Committee for the Study of Digital Platforms

Privacy and Data Protection Subcommittee

Report

July 2019
Subcommittee members

Lior Strahilevitz, University of Chicago (Chair)
Lorrie Faith Cranor, Carnegie Mellon University
Florencia Marotta-Wurgler, New York University
Jonathan Mayer, Princeton University
Paul Ohm, Georgetown University
Katherine Strandburg, New York University
Blase Ur, University of Chicago

Contributing Co-Authors

Sebastian Benthall, New York University
Filippo Maria Lancieri, University of Chicago
Jamie Luguri, University of Chicago
Mark Verstraete, New York University

DISCLAIMER: The purpose of this report is to foster discussion and illuminate key problems in privacy and security. The report is a document reflecting the subcommittee consensus, but not every part of the report reflects the views of each individual author.

* The Committee in-person meetings were partially supported by a grant from the Alfred P. Sloan Foundation, whom we also thank for supporting this project
Table of Contents

Executive Summary ........................................................................................................................................... 4

Introduction ..................................................................................................................................................... 9

I. An Overview of Some Key Problems in Privacy and Security ................................................................. 10
   A. Why Market Solutions Often Fail ........................................................................................................... 11
   B. Shortcomings of Notice and Choice ....................................................................................................... 12
   C. Harmonization Challenges ..................................................................................................................... 13
   D. Limited Resources for Deterring Privacy Violations ............................................................................ 14
   E. Data Security Threats .............................................................................................................................. 15

II. Existing Approaches to Protecting Privacy and Security ........................................................................... 18
   A. FTC Enforcement ..................................................................................................................................... 18
   B. California law .......................................................................................................................................... 19
   C. Proposed Domestic Legislation ............................................................................................................. 19
   D. GDPR ..................................................................................................................................................... 20
   E. ALI Privacy Principles Project ............................................................................................................... 21
   F. Industry self-regulation ........................................................................................................................... 22

III. Paths Forward: Default Rules, Constraints on Dark Patterns, and Improved Authentication ............. 23
   A. Default Rules for Privacy Policies ......................................................................................................... 23
      1. Determining the Contents of Privacy Defaults .................................................................................... 26
      2. Data about Consumer Privacy Preferences and Expectations ............................................................ 26
      3. Toward “Consumertarian Default Rules” ............................................................................................ 29
   B. Dark Patterns and Manipulation ............................................................................................................. 32
      1. Defining Actionable Manipulation ....................................................................................................... 33
         a. Transaction Costs Dark Patterns ..................................................................................................... 34
         b. Manipulation by Targeting Vulnerabilities ..................................................................................... 34
      2. A Data-Driven Approach to Spotting Problematic Dark Patterns .................................................... 37
      3. Legal Framework .................................................................................................................................. 43
   C. Institutional Implementation Considerations for Default Rules and Dark Pattern Regulations ............ 50
   D. Mitigation for Security Threats Caused by Data Breaches .................................................................. 52
   E. Privacy-Preserving Measurement and Coordination ............................................................................ 56

Conclusion ....................................................................................................................................................... 58
Executive Summary

Any serious effort to think systematically about the emerging policy issues surrounding digital platforms must contend with a host of privacy and security challenges. It is becoming increasingly clear that core aspects of the American approach to privacy, such as faith in industry self-regulation, the embrace of a sectoral approach involving overlays of state and federal laws, heavy reliance on notice and choice, and the lack of remedial powers for the nation’s primary privacy regulator, leave the world’s largest economy ill-equipped to vindicate important interests in privacy and security. The weaknesses and idiosyncrasies of the American approach impede efforts to harmonize global privacy law, and that lack of harmonization threatens the free flow of data in international e-commerce.

There are several key reasons why neither industry self-regulation nor notice-and-choice approaches to protecting privacy and security succeeded. Firms that collect personal information do not internalize all the harms associated with consumer privacy and security breaches, nor do they have adequate incentives to take account of how decisions they make may affect the interests of consumers who are not their customers. These problems are compounded by the highly technical nature of privacy and security decisions, the difficulty of establishing clear causal links between particular practices and subsequent consumer harms, and the challenges of monitoring and evaluating firms’ key investments in data security. Notice and choice, by contrast, largely fails as a strategy because it does not live up to the promises its name suggests. More precisely, the standard approach is to provide consumers with a lengthy wall of legalese text that they will not read and then to pretend that consumers are making meaningful choices that vindicate their interests in response. Moreover, firms have become skilled at developing choice architectures that nudge consumers toward options that benefit company profitability but may not reflect consumers’ actual preferences or expectations.

There are a number of existing reform proposals in the privacy and security domain, some quite laudable, others more dubious in terms of their benefits. Our subcommittee’s approach is not to provide a roadmap for comprehensive national privacy legislation. Rather, we have focused our attention on developing three complementary approaches to protecting privacy and security interests. These approaches are modular, so they can be integrated into any existing proposals, though each would also be effective as a stand-alone reform.

The first of our three proposals advocates for the use of data-driven contractual default rules in privacy and security. Default rules are starting points for contractual relations between parties. For example, they govern the scope of data collection and retention of a consumer’s personal information by a platform. By definition, any default rule can be modified by the mutual agreement of the contracting parties. We can contrast these default rules with mandatory rules, which provide contractual rights and responsibilities that cannot be altered by the parties. While there is an important role for mandatory rules to play in instances where consumer preferences are very homogenous, where collective action problems arise, or where significant
information asymmetries exist, as with highly technical and complex matters, default rules are a vital tool in the regulatory arsenal. Default rules are particularly useful in the many instances where consumers have heterogeneous preferences, where consumers or firms possess relevant information to which regulators do not have ready access, and where substantial externalities are not present in a transaction.

We propose that the content of contractual default provisions will depend on the articulated preferences of ordinary consumers as measured by scientifically rigorous survey instruments. Based on our own pilot testing of such instruments involving the privacy and security practices of Facebook, Google, Amazon, and other platforms, consumers will often – but not always – prefer and expect default provisions that enhance their privacy and security. In privacy and security settings there will be many instances in which it is appropriate for the law to use “consumertarian” default rules – i.e., the legal defaults preferred or expected by a majority of consumers. While these default rules will not always reflect the preferences of platforms and other firms that are contracting with consumers, these firms will have the ability to convince consumers to waive the protections required by default if they can convince consumers that waiving such protections will make consumers better off. In that sense, consumertarian default rules and subsequent efforts to convince consumers to waive protections that firms find problematic for their business models will function as information-forcing devices that reduce unexpected surprises, encourage dialogue, and prevent firms from seeking to engage in privacy and security practices that might prompt customer backlash. Because many default protections will be sticky under these circumstances, and firms will have incentives to be selective about which rights they ask consumers to waive, the result of our proposal on net will be to heighten privacy and security protections for consumers. This proposal for consumertarian default rules is somewhat similar to the Privacy-by-Default regime that was enacted as part of the European General Data Protection Regulation (GDPR), though we believe our approach does a better job of creating predictable, transparent benchmarks.

Under our approach, the protections granted by default rules can be waived by consumers, but only via a process that takes the notion of informed consumer consent more seriously than the law does currently. Our discussion of dark patterns, which we will now explain, provides a yardstick for measuring the sufficiency of such waivers.

Our second set of proposals concerns dark patterns. Dark patterns are user interfaces that make it difficult for users to express their actual preferences or that manipulate users into taking actions that do not comport with their preferences or expectations. Examples of dark patterns abound in privacy and security. For example, Google Maps repeatedly asks users whether a site that they regularly return to should be labeled “home” or “work.” If the user agrees to label the geolocation, then the pop-up queries will cease. If the user clicks on “Not Now” then there will be more queries a few days later. The result is that the application may be so persistent in asking for users to confirm personal information that they will eventually relent to prevent further
nagging, and not because they want to share this information. Alternatively, many firms make it easy to alter one’s defaults in a way that benefits the firm financially but quite cumbersome to alter default settings in a way that will make the customer less profitable for the firm. Some firms attempt to hide what they are doing, for example when firms add items to a consumer’s online shopping cart without asking the consumer, or when they add a hidden service to an online transaction by preselecting the addition so as to ensnare consumers who they know will quickly click through a screen to complete the transaction. Firms may employ intentionally ambiguous terminology in an effort to confuse consumers into opting for a service they do not want, or they may manipulate consumers by targeting acute emotional vulnerabilities. One attribute all these dark patterns share is a tendency to exploit “System 1” (quick, instinctive) decision-making and suppress more deliberative “System 2” thought processes.

We surmise that firms have done rigorous beta testing of dark pattern techniques because they have become prevalent in recent years. Academics and non-profit organizations have documented the prevalence of dark patterns, but until now no researchers have published research that examines the efficacy of these dark patterns in prompting consumers to make choices that are inconsistent with what consumers would choose in a neutral decision architecture. Our report fills a significant gap in the literature, thanks to an extensive data collection effort by Jamie Luguri and Lior Strailevitz. Those authors, after obtaining IRB approval, exposed a census-weighted, nationally representative sample of 1,762 Americans to a decision-making framework in which the control group was offered an easy yes/no choice over whether to sign up for an expensive identity theft protection plan, an experimental group was subjected to rather mild dark pattern interventions, and a second experimental group was subjected to the aggressive use of dark patterns. Both dark pattern conditions were designed to prompt consumers to agree to pay for an identity theft protection plan that few members of the control group wanted.

The bottom-line results from this dark pattern experiment were striking. Employing mild dark patterns increased the percentage of consumers who ultimately agreed to accept the data protection plan by 228% (from roughly 11% to 26%). Employing aggressive dark patterns increased the percentage of consumers who agreed to accept the data protection plan by 371% (from roughly 11% to 42%). In other words, in both the mild and aggressive dark pattern environments, it was more likely than not that consumers were agreeing to sign up for the plan our researchers were selling them because of the dark pattern, and not because of an underlying desire to purchase the plan itself.

Notably, the experiment’s use of aggressive dark patterns generated the equivalent of a customer backlash. Consumers in the aggressive dark pattern condition had their moods adversely affected, they were less likely to agree to participate in follow-up research by the same researchers when given the opportunity to do so, and they were more likely to withdraw from the experiment, forfeiting their entitlement to be compensated for taking the survey. This data
provide evidence that the market itself constrains the use of aggressive dark patterns somewhat. On the other hand, the use of mild dark patterns generated either no such effects or far smaller effects – with respect to their mood at the conclusion of the experiment, consumers exposed to the control group decision architecture and the mild dark pattern decision architecture were statistically indistinguishable. To summarize, then, firms face significant incentives to avoid using the most blatant and annoying dark pattern strategies, but the use of more subtle dark patterns seems to be all upside from the perspective of a firm’s bottom line. These mild strategies seem to substantially increase the percentage of consumers who will sign up for a good or service without alienating those customers, at least in the short run.

The more highly educated consumers were, the less vulnerable they were to having their choices manipulated via dark patterns. These effects were statistically significant, and highly troubling. Dark patterns work on many people, but lower socio-economic status individuals are especially vulnerable to them. Less educated individuals were particularly susceptible to mild dark patterns.

In light of these findings, our report advocates a per se legal rule that will apply to many situations involving the use of dark patterns to prompt consumers to share personal information. Where a firm’s choice architecture more than doubles the percentage of users who agree to share information, when compared with a neutral choice architecture, consumers’ consent to share such information is not valid. Moreover, dark pattern tactics that satisfy this “more likely than not” test should be treated as unfair and deceptive practices in trade, which are proscribed by federal and state consumer protection laws. There may be other domains in which a dark pattern is highly problematic but does not satisfy this per se test. To deal with those situations, we offer a multi-factor balancing test that can be used to identify the dark patterns that are most likely to diminish consumer well-being. That test looks to the extent to which a dark pattern unnecessarily raises the transaction costs of opting out of a protection that large numbers of consumers expect or prefer, the extent to which the dark pattern targets problematic consumer vulnerabilities, or the extent to which a dark pattern is hidden rather than transparent.

The final proposal in our report focuses on mitigating the security threats that are caused by data breaches. A single data breach at one platform or digital service can present major problems for other platforms and services. The reason stems from password reuse. Consumers frequently use identical or very similar login credentials at multiple sites. As a result, hackers may obtain credentials from one site and then quickly try to use those same pilfered credentials to gain access to various other sites and platforms. One main way that firms currently try to protect themselves is by purchasing stolen credentials, which creates perverse incentives.

Among the various reforms to be considered, private data breach clearinghouses are preferable, given existing technological constraints. Ideally, such clearinghouses could use techniques that employ advanced mathematics to test whether user passwords are repeated across multiple sites without disclosing login credentials. Firms would be required or strongly
incentivized to make their own data available for queries in order to ping a centralized database. The clearinghouse proposal would encounter some challenges, ranging from the paramount need to protect the clearinghouse as a single source of failure to the technical challenges associated with identifying similar but not identical passwords that are being used across multiple sites. Still, the subcommittee has concluded that, on balance, such an approach is superior to the viable alternatives that the report discusses.

The subcommittee report concludes with an overview of the need to balance privacy interests against transparency considerations. The other subcommittee reports on digital platforms laud the benefits of greater data transparency to evaluate the role of platforms in markets, media, and politics. These are worthwhile goals. At the same time, well-meaning efforts to make data transparent can expose individuals’ sensitive private information. Differential privacy and secure multiparty computation are two of the most promising technologies for protecting privacy in these domains, and policymakers should ensure that these strategies are implemented alongside transparency initiatives.
Introduction

It is rare for a week to pass in the United States without some new privacy scandal. Sometimes the scandal involves a massive breach of sensitive personal information that was inadequately protected. Other times it involves a deviation from promises to keep information confidential or secure. And other instances involve unexpected or unwanted data collection, retention, or use, or the repurposing of data to further a different, unanticipated objective. These privacy scandals are costly to society. They result in embarrassment, psychological harm, a loss of control, and financial damage. As a result of these harms, consumers may disengage from using digital platforms, they may engage in less online commerce, they may become more reluctant to say what they think, they may curtail their communications with intimates, and they may take steps to disguise their identities through the use of deception and other self-help strategies. Failing to protect privacy generates significant social costs; that much is clear. What’s less clear is the answer to the question, “What should be done?”

In addressing this question it is important to recognize that there are issues about which consumers’ preferences and needs are heterogeneous. Some consumers are quite concerned about the privacy of certain personal information and others are not. Some would gladly trade cost or convenience or appealing product features for less privacy, and others would strongly object to such swaps. Some care a great deal about keeping information about their political beliefs confidential but are less reluctant to share information about their intimate associations. For others this hierarchy is reversed. Sometimes consumers want to exercise choices or control regarding their private information but find the options confusing or difficult to exercise.

A response to this question must also recognize that differences in individual privacy expectations, preferences, and needs may be attributable to societal or cultural factors. Individuals have differing experiences with technology, socioeconomic backgrounds, and nationalities, any of which may shape their distinct privacy perspectives. A response must be sensitive to these differences and must avoid magnifying inequities and other societal concerns. While the sheer complexity of the privacy and security decisions people are confronted with on a daily basis may justify a significant role for technocratic expertise, it is important to remain cognizant of the dangers of regulatory capture, the slowness of bureaucratic decision-making, and the dangers of paternalistic decision-making that is out of step with evolving consumer preferences and practices.
I. An Overview of Some Key Problems in Privacy and Security

The American approach to privacy makes the country something of an outlier, at least in comparison to other liberal democracies. Notable features of the present American approach include: (1) its failure to enact comprehensive consumer privacy legislation at the federal level, relying instead on sector-specific federal privacy law and state privacy law; (2) the relatively weak regulatory powers of the primary federal enforcement agency in the United States; (3) a reliance on class action suits to deter and punish various privacy violations and security breaches; and (4) a hierarchy of values that generally emphasizes free speech interests. As a result, significant gaps exist in American privacy law, and whether a particular act generates legal consequences depends on which part of the United States a party finds itself in and what the incentives are for regulatory agencies or private litigants to file suit. Moreover, in some instances, significant privacy harms may not lend themselves to constitutionally permissible remedies in the federal courts.

Foreign observers sometimes believe that American privacy protections are nonexistent because there is not a single authoritative and universal law that protects a particular set of privacy interests. That is an error. Some key components of global privacy law—like data breach notification laws or the Fair Information Practices—have emerged in the United States and been widely adopted elsewhere. There are some American states that have embraced or are moving towards comprehensive consumer privacy legislation, such as the recently adopted California Consumer Privacy Act. And there are some areas of the economy—such as the telecommunications, health care, criminal justice, and education sectors—where federal privacy protections are relatively robust by global standards. American privacy laws are relatively complex, and in most of the country they are relatively lax or incomplete, but legal protections for privacy are far from nonexistent.

Another distinct feature of the American approach to privacy is a relatively high level of stated government confidence that market incentives will safeguard consumer privacy and security interests without the need for regulatory interventions. From that perspective, firms will compete over privacy and security, and the companies that fail to deliver what consumers want will be driven out of business. Whatever the merits of a hands-off approach to privacy in theory, in practice it has largely failed. To be sure, we do see evidence that firms in industries where privacy and security are particularly important (such as financial services or cloud computing) invest more resources in privacy and security than firms in industries where those concerns are less salient (Marotta-Wurgler, 2016). In some extreme and salient cases, executives have lost their jobs because of privacy snafus. But prominent market failures persist, justifying smart regulatory interventions.
A. Why Market Solutions Often Fail

There are several important potential sources of market failure. First, many of the harms associated with privacy and security breaches are not internalized by firms. A breach might not be discovered until months or years after it occurs—if ever. Another reason for this dynamic relates to the difficulties of tying many secondary harms to a particular failure by a company. For example, a consumer might be victimized by identity theft but unable to trace the identity theft to any particular breach. Perhaps the same consumer information was breached several times in recent years, making it difficult to establish a causal connection between a corporate practice and a negative consequence. The more breaches occur, the more vexing this problem becomes.

A second reason why harms aren’t fully internalized involves the costs to consumers of monitoring the consequences of privacy snafus. As corporate errors become more commonplace, there is less sustained attention devoted to each one in the media and other sources. With the exception of catastrophes like the Equifax breach or Cambridge Analytica scandal, it is likely that a new privacy goof will come along quickly to push the most recent breach out of a consumer’s news feed. Even individualized data breach notifications, whose prompt dissemination is mandated by law, can get lost or ignored in a sea of other mandated disclosures.

Third, decision-making over privacy is so complicated that consumers often do not understand the nature of the bargains they are making when they agree to share personal information in order to use a non-priced good or service. A major reason is the problem of unanticipated uses and failures of imagination. Thanks to advances in computing power and data mining techniques, new uses of old data are regularly discovered. Many consumers do not even understand how data they surrender is used contemporaneously. It is therefore unreasonable to expect them to anticipate the sorts of uses that data they share today will be put to in three, five, or ten years. If and when such data is used in a way that disadvantages consumers, they will be unable to tie that harm to the company they shared it with, even if the company still survives as a going concern. When consumers come into direct contact with dozens of companies and indirect contact with hundreds, it is unrealistic to expect them to perform due diligence by reading privacy policies and devoting resources to understanding all their implications. As a result, markets function poorly to constrain companies that engage in controversial privacy practices.

Fourth, a great deal of personal information is held by firms with which consumers have no direct contact. These may be data brokers, credit agencies, and vendors who have purchased data; or prospective employers, landlords, and insurers with whom a contractual relationship never materialized. Any consumer efforts to penalize firms that have behaved badly will be dampened by the indirect nature of these relationships, and intermediary firms therefore will not internalize fully the externalities associated with data breaches.

Fifth, in many instances markets may fail to satisfy consumer preferences because of the “collective privacy” problem (Strahilevitz, 2010; Barocas & Levy, 2018). That is, information
about each consumer is distributed, leaving the person whose information is at issue with incomplete control over the dissemination of that information, even if she takes all reasonable precautions to preserve its confidentiality. For example, suppose one sibling decides to share her information with a genetic testing firm. The other sibling, whose genetic attributes can now be inferred, may object strenuously to the placement of this information in the hands of a proprietary firm. But the law provides the objecting sibling with essentially no recourse. Along similar lines, even if an individual elects not to join a social media platform, her friends and relatives may reveal a good deal of information about her that can then be used in ways that affect her life. Photos of her may appear, and stories about what she said or did may be widely shared. The problem is particularly acute for children, whose parents and peers often share sensitive information about them online without fully understanding the future ramifications.

Sixth, firms often face dampened incentives to differentiate themselves with respect to privacy, especially via consumer-facing advertising. Except in rare instances, privacy is not the most salient attribute for consumers when considering a good or service. A firm that seeks to raise awareness about the relative strengths of its privacy practices compared to its competitors has to worry about spooking consumers into avoiding the product or service line altogether. As a result, while there have occasionally been splashy marketing campaigns emphasizing a particular company’s commitment to privacy, these sorts of campaigns have been either short-lived or implemented on behalf of niche products with small market shares.

Finally, consumers are often left to bear the burden of data breaches themselves. While consumers may hear about data breaches after they occur, they rarely know what steps to take in reaction. Data breaches can have cascading consequences as hackers leverage the information stolen to cause further damage. Consumers face difficulties evaluating these cascading consequences and mitigating the harms. Furthermore, it is difficult for consumers to evaluate a firm’s investments in data security. Indeed, firms have incentives to obfuscate their efforts on the data security front because information they share with consumers will inevitably make its way to hackers, who can use this information to discover vulnerabilities.

In summary, while firms plainly have some incentives to deliver privacy and security to consumers, there are lots of reasons to explore regulatory interventions.

**B. Shortcomings of Notice and Choice**

One variant of a market-oriented approach to protecting privacy is notice and choice. The notice and choice approach dictates that consumers be informed of what firms are doing with personal information so they can make their own choices about how and whether that data should be used. There is nothing wrong with this approach in the abstract. Indeed, the approach has the potential to accommodate the heterogeneity of consumer preferences and values. In practice, however, notice and choice has largely failed as a regulatory strategy for some of the aforementioned reasons. For example, the kinds of choices that consumers are being asked to
make are too complex and too speculative, especially given the open-ended nature of the privacy policy language that is placed in front of them.

Notice and choice, as presently practiced, fails for a broader reason as well. The information that gets disclosed to consumers is too voluminous and intricate for consumers to read, understand, and then make a well-informed choice that reflects their values, preferences, and interests (McDonald & Cranor, 2008; Bakos et al., 2014). Were consumers to have relationships with just a few entities, such investment of time and cognitive resources might be realistic. In a world where consumers have dozens of apps on their smartphones, visit numerous web sites, and bring an increasing number of connected devices into their homes and workplaces, notice and choice fails. Consumers click “I agree” without reading and hope for the best.

Various proposals have emerged to enhance notice and choice through techniques like visceral notice or highlighting unexpected terms (Calo, 2012). While these approaches represent an improvement over the status quo, they too run up against constraints. For example, visceral notices that grab consumers’ attention may work well initially, but once the technique is employed in even a modest number of interactions it appears to lose its force. When everything is visceral, nothing is. The limited empirical testing that has been done on these sorts of techniques also suggests they are of limited utility.

A further problem with notice and choice is that a consumer’s choice might not be freely exercised. Companies have become increasingly sophisticated at nudging consumers into acts and omissions that result in privacy practices that are good for corporate bottom lines but may be at odds with what consumers would prefer were they to understand fully the nature of their interactions. The legal system in the United States has been quick to deem consumers as having consented to terms and conditions despite genuine reason to believe that their consent is the product of manipulation rather than free choice (Lemley, 2006). Below, we will examine this issue in much more depth and identify appropriate interventions.

C. Harmonization Challenges

Digital Platforms operate in global marketplaces. This presents real challenges for firms. First, because national and multinational regimes for regulating privacy and security vary, practices that are lawful in one country may be unlawful in another. Second, for efficiency reasons, it may make sense for personal information to be gathered in one country and then analyzed in another. Third, even firms that primarily operate domestically in the United States must deal with increasingly diverse state law regimes. This means that cumulative obligations regularly arise under state law, compliance burdens increase, and legal conflicts can occur—especially where extraterritorial law enforcement or national security interests are involved.

International tensions involving data privacy have already manifested. Most prominently, the Court of Justice of the European Union’s decision in Schrems struck down the US-EU Safe Harbor Agreement that permitted personal data of EU citizens to flow across the Atlantic. The
quick negotiation and implementation of the EU-US Privacy Shield Framework as a replacement prevented an immediate crisis, but there are reasons to worry that these kinds of issues will recur, particularly if the GDPR and American law continue to diverge. Indeed, new legal challenges to Privacy Shield are presently pending in Schrems II before the Court of Justice. The results could be quite negative for American technology companies that have substantial business activities overseas.

The costs of complying with different sets of state laws also can be high. States may legislate without giving adequate consideration to the compliance burdens that are imposed on firms that operate nationally. These kinds of costs may be borne more easily by well-capitalized digital platforms that enjoy economies of scale. For new start-up the costs may be much more significant, and the burdens associated with complying with every state law could function as barriers to entry. In other instances, the existence of an unusual law in one state may create surprises for firms. For example, Illinois has a unique law limiting the collection and use of biometric information, one that enables people whose rights are violated to file a civil suit and recover minimum statutory damages. The law has given rise to a number of class action suits involving the use of facial recognition and fingerprint applications. In the first half of 2019, class actions invoking the Illinois law were being filed at a rate of approximately one per day. While some companies were no doubt aware of the Illinois law when they were designing their products to integrate biometrics, other companies were caught unaware and now face the prospect of significant legal liability. Ignorance of the law is no excuse, but imposing obligations of this sort at the national level provides greater notice to firms that wish to operate in a national marketplace.

**D. Limited Resources for Deterring Privacy Violations**

To the extent that the American legal system has a primary cop on the beat of privacy and security, that entity is the Federal Trade Commission (FTC) (Hoofnagle, 2016). But the Commission is hamstrung by its limited authority to police privacy. The FTC primarily addresses privacy issues pursuant to its power to regulate unfair and deceptive practices in trade. Congress has imposed significant procedural burdens on administrative rulemaking under that authority, such that the FTC must resort to individual enforcement actions and case-by-case articulation of privacy law. Congress has also constrained the FTC’s monetary penalty authority in unfairness and deception cases to violations of consent decrees, effectively creating a “two-strikes” system—a firm’s first privacy violation results in a consent decree, and only subsequent violations can result in penalties. Thus, for example, the FTC’s ability to fine Facebook $5 billion in 2019 for its actions with respect to Cambridge Analytica depends entirely on a 2012 consent decree between Facebook and the FTC, which arose from a prior privacy snafu. Were it not for that earlier consent decree, Facebook would not face monetary penalties for its actions, at least not insofar as the FTC is concerned.
It is also widely believed that the FTC lacks the resources to regulate privacy effectively. Only 46, or four percent, of the agency’s 1,141 employees work in the Division of Privacy and Identity Protection. And only about five of the FTC’s employees are technology experts. The FTC’s professional consumer protection staff is commendable but as the role of digital platforms in our economy has grown, regulatory resources have not kept up. As a result, many major problems involving privacy and security are discovered and publicized by other entities, such as investigative journalists, state attorneys general, academic researchers, and experts hired by class action attorneys. Resource constraints render the FTC a reactive regulator rather than a proactive one.

Class action litigation has achieved some success, mainly from a deterrence perspective. However, class actions rarely result in the victims of privacy and security snafus being made whole for the associated psychological costs. Such litigation is lucrative for the attorneys who bring suits successfully and has incidental benefits for the privacy-related non-profits that sometimes receive large payouts pursuant to settlements. Plaintiffs’ lawyers will gravitate to bringing cases under statutes that contain minimum statutory damages provisions. As a result, privacy interests vindicated by those statutes are enforced rather aggressively, and comparable interests that are embedded in legal frameworks without such provisions tend to get inadequate attention. Two results are skewed priorities and a risk of over- and under-deterrence in areas of privacy law.

**E. Data Security Threats**

Repositories of consumer data have come under increasing attack in recent years due to a unique confluence of technological and market factors. Rather than providing a framework for omnibus interventions that would tackle the myriad of problems associated with data security, our subcommittee has chosen to focus on a very important but relatively soluble problem, one revolving around the use of passwords as access credentials for digital platforms. The reason for this focus is that problems around access credentials have similar roots to many of the problems pinpointed above in relation to data privacy: the over-reliance on the user to address all the shortcomings of their personal choices.

Despite repeated efforts to advance alternative schemes for authentication, passwords remain ubiquitous on the web because no single alternative scheme is superior to passwords on every relevant metric, and passwords have advantages in familiarity and deployment. Large-scale data breaches have unfortunately become a common occurrence, ranging from the breach of credit reporting agency Equifax to the breaches of hundreds of different websites, including major online services like Yahoo. Collectively, billions of credentials (pairs of usernames and passwords) have been stolen. The most obvious consequences of these breaches are to the service that was breached. Once a breach is discovered, which unfortunately can take years, the breached company typically forces a password reset for all affected accounts. However, in many cases other companies are at
risk. While each website or service typically runs its own authentication system (i.e., most users have an account unique to each service, rather than a federated identity controlled by a single service-agnostic entity), information stolen from data breaches can inextricably bind the fates of otherwise independent accounts at competing companies.

Most websites limit the number of log-in attempts for a particular account, which might normally prevent guessing attacks for all accounts other than those with the most predictable passwords. However, when an account holder has had their account credentials on another service breached and the accounts can be associated across services (e.g., because they share the same username or registration email address), guessing attacks can become a major threat. This is because users frequently reuse passwords across accounts. Even when the passwords are not exactly the same, attackers can often guess similar passwords in fewer guesses than would set off alarms on most services. As a result, attackers use credentials stolen in data breaches to make highly targeted guesses, frequently compromising accounts successfully.

A core issue is that the whole authentication system overly relies on users policing their own password use. Crucially, companies and organizations do not know which of their users have chosen a similar password for their account with a competitor—something that prevents “security coordination” among companies. Compounding this problem, users themselves are many times not fully aware of the risks involved in password re-use. The makers of password manager software have tended to design the software not to castigate users for reusing passwords, worried that being too heavy-handed would encourage the user to stop using that password manager and potentially turn to a competitor. The abundance of websites that require logins and passwords for trivial matters, and the feeling that these are low-stakes decisions, encourage re-use and diminish incentives for monitoring data breaches. In addition, companies may not disclose data breaches to users in sufficient detail or in a timely manner. Even when notified of a password-related data breach, users may not fully understand the causes of, or mitigations for, their vulnerability to account compromises related to password reuse.

In short, the system places a significant burden on users to constantly police the security of their accounts in a context where many might not even recall that they reused the same password elsewhere, or they might not understand why doing so is problematic. As a harm-mitigation strategy, companies like Facebook seek out (and in some instances purchase) lists of stolen credentials from hackers to proactively lock their own users’ accounts. This state of affairs represents a market failure. Authentication systems are siloed, each controlled by a single company. Following data breaches, other companies and organizations are at risk because of password reuse, yet they do not know for which accounts this is the case, nor do the users themselves. And when companies buy information from hackers to try to fill these gaps, they provide a (marginal) incentive for hackers to obtain sensitive personal information in the future.

This dynamic takes place in a context where data breaches are becoming increasingly costly. Data about an individual stolen in a data breach can also be weaponized against data
subjects or even their employers, friends, and relatives in other ways, such as by enabling an attacker to engender misplaced trust by demonstrating knowledge of this information. For example, phishing attacks (fraudulent emails designed to cause an individual to disclose personal information or credentials, or to provide access to a resource) have become increasingly targeted through the inclusion of user-specific personal information (e.g., knowledge of friends’ names, the inclusion of the user’s phone number or past purchases) in recent years. These targeted attacks are known as spear phishing. We expect that spear phishing attacks will become even more targeted in the near future as attackers amass data stolen in data breaches, including an individual’s personal information lost directly in the data breach, information gleaned from accessing accounts (e.g., an email inbox) using credentials stolen in a data breach, and the ability to send messages from breached accounts in the first place. These types of information hold the potential to fool a victim into mistakenly thinking an email is legitimate. Spear phishing can have disastrous consequences for the victim, as exemplified by the exfiltration of John Podesta’s emails during the 2016 presidential campaign. Unfortunately, individuals will often know, at best, the broad types of information stolen in a data breach, not the specific information nor comprehensive steps for remediating the breach. As a result, targeted phishing attacks using stolen information will become increasingly difficult for individuals to recognize.
II. Existing Approaches to Protecting Privacy and Security

A. FTC Enforcement

The Federal Trade Commission seeks to deter unfair and deceptive consumer privacy and data security practices though enforcement of section 5 of the FTC Act against entities engaged in practices that are likely to cause substantial injury to consumers. In addition, the FTC is charged with enforcing the Children’s Online Privacy Protection Act of 1998 (COPPA), the US-EU Privacy Shield, and, joint with another agency, the Fair Credit Reporting Act (FCRA) and Gramm-Leach-Bliley Act (GLBA). These last two statutes, among other things, seek to protect financial information. Almost all FTC actions result in a settlement or default judgment. As a result, there are barely any judicial decisions involving the FTC in this area.

Since 1995 the FTC has enforced the self-imposed duties that firms laid out in privacy policies. Though the FTC did not require any specific terms in such policies, it did require that firms live up to the promises made in those agreements as failure to do so would be considered a deceptive trade practice. Most FTC activity in this space involved actions of this type. These include actions against Facebook for failing to keep its promise to keep consumer information private, against AshleyMadison.com for suffering a massive data breach and thus failing to keep its promise to keep their customer information secure, and against Uber after it breached its promise to monitor employee access to consumer data, among others. As parts of the consent decree with the FTC, the violating companies agree to correct their violating behavior by, for example, implementing comprehensive data-security assessment in the case of AshleyMadison.com, or undergoing a comprehensive privacy program and obtaining regular independent audits in the case of Uber. The consent decree also will usually provide “fencing-in relief” that sweeps more broadly than the initial violation, providing the FTC a foundation for subsequent enforcement actions involving the same firm.

A limitation to this approach is the fact that firms making few or no promises in their privacy policies can avoid some FTC actions. In a handful of cases, the FTC has brought actions against firms for deceptive omissions, as it did in an action against Nomi Technologies, a firm providing in-store tracking technology that promised to give consumers an opt-out choice but later failed to do so. In a minority of cases, the FTC has brought actions against firms that it alleged were engaging in unfair practices. While “unfairness” is an intentionally broad concept, section 5 requires additional elements for an unfairness claim (including harm to consumers) that can be difficult to prove in some privacy cases.

The FTC has brought around 200 privacy cases to date, representing an average of about ten cases a year. While the FTC is strategic in the actions that it brings, often focusing on large companies, there is reason to doubt the overall deterrent effect given the small number of cases and the small penalties.
B. California law

Perhaps the most notable state regulation is the California Consumer Privacy Act (CCPA), which becomes effective on January 20, 2020. The CCPA applies to for-profit businesses that have annual gross revenue in excess of $25 million, receive or disclose information of more than 50,000 California residents, or derive more than 50% of their annual revenue from selling California residents’ data. Personal data is defined broadly, and includes information that relates to, describes, or could be used to identify California residents or households. The CCPA provides exceptions for de-identified or aggregate data, but the scope of those terms remains ambiguous.

The CCPA requires businesses to inform consumers, at or before the point of collection, of the categories of personal data being collected and the purposes the data will be used for. In addition, businesses must provide notice and the opportunity to opt out of third-party data sharing. Online privacy policies must describe a consumer’s CCPA rights, and businesses are prohibited from including contract provisions that limit a consumer’s enforcement remedies. Consumers also have the right to request information concerning the source of the data, the specific types of data being collected, and the categories of data being shared with third parties. In general, the CCPA does not create specific data security rules, though it does require businesses to maintain reasonable security procedures appropriate to the nature of personal information being collected.

The California Attorney General is given primary enforcement authority, though consumers also have a (very) limited individual and class action right of action regarding the law’s data breach provisions. The AG may seek injunctive remedies, or impose fines of up to $7,500 for each intentional violation and $2,500 for unintentional violations.

Even before the CCPA was enacted, California had heightened privacy requirements on the books. The California Online Privacy Protection Act (CalOPPA), for example, requires online services to post privacy policies, which sets up subsequent FTC or attorney general enforcement. The state’s data safeguard law also requires reasonable data security precautions and is enforceable as a violation of California’s unfair competition law.

C. Proposed Domestic Legislation

Privacy and security concerns have helped spark creative legislative proposals. Numerous pieces of proposed legislation have been introduced within the last year at both the state and federal level. The list of pending bills is long and grows by the month. Here we wish to highlight a couple of significant recent proposals that are particularly germane to this report’s emphasis and recommendations.

In January 2019, Washington State Senator Carlyle introduced the Washington Privacy Act, which was approved by a majority of the state Senate but stalled in the state’s House of
Representatives. The law was similar to the CCPA in many respects, though the version approved by the Senate differed from the California law in that it lacked a private cause of action, ceding enforcement to the state attorney general’s office. The proposed legislation would also restrict the use of facial recognition technologies in both the private and public sectors. It is likely that such legislation will be reintroduced in the 2020 legislative session. Other states such as New York, Texas, and Massachusetts are also considering similar legislation, and Maine and Nevada have enacted more limited versions.

In April 2019 Senators Warner and Fischer introduced the federal Deceptive Experiences to Online Users Reduction (DETOUR) Act. The bill is, as far as we know, the first federal legislation that takes aim at the problem of dark patterns online and their use to convince consumers to part with personal information. The legislation would only apply to online services that have more than 100 million monthly users. Among other provisions, the bill would make it unlawful “to design, modify, or manipulate a user interface with the purpose or substantial effect of obscuring, subverting, or impairing user autonomy, decision-making, or choice to obtain consent or user data.” The proposed legislation also includes a safe harbor for firms engaging in conduct that establishes “default settings that provide enhanced privacy protections to users or otherwise enhance[s] their autonomy and decision-making ability.” The FTC would have authority to enforce the law, which treats violations as unfair or deceptive practices in trade. A key dimension of the bill is how to identify user interfaces that have the “substantial effect of impairing user autonomy, decision-making, or choice.” That is a problem to which our report devotes significant attention. We provide a proof of concept for a relatively clear rule that can differentiate permissible persuasion from impermissible dark patterns.

D. GDPR

The European Union’s General Data Protection Regulation (“GDPR”) is perhaps the most ambitious privacy and security law to date. The GDPR imposes strict rules for data processing and creates significant rights for data subjects. The GDPR defines personal data as any information relating to an identifiable or identified person, and provides heightened protections for sensitive personal data, including race, health, sexual orientation, and criminal records.

The GDPR applies to all EU entities and to non-EU entities that process personal data of EU residents either in connection with an offering of goods or services or for the purposes of behavioral tracking. EU member state data protection authorities will be the primary enforcers and can assess fines as high as 4% of an entity’s global annual revenue or €20 million, whichever is greater. The GDPR also includes a private right of action, a class action right, and a third-party right of action that allows non-profits and trade associations to sue on behalf of consumers.

The GDPR distinguishes between data “controllers” and “processors.” Data controllers determine the purpose of data collection and the means of data processing. Data processors
receive and handle data from controllers. Controllers generally must comply with heightened obligations. Controllers, for example, must demonstrate compliance not only for themselves, but also for the processor. In addition, controllers are also generally responsible for monitoring their processor’s behavior. The GDPR requires that data controllers inform consumers about how their data will be used, how long the data will be kept, and how they can exercise their data-related rights. Controllers must also disclose any third party that will handle consumer data. It also requires that all privacy policies be written in clear, plain language. Furthermore, the GDPR incorporates principles of privacy by design and privacy by default. The former requires data controllers to implement privacy protective measures like pseudonymization and data minimization into the design of products and services. The latter obligates controllers to establish default rules that reduce the risks associated with the unnecessary collection, processing, retention, or dissemination of personal information.

The GDPR also provides consumers with a number of rights. Consumers can request that data controllers provide an explanation of what data they are collecting and how they are using it. In addition, consumers can request that data be corrected or erased. Though controllers may share personal data with third parties to fulfill the original purpose of processing, they may not do so for a different purpose unless the consumer consents or the controller uses a new legal basis. Personal data can also be transferred outside the EU, but generally only under circumstances where substantially equivalent privacy protections remain in effect. One important such ground is an “adequacy decision” by the European Commission, which certifies that the non-EU country has adequate personal data protection.

Finally, the GDPR requires firms to maintain certain data security practices. Data controllers, for example, must engage in data minimization by collecting only the data necessary to carry out a particular task. Firms must also implement appropriate technical measures to ensure security appropriate to the risk of accidental or unlawful destruction, loss, or unauthorized disclosure or access of personal data. Although the GDPR does not impose any specific security practices, it recommends pseudonymization, encryption, and regular security testing, among other things. In addition, personal data can only be retained for as long as necessary to fulfill the original basis for collection and processing, though there are a few exceptions for when data is used for the public interest.

E. ALI Privacy Principles Project

The American Law Institute’s (ALI) Data Privacy Principles project began in 2013 under the leadership of Paul Schwartz and Daniel Solove. The ALI project (which the subcommittee chair has worked on as Adviser) is an ambitious effort to identify best practices in data privacy and security and to use these principles to help lawmakers and regulated entities develop sound principles for managing personal information. The project has made considerable progress in the six years since it began and was approved by the ALI Membership in 2019, marking the
project’s completion. Since the process for drafting ALI Principles is highly collaborative, and the norms of the organization nudge its work product towards consensus ideas, its drafting has offered opportunities for many stakeholders to shape its content.

The core provisions of the current draft of the Privacy Principles deal with the transparency of use of personal information, the appropriate role and process for providing notice and obtaining individual consent, the scope of confidentiality duties, the importance of use limitations, and the placement of limits on data retention and downstream transfer. The Principles also advocate for user access, error correction, and data portability rights that are grounded in existing frameworks like the Fair Information Practices and the GDPR. Other provisions in the principles would impose obligations on firms that collect or process personal data to employ reasonable data security protections. The Privacy Principles project embraces the imposition of some new duties on the operators of digital platforms, and it attempts to do so in a relatively comprehensive way. Given its recent adoption, we do not endeavor here to replicate the comprehensiveness of that effort. Nor are we as constrained as the ALI is to identify existing approaches that are already working in some parts of the world or nation. We hope the approach we lay out below will supplement the ALI’s work by being both narrower in its scope and also more ambitious, nimble, and imaginative about how thoughtful legal regulation can proceed.

F. Industry self-regulation

There have been a number of attempts by firms, sectors, and trade groups to self-regulate, including attempt to adopt “trustmarks” (such as TRUSTe and BBB Online) and codes of conduct. These efforts have mostly failed for lack of adoption, limited consumer protections, and lax enforcement and monitoring.

A related approach has been the development of privacy protections through multi-stakeholder processes. The National Telecommunications and Information Administration (NTIA), for example, worked with industry groups to develop privacy guidelines for the Organization for Economic Cooperation and Development (OECD). More recently, through cooperation between government, industry leaders, and consumer advocates, the NTIA has developed reports outlining best practices for data security and the commercial use of facial recognition, among other technology topics. Multi-stakeholder cooperation is attractive in theory because solutions would reflect industry needs and knowhow as well as consumer privacy interests. Yet multi-stakeholder regulation can only work if there is scope for agreement among key stakeholder groups, incentive to reach agreement, and self-monitoring and policing. These conditions have yet to manifest themselves. Our candid impression is that multi-stakeholder processes have often been employed more as a pretext for delay than as a substantive alternative to privacy regulation.
III. Paths Forward: Default Rules, Constraints on Dark Patterns, and Improved Authentication

The enactment of a comprehensive privacy and data security law at the federal level is a major item on the congressional agenda. Various thoughtful proposals have emerged from legislators and from organizations with substantial expertise. Our hope in this section is to offer a possible central organizing principle for such legislation, one that differs in emphasis from both the American status quo and a European approach that combines prescriptive rules with enormous discretion to bureaucratic decision-makers. One aim of our proposal is to accommodate the significant heterogeneity that exists among consumers with respect to personal information while condemning corporate practices that use that heterogeneity as a pretext for manipulating consumers into making choices that undermine their welfare.

Our second goal is to create legal safe harbors for competing firms to collaborate with respect to a common threat stemming from state- and non-state actors seeking to penetrate existing data security protections. Existing efforts to facilitate the sharing of information between competitor firms have not solved the legal problems associated with this sharing, nor have they developed adequate incentives to facilitate such sharing, like well-designed clearinghouses for personal information that may be mirrored to control access to the interfaces and databases of many companies. Our proposal attempts to make progress on that key challenge.

A. Default Rules for Privacy Policies

In the United States, contractual relations between individuals and firms are typically governed by bodies of law that include both mandatory and default rules. Mandatory rules govern parts of a contractual relationship that are determined by law and that provide rights and obligations that cannot be waived. An example of such rules is the duty of good faith under Article 2 of the Uniform Commercial Code (UCC), which governs the sales of goods. Default rules are also determined by law, but they can be modified contractually by the parties. Default rules can be created by various organizations, be they public or private, and then adopted contractually by the parties. Yet it is the state that typically selects the content of both default rules and mandatory rules.

Most contract rules are default rather than mandatory, since default rules allow transacting parties to opt out and customize aspects of their contractual relationships to suit their preferences. Their main function is to provide off-the-rack rules that allocate rights and risks between parties. Oftentimes default rules mimic the terms that most contracting parties would have agreed to mutually, leaving the cost of opting out to be borne by an idiosyncratic minority. Other times default rules are information-forcing—they penalize contracting parties with private information by encouraging them to reveal such information by contracting out of the unfavorable default. Another vital function of default rules is to fill in gaps in incomplete agreements. Default rules govern when contracts are silent as to a particular obligation. Parties
that fail to specify an alternative obligation are thus governed by the default, even when their agreement says nothing about it.

In their traditional setting, default rules are designed to minimize contracting costs by supplying gap fillers and minimizing the costs of opt outs. These purposes fit somewhat awkwardly into the consumer setting because consumers are typically ignorant of both the content of default rules and many terms of the agreements they enter. Consumers might even be mistaken about the relative value of different rules. In some settings, consumers also will lack the bargaining power necessary to prompt firms to change the terms of a contract. Most consumer contracts are offered in long, standardized forms, usually on a take-it-or-leave-it basis. Privacy policies are perfect examples of this.

In other contexts, as a result of insights from behavioral economics, default rules have been designed to be “sticky” and to encourage socially desirable behaviors. Sticky defaults take advantage of the costs of opting out. A prominent example of this can be found in the context of retirement savings, where the employees are defaulted into saving plans and only a few employees will be willing to incur the cost of opting out or cancelling (Thaler & Benartzi, 2004).

As noted, default rules are designed to minimize opt-out costs and, in the context of nudges, can be sticky. A recent study (Bar-Gill & Ben-Shahar, 2019) has identified an additional cost that should factor into the optimal design of default rules: information costs. When the knowledge consumers need to make informed choices is high, consumers might opt-out, even from a sticky default, when it is not in their best interest to do so. Thus, when thinking about default rules, regulators should consider both the cost of mechanical opt outs (i.e., the cost of clicking, or itemized signing, or reading long forms) as well as the costs of becoming informed. As we explain below, firms that have a self-regarding interest in having consumers opt out of consumer-friendly defaults can manipulate consumers into waiving such protections through various types of behavioral nudges.

While default rules have been a preferred approach, reliance on mandatory rules rather than default rules may be appropriate when significant externalities are present, or when there is reason to believe that the entities formulating the mandatory rules can determine what collective choices are socially optimal.

In addition to the aforementioned reasons cautioning against a wholesale use of default rules, recent events have suggested that while relying on default rules could accommodate the heterogeneity of consumer preferences with respect to what should be done with their personal information and what tradeoffs they are comfortable with, constructing a choice architecture that facilitates well-informed and autonomous decision-making by consumers is no easy task. There is a continuum of privacy and security choices that consumers make every day, and they do so subject to constraints on their time, energy, information processing capacity, and cognitive ability. Some decisions that consumers are charged with making are straightforward enough that
boundedly rational consumers can express preferences that are meaningful and likely to reflect their own values. Under these circumstances the legal system ought to respect their autonomous choices. For example, even if consumers do not know all the consequences of turning on location services while using a navigation app like Google Maps or Waze, many of them likely understand enough of the tradeoffs to render their expressed authentic preference a meaningful and relevant data point in predicting what they want. Similarly, a consumer faced with a choice of whether to store their credit card information at a shopping site they use frequently can make a reasonably well-informed choice as to the convenience versus data-security tradeoff involved. As long as consumers are adequately informed about the relative value of the default and opt-out, empowering consumers to make these kinds of decisions, rather than enabling technocratic decisionmakers to decide for consumers, has real virtues. That being said, regulators should consider the aggregate effect of forced-choice regimes on consumers’ time and cognitive bandwidth.

At the same time there are other contexts, like those involving privacy and security choices, that are very technical or complex (and thus costly for consumers to learn about). In these contexts, consumers may be especially prone to exploitation, significant collective action problems may arise, and bargaining and preference asymmetries can emerge. In other environments, the overwhelming majority of consumers may have a known, homogenous preference with respect to aspects of a transaction that are not especially salient. Relying on consumers to vindicate their interests through some combination of notice and “choice” is unrealistic, given the other demands on consumers’ time and attention. These kinds of problems are sufficiently prevalent to render mandatory rules a key toolkit for privacy regulators, precisely because in those settings we can be less certain that whatever preferences individual consumers express via assent to boilerplate language actually further their interests.

Instances involving externalities and collective action problems present perhaps the clearest case for shifting from default rules to mandatory rules. An individual consumer’s decision to share her DNA or location may also reveal a great deal about her relatives’ genetic information or her spouse’s whereabouts. Or an individual may feel compelled to reveal personal information he would otherwise prefer to keep confidential because of an unraveling dynamic, such as when failure to disclose will induce others to assume the concealer has something negative to hide (Peppet, 2011). In these instances, deferring to even authentically selected private choices may not produce socially optimal outcomes, and there is a strong case to be made for employing mandatory rules, especially where society has confidence in the ability of the state to identify welfare-enhancing privacy and security choices.

Our emphasis here is towards developing privacy default rules that reflect the tradeoffs that consumers actually want to make, and that they are capable of making, given the costs of educating themselves, evaluating different options, and making choices. Default rules should also aid in the important task of filling gaps in the face of contractual silence. It is not uncommon
for firms to hide their information practices by disclosing next to nothing, or by making it
difficult for regulators to police unfair and deceptive practices. In such cases, market forces
sometimes (but not always and not always adequately) penalize firms for engaging in practices
that do not reflect consumer welfare interests. A complete set of rules, default and mandatory,
would fill that significant void.

1. Determining the Contents of Privacy Defaults

Existing scholarship has identified several basic approaches to determining the content of
default rules generally. The most common approach is the “majoritarian default rule” (Listokin,
2010; Porat & Strahilevitz, 2014). A second approach to determining the content of default rules
is alternatively referred to as an “information-forcing default rule” or “penalty default rule”
(Ayres & Gertner, 1989). Such an approach to setting default rules arises in settings where it is
important to elicit private information from one of the parties. The information-forcing default
rule imposes a choice by default that the parties are very unlikely to prefer. Because the
consequences for a consumer of sticking with the default rule are likely to be quite negative, the
consumer will have a strong incentive to reveal what he prefers to the company with which he is
doing business, and the company can then satisfy the consumer’s preference.

In the absence of mandatory rules or other benchmarks, firms are presenting consumers
with terms that maximize profits for the company rather than offering what well-informed
consumers would prefer if given enough time to make a decision and understand the
consequences. This strategy of selecting producer-friendly terms is quite plausibly not social
welfare maximizing, given the potential for disconnect between what consumers say they want
and what they appear to be receiving from digital platforms. Other times, firms might choose to
say nothing about particular data practices, leaving consumers (and regulators) uninformed about
what such practices are.

2. Data about Consumer Privacy Preferences and Expectations

The foregoing discussion suggests that it is worth conducting empirical research to assess
whether it is possible to identify both a consensus among consumers over firms’ practices with
regard to personal information and sufficient heterogeneity in consumer preferences to warrant
the use of default rules rather than mandatory rules. In the domain of privacy, consumers have
well-formed preferences and expectations, particularly in their interactions with familiar digital
platforms. Frequently those preferences and expectations diverge. Other times, consumers hold
incorrect beliefs regarding firms’ practices or their own attributes. To fill in what would
otherwise be knowledge gaps in this white paper, Jamie Luguri and Lior Strahilevitz launched an
empirical study of American consumers’ preferred default rules in the consumer privacy domain.
The study relied on a survey of a census-weighted representative sample of nearly 2000
American consumers recruited by the survey research firm Dynata. These survey respondents
were randomly assigned to answer a series of questions about either the level of privacy they expect or the level of privacy they desire, and they were asked to confront some of the tradeoffs associated with life in the modern world, where consumers often trade personal information in exchange for a zero-cost service. The Luguri and Strahilevitz study will be published separately this year.

The study, like previous research, reveals that there was a great deal of heterogeneity in terms of how consumers expect digital platforms to collect, use, and safeguard personal information (McDonald & Cranor, 2010; Zheng et al., 2018). For example, a supermajority of respondents understood that Amazon would store voice commands that a consumer gave to an Echo smart speaker, and among those respondents who understood such storage would occur, the majority stated that this information would be deleted either when a user actively deleted that information or when Amazon elected to do so. This understanding is consistent with Amazon’s policies. Respondents were roughly equally divided on the question of whether the law permitted Amazon to pool information with Fitbit to identify customers who were likely to be training for long-distance races. A narrow majority was inclined to believe the law permits Amazon to sell information it collects via Echo devices to companies such as music streaming services. From a review of their privacy policies it appears that Amazon probably does not sell personally identifiable Echo data to third parties like music streaming services, though the policy is not clear in this respect; there do not appear to be any limits on the transfer of aggregated data, and the policies could be changed by Amazon at any time. It is not evident from Amazon’s privacy policies that there are limits on the company’s ability to purchase data from a third party like Fitbit, to aggregate that database with Amazon’s own data, and then to identify particular kinds of consumers (e.g., long-distance runners) on that basis.

Respondents who were asked about Amazon Echo smart speakers were divided on the question of whether they would be willing to pay extra for a version of the Echo that did not share users’ personal information with other companies. About 40% of respondents said they were willing to do so, and on average they stated that they would be willing to pay an extra $50 to $60 for such a privacy-protective option after being told that the base price for an Echo was about $150. This data suggests a substantial minority of consumers might be willing to pay a third more for a smart speaker with these features, though it is possible that Amazon generates more than this amount of revenue from the information supplied by each household with an Echo. This kind of information could help inform regulatory decision-making about consumer preferences and tradeoffs. That said, while this kind of survey data is illuminating, a cautionary note is appropriate because willingness to pay expressed in a survey might not materialize when consumers make real-world purchasing decisions. Observational studies therefore would be very valuable.

When researchers examine respondents’ normative views it becomes evident that respondents view the storage and transfer of data from Amazon Echo devices as distressing. A
clear majority believe Amazon should not store such information, and there is a strong consensus among respondents that it would be undesirable for Amazon to share information it collects with a music streaming service or to merge Echo data with Fitbit data so as to identify long-distance runners.

There were similar dynamics at play when respondents were asked about the use of facial recognition data by Facebook and other social networking platforms. Most respondents understood that Facebook does use facial recognition technology to help it create templates to recognize users in uploaded photos, and that it retains this data until a user or Facebook deletes it. Users were divided over the question of whether Facebook is allowed to share facial recognition information with a third party such as a maker of police body cameras, though a narrow majority of the representative sample said the practice was not permitted (mean = 3.66 on a 7-point Likert scale, with 1 indicating definitely impermissible). When asked for a normative judgment about such information sharing with a body camera firm, respondents were much more hostile (mean = 2.40). It appears from Facebook’s full data use policy that Facebook does not engage in such third-party transfers of user information, though the prohibition applies to sales and could be altered by Facebook, at least outside of Illinois. Respondents were also close to evenly divided on the question of whether Facebook uses information from its facial recognition algorithm to tag users in photos uploaded to the site by other users (mean = 4.40)—Facebook does engage in this practice unless a user objects. Again, posing the question to consumers as a normative one about what the law should permit lowered these values by a little over one point (mean = 3.30). The divide between consumers’ expectations and their preferences is particularly stark when consumers are presented with binary choices. Fully 67% of respondents said that Facebook is allowed to store users’ facial information that it connects with its facial recognition technology, but only 36% of respondents said that Facebook should be able to store such information.

The same basic pattern played out with respect to Google and its collection and storage of information from Google Maps. A super-majority of respondents believe that Google retains data about a Google Maps user’s geolocation after the completion of the trip, and that this information is retained until either Google or the user elects to delete it. A clear majority of respondents believe that Google Maps is permitted to track a user’s location whenever the phone is turned on, even when the app is not in use, as long as the user consents to this when first using the app. Respondents were pretty evenly divided over questions involving Google’s sharing of geolocation information collected through Google Maps. A little more than half of respondents thought Google was legally permitted to share data about individual users’ whereabouts with stores and restaurants that wanted to deliver advertisements to customers who were nearby. And a little less than half of respondents thought Google was legally permitted to sell data it collected about individual users “to provide other services to consumers free of charge.”
Again, respondents’ expectations differed from their normative preferences. Clear majorities of respondents objected to the sharing of Google Maps information with nearby restaurants and stores. Noting that Google would use revenue earned from selling that user information to provide other services (like Google Maps or Gmail) to consumers at a zero price did not cause that assessment to change. Similarly, respondents did not believe that Google should be permitted to retain information about a trip that was taken with the assistance of Google Maps once the trip had ended. Most respondents thought it was wrong for Google to collect geolocation information from phones that were not using the Google Maps app notwithstanding users’ previous authorization of such data collection.

This disconnect between users’ expectations and their preferences plays out similarly with respect to other kinds of privacy scenarios presented to consumers in the same study. The results from studies involving the use of genetic information supplied to 23andMe or cell tower geolocation information supplied to Verizon Wireless or Gmail storage of user emails were broadly similar to the results described above, except insofar as consumers were particularly hostile to the sharing of genetic information by a genetic testing firm (e.g., sharing information with pharmaceutical companies to help them research new drugs and treatments or selling genetic information in order to lower the prices it charged consumers for genetic testing). Moreover, the study also measured the effects of posing questions to consumers involving established companies like Amazon, Facebook, and Google versus new start-ups entering the same industry in order to compete with those highly successful firms. By and large, consumers’ preferences and expectations were similar regardless of whether a dominant firm or a start-up was involved. The consistent similarity of those responses helps ameliorate what would otherwise be methodological concerns about how to elicit an accurate reflection of consumer preferences using survey instruments.

3. Toward “Consumertarian Default Rules”

We propose that the law select the contents of such default rules based on the results of well-designed, scientifically rigorous studies that elicit consumer preferences, opt-out costs, and knowledge of the rules and alternatives, as well as ignorance and biases of such rules’ potential costs and benefits. Where consumer preferences and expectations match firm preferences and practices, those choices should be adopted as majoritarian default rules. Where consumer preferences and expectations diverge from firms’ preferences, it often will be appropriate to use the consumers’ preferred starting point as a default rule, establishing rights that can be waived if firms are able to convince consumers that waiving those rights is worthwhile. Though our proposal mirrors neither the substance nor the structure of the GDPR, the expectations-based approach we outline here is compatible with it. Under Recital 47 of the GDPR, “the reasonable expectations of data subjects based on their relationship with the controller” may create a legal basis for the processing of personal information. The GDPR does not develop a clear methodology for determining how data subjects’ reasonable expectations are to be determined,
and in that sense the data-driven approach we outline offers the comparative virtue of greater clarity and predictability.

To be sure, such an approach is not devoid of implementation challenges. What should happen in instances like those described above, where there is a divergence between what consumers say they want and what they expect? There are cases to be made for using either consumer preferences or consumer expectations where the two diverge. The legal system might determine the default by averaging the two, or by adopting either the preference default or expectation default depending on the context of the substantive rule at issue. The law might use preferences to set the content of the default rule when consumer expectations do not match actual company practices or when a new technology uses personal data in novel ways. In some other instances, consumers’ preferences may be unrealistic (because imposing their preferred limitations on the use of data would make it impossible for a company offering a useful product to be profitable), too abstract (because they are not tied to price versus privacy tradeoffs), or unreliable (because they are based on mistaken consumer assumptions, such as when consumers misunderstand the fundamentals of the technology they are using). In these varied contexts, consumer preferences and expectations could be relevant rather than decisive in determining the content of the appropriate default rule.

Consumers should be able to waive these default protections in instances where their counterparty convinces them to do so, provided that the choice architecture employed by the firm is non-manipulative and enables consumers to make well-informed decisions about tradeoffs. We propose a framework below, in our discussion of dark patterns, for determining whether a particular choice architecture complies with this standard.

There is a sense in which this approach is consistent with the lessons of law and economics, in which majoritarian default rules should be employed to minimize transaction costs. For example, if both a digital platform and its customers are engaged in a transaction where collecting personal information is necessary to facilitate the underlying service that customers want and expect from the platform, then it is unproblematic to impose such collection as a term of the contract. Doing so economizes on the costs of articulating that shared preference in a written contract or privacy policy.

Majoritarian default rules maximize contracting parties’ joint welfare by selecting rules that both parties want. Selecting consumer preferences or expectations as a starting point will often be preferred only by parties on one side of the transaction. A more apt moniker for this approach to setting default rules is “consumertarian default rules”—selecting a default rule that is preferred by the majority of unsophisticated parties in a transaction, though perhaps not by the majority of sophisticated counterparties.

Conceptually, consumertarian default rules have more in common with information-forcing default rules than they do with majoritarian default rules. Where a firm does not view the
choices preferred by a majority of consumers as a desirable contractual arrangement, it has two options. Either it can stop offering the good or service in question to consumers, or it can devise ways to convince consumers to waive the protections afforded them by default. The available evidence suggests that consumers can be convinced to waive legal rights that the legal system assigns them by default. For example, research by Lauren Willis shows that banks have been quite effective at convincing consumers to waive default protections conferred on them by federal law concerning bank overdraft fees. She finds that firms can be successful at overcoming “sticky” defaults when (a) they have a strong motivation to do so, (b) they have opportunities to ask consumers to waive their rights, (c) consumers find the decision-making environment confusing, and (d) consumer preferences are well-defined (Willis, 2013).

To the extent that firms are convincing consumers to waive their default protections by confusing them, pestering them, or misleading them, there is no good justification for honoring such waivers. But sometimes a firm can and does convince consumers to waive rights that they have by default by providing consumers with goods or services that they value more than they value those default protections. Indeed, essentially every successful digital platform that employs zero-dollar-pricing has done exactly that by convincing consumers that it is in their interest to trust a third party with sensitive personal information to which the third party would otherwise lack an entitlement. In light of these dynamics, we can expect that the initial assignment of privacy-friendly default protections to consumers would not necessarily result in most consumers keeping those entitlements. Large numbers of consumers could elect to waive those protections in exchange for services they value more from digital platforms. For this reason, regulators should pay attention to the cost of opt-out as well as the costs of consumers becoming informed about the value of the opt-out relative to the default. Ignorant opt-out can result in welfare losses (Bar-Gill & Ben-Shahar, 2019).

That said, assigning these protections to consumers would function as a constraint on firms that seek personal information from their customers. So long as some well-identified, welfare-enhancing practices become mandatory, asking consumers to waive particular consumertarian default rights means imposing on their customers’ time. We propose below stringent constraints on what constitutes a waiver of a right protected by a consumertarian default rule. Waivers would have to meet the standard that prevails in American courts where key rights are at stake—there must be a knowing and voluntary waiver of a right. Meaningless rituals that some courts have deemed sufficient to create a contract (e.g., presenting consumers with an avalanche of complicated text that the firm knows nearly no consumers will read) would not satisfy this heightened standard. Securing these kinds of waivers operates as a time tax on both firms and consumers. Firms might not want to initiate those kinds of conversations very often, and they will not want to do that with respect to low-stakes issues. Rather, they will of necessity pick their battles. For these reasons, in proposing that consumertarian default rules become the default for consumer privacy and security, we regard the sticky nature of default rules as a
feature rather than a bug. Asking consumers to waive rights would squander some good will that firms have accumulated with consumers and would risk losing customers by adding friction to the user experience. Given that such waivers would need to be narrow in their scope, firms would, at a minimum, pick their battles, turning those default rules that firms could live with into de facto mandatory rules.

Moreover, contractual silence will no longer be a benefit for firms where personal data is concerned if a company is using personal data in ways that counter consumer expectations and preferences. Rather, such silence will become an obstacle that firms need to overcome if the benefits of obtaining meaningful customer consent are high enough. Some firms will decide that the process of informing their customers of what they want to do and why they want to do it will spook enough of their customers away from using their good or service to render it unwise to seek permission to waive a default. Requests that would reveal unsavory or controversial data practices may bring unwelcome regulatory scrutiny as well.

In a sense, then, implementing consumertarian default rules will provide some of the benefits of information-forcing default rules. By selecting default rules that firms often will not prefer, these rules will prompt firms to provide information to consumers and regulators about why retaining their entitlements may not be worthwhile. The end results may be conversations in which consumers wind up with more information about companies’ use of their personal information and the associated tradeoffs. As a result, even instances in which consumers elect not to waive their rights could result in learning opportunities for consumers as well as vehicles for reflection. All of this raises hard questions about whether these conversations can ever be structured in a way that is fair, informative, and satisfying to consumers. We now turn to those issues.

B. Dark Patterns and Manipulation

Dark patterns are user interfaces that can confuse users, make it difficult for users to express their actual preferences, or manipulate users into taking certain actions. The term “dark pattern” was coined by user interface designer Harry Brignull in 2010 and is widely used among computer scientists. Behavioral economists have tended to use the term “sludge” (i.e., an evil nudge) to describe the same phenomena, though the category of sludge is not limited to online interactions (Sunstein, 2019). Legal scholars have also analyzed similar phenomena, often using the term “market manipulation” (Hanson & Kysar, 1999; Calo, 2014).

Every reader of this report will have encountered numerous dark patterns in their online activities. For instance, when a website offers users a chance to sign up for a recurring newsletter, the “accept” button might be much easier to find than the “decline” button. Worse still, the design of the webpage may appear to require a user to sign up for the newsletter in order to continue browsing the site. A firm might employ ambiguous language that confuses consumers into sharing more personal information than they intended, or it might require
consumers who want to select popular settings that protect their privacy but decrease firm profitability to jump through a large number of hoops in order to do so. Or a shopping site might sneak extra goods a consumer did not select into a virtual shopping cart by default, forcing the consumer to delete the items to avoid purchasing them. In these cases, the design interface confuses users about their possible choices or makes unrealistic assumptions about what consumers are likely to prefer. Dark patterns appear to be proliferating, both in terms of their prevalence in e-commerce and the variety of different techniques employed. A recent semi-automated analysis of popular shopping web sites found that more than 11% of sites employed at least some dark pattern strategies (Mathur et al., 2019).

The effectiveness and proliferation of dark patterns is partly a product of technology. To start, many interactions are mediated by digital interfaces. People use smartphones and computers to complete many tasks and transactions that were previously done in person. The rise of digital mediation provides many opportunities for interface designers to rely on dark patterns to influence user behavior.

Many of the inherent problems with dark patterns have implications for information privacy. Dark patterns are often used to direct users toward outcomes that involve greater data collection and processing. Additionally, the proliferation of data-driven computational methods allows firms to identify vulnerabilities of users and to target specific users with these vulnerabilities.

While dark patterns come in a variety of different forms, their central unifying feature is that they are manipulative, rather than persuasive. More specifically, the design choices inherent in dark patterns push users towards specific actions without valid appeals to emotion or reason.

1. **Defining Actionable Manipulation**

The line between manipulation and persuasion is sometimes difficult to draw, even from a purely ethical perspective. Here, we propose a framework that we believe will allow legislators, regulators, and courts to define the category of manipulations warranting legal action in a way that is workable and defensible on both economic and moral grounds. The dark patterns that we are concerned with can be divided into two (somewhat overlapping) camps: manipulation by transaction costs and manipulation by targeting certain sorts of vulnerability. Both create market failures by obstructing the market’s responsiveness to consumer preferences. As the sparse dark patterns academic literature emphasizes, dark patterns are aimed at “System 1” thinking, which takes place in decision-making contexts where information is processed quickly and automatically, with little consideration and cognitive effort. Dark patterns will be much less effective when consumers are making “System 2” decisions that are characterized by slow and deliberative weighing of pros and cons (Bösch et al., 2016). Dark patterns that target and exploit certain sorts of vulnerability raise additional moral objections. Both implicate the sorts of consumer protection issues routinely addressed by legal regulation.
a. Transaction Costs Dark Patterns

Some dark patterns—through their design features—impose transaction costs unnecessarily on users in order to get them to behave in a way that is advantageous to the pattern designer (and often contrary to a consumer’s own interests or wishes). Transaction costs dark patterns are quite common and, for the most part, easily recognizable. Examples include requiring a user to uncheck multiple boxes to unsubscribe from some website feature, or designing a frictionless process for opting in to some web service while making it difficult and time consuming for users to opt out. An app might repeatedly prompt users to opt in to sharing their locations, but then never ask users who eventually accede to the requests to stop sharing their locations. While transaction costs are endemic to market transactions, they are always wasteful. Transaction costs dark patterns of this sort go further, however, by imposing unnecessary transaction costs in an attempt to manipulate consumer choices.

While users across the board will suffer the market waste and distortion caused by transaction costs dark patterns, some users will experience the increased transaction costs more acutely. Specifically, users who are less tech savvy or do not have the extra time to devote to navigating byzantine opt out procedures will be less likely to persist so that they can express their authentic preferences in the transaction. Further, these groups may preferentially include those who are already at some social disadvantages, such as elderly people with less developed technology skills or less educated people.

Identifying transaction costs dark patterns should be relatively straightforward in most cases. The imposition of unnecessary transaction costs is often apparent on the face of the transaction, at least as a prima facie matter. For example, if the opt-in design is seamless with limited transaction costs, while the opt-out process is burdensome, and if most users would prefer to opt out when given an easy option to do so, then there is a prima facie case that the website operator is merely adding costs to encourage users to behave according to the website operator’s wishes. Similarly, if there is an obvious design that could reduce transaction costs for users but, instead, a website chooses a design that requires additional transaction costs for users, then the website is likely employing a transaction cost dark pattern to influence user behavior. Discovery or investigation may sometimes even reveal direct evidence of this sort of manipulative deployment of transaction costs. Moreover, while there will always be borderline cases, potential liability for transaction costs dark patterns should incentivize designers to internalize consumