers."[60]

Market incentives alone, however, are not enough, and as discussed above, credit reporting is governed by the Fair Credit Reporting Act, which requires reasonable procedures to assure maximum possible accuracy in reporting. The law also imposes obligations on those who furnish information to credit reporting agencies ("furnishers"), requires notice to consumers when credit report information results in an adverse action, and allow consumers to dispute information in their file. All of these requirements are aimed at assuring accuracy of credit report information.

Credit reporting agencies face a difficult task of matching incoming information to the right file. Names may appear differently in different accounts, initials may replace names or vice versa, and names may change over time, sometimes repeatedly. Although mobility has declined over time, addresses change with much greater frequency than names; an average of more than 35 million people move each year.[61] Social Security Numbers are subject to transposition and other errors, which are difficult to detect because, unlike credit card numbers, the SSN does not include a checksum digit. When information is withheld for privacy reasons, such as using only the last four digits of a SSN, the risk of mismatch increases. The lack of SSNs in many public records has been a particular problem in matching potentially important risk information to the right consumer. The risk of a mistake also depends on the quality of the information voluntarily provided by data furnishers. Even the best matching algorithms cannot overcome bad data.

It is obviously a mistake to include information in one consumer's file that is not in fact about that consumer. Moreover, even information that is included in the right file may be in

[59] FTC Report to Congress under Sections 318 and 319 of the FACT Act of 2003, at 7 (December 2004).

[60] Robert B. Avery, Paul S. Calem, and Glenn B Canner, An Overview of Consumer Data and Credit Reporting. Federal Reserve Bulletin at 50-51 (2003), available at [HYPERLINK "https://www.federalreserve.gov/pubs/bulletin/2003/0203lead.pdf"].

[61] Average of U.S. Census data since 2010.

error. These are the kinds of inaccuracies that most studies of credit report accuracy have examined.

The most reliable study of accuracy, released by the FTC in 2012, used guided consumer reviews of their credit reports and submitted any identified errors through the dispute resolution process. The study identified potential inaccuracies in 24 percent of credit reports, but only 6.6% of consumers saw their credit score change after going through the dispute process. In 2 percent of the files, credit scores rose by 25 points or more after disputes were resolved.[62]

There have been significant changes in the industry since the FTC study that should have improved credit report accuracy. Potentially the most important of those changes is the initiation of supervisory examinations by the CFPB. The Bureau's 2017 Special Issue of Supervisory Highlights focused on credit reporting, and identified the many changes the Bureau directed to improve accuracy, including increased oversight of furnishers and monitoring of dispute metrics to identify the root causes of disputes. The Bureau has also examined furnishers, and enforced obligations to review consumer disputes, including any relevant information provided by the consumer.[63] In addition, the national credit reporting agencies (CRAs) reached an agreement with state Attorneys General to make various improvements in accuracy, including establishing a National Consumer Assistance Program (NCAP) to facilitate error correction and improve accuracy.[64]

Have these steps, which on their face seem reasonable, actually worked to improve accuracy? We do not know. The most effective way to find out would be to conduct another study like the 2012 FTC study, designed in such a way as to allow comparisons to the earlier results. Such a study is unlikely to tease out the effects of particular improvements, but it can tell us about the current state of accuracy of credit reports. The consumer-focused methodology would also offer an opportunity to study consumer experiences and satisfaction with the dispute resolution process.

The Bureau should also seek to study a more subtle error in credit reports: the failure to include information that in fact should be part of a consumer file. Such errors of omission reduce the value of credit reports to lenders, because a report that does not include all of the relevant information about a particular consumer is less likely to be predictive of future behavior. In some cases, the failure to include relevant information may leave a consumer with a thin file and limited access to conventional credit, as discussed in more detail in the following section.

---

[62] FTC, Report to Congress under Section 319 of the Fair and Accurate Credit Transactions Act of 2003 (December, 2012), available at [HYPERLINK "https://www.ftc.gov/sites/default/files/documents/reports/section-319-fair-and-accurate-credit-transactions-act-2003-fifth-interim-federal-trade-commission/130211factareport.pdf"].

[63] https://files.consumerfinance.gov/f/documents/201703_cfpb_Supervisory-Highlights-Consumer-Reporting-Special-Edition.pdf

[64] [HYPERLINK "https://www.ohioattorneygeneral.gov/Files/Briefing-Room/News-Releases/Consumer-Protection/2015-05-20-CRAs-AVC.aspx"].

One regulatory change that would allow an empirical assessment of the tradeoff between errors that result from mistakenly including information and errors from mistakenly excluding information is the impact of the NCAP provisions requiring a minimum amount of identifying information (name, address, SSN and/or date of birth) before public record information is included in a credit report. When the agreement took effect, the Bureau found civil judgments, previously the most common public record in credit reports, disappeared, and tax liens fell by almost half.[65] The consumer-focused approach of the FTC accuracy study could potentially address whether the removals were in fact accurate. Moreover, as the Bureau noted in 2018, it could not assess the impact of the change on the predictiveness of credit scoring models, because it lacked the two years of data that is the standard time for evaluating such models. Sufficient time has now elapsed to conduct such an assessment and evaluate empirically the tradeoff between different types of mistakes. Such data could also be useful as the Bureau considers the use of alternative data in credit scoring, where concerns about ambiguity in matching information may loom particularly large.

The Bureau should also seek to study the problem of "file fragments" more broadly. File fragments result when incoming information cannot be matched with sufficient certainty for inclusion in a particular consumer file. The failure to include accurate information is an error in any credit report, but it is of particular concern when the result is a "thin file" – a credit report with insufficient data to determine a credit score.

2. Alternative Data

Many consumers have insufficient data in their credit report to generate a score in typical credit scoring models. The Bureau has estimated that 26 million consumers are "credit invisibles," with no records with the national CRAs, and additional 19.5 million have records that either have too few accounts or accounts that are too stale to score.[66] The result is often an inability to qualify for mainstream credit, leaving only high cost alternatives. The thin file problem disproportionately affects the young (more than 80 percent of 18 and 19 year olds), Blacks and Hispanics (28 percent of each group, versus 16 percent for Whites), and lower income consumers (45 percent of the lowest income group, versus 8 percent of the highest).

Data not traditionally included in credit report can reduce the incidence of thin files and increase credit availability for underserved populations. Studies have shown that adding positive payment information from utilities and telecommunications providers, in addition to the negative information that most now report, can improve the credit scores of those with thin files that otherwise do not have sufficient information to support a reliable credit score.[67] Most recently, a

[65] CFPB, Public Records, Quarterly Consumer Credit Trends, February 2018.

[66] The CFPB Office of Research, *Data Point: Credit Invisibles*, 16, 2015 ([HYPERLINK "https://files.consumerfinance.gov/f/201505_cfpb_data-point-credit-invisibles.pdf"])

[67] Michael A. Turner and Amita Agarwal, "Using non-traditional data for underwriting loans to thin-file borrowers: Evidence, tips and precautions," 1 *Journal of Risk Management in Financial Institutions* 165 (2008). The Policy and Economic Research Council (PERC) has been researching such alternative data uses for a number of years. Its work

HUD-sponsored study found that reporting rent payments of HUD-assisted families would increase the number of these families with credit scores above 620 by 54 to 65 percent.[68] Such additional information can help to further reduce differences in the accessibility of credit on reasonable terms.

Although the credit reporting system is voluntary, pressure from regulators has assured that most financial institutions share payment data with the national CRAs. That is not the case for numerous other users of credit reports, including wireless carriers, energy utilities, and media companies such as cable TV, broadband internet service providers, and landline telephone companies.[69] Moreover, when such companies report, they often report only derogatory information, rather than reporting the consumer's full payment history. In effect, they use credit reporting to gain leverage in collecting payments by threatening a bad credit report, but do not allow creditors to assess those negatives in the context of the consumer's full payment history, and do not allow consumers credit for the larger number who pay their bills on time. Some have even argued that such companies should be required to report full file information.[70]

Given the wide diversity of potentially covered entities, the Task Force does not endorse mandatory reporting. We believe, however, that Congress should clarify that, regardless of other privacy laws, any entity other than a health care provider with a consumer account that requires regular payments can share payment histories for the purpose of credit reporting. Moreover, state and local regulators should encourage entities subject to their jurisdiction to report full-file information, particularly when those entities do report derogatory information. These practices are examples of "laws or action or inaction by industry" that impede the flow of credit information, and also "lower the availability of credit and raise its price to consumers."[71]

---

is summarized in Alternative Data Initiative: Report & Study Summaries (May 2020), available at [HYPERLINK "https://www.perc.net/publications/alternative-data-initiative-report-study-summaries/"].

[68] https://www.hud.gov/press/press_releases_media_advisories/HUD_No_20_030

[69] See Comments of PERC on the December 10, 2019 Accuracy in Consumer Reporting Workshop, January 31, 2020.

[70] Id.

[71] NCCF Report at 213.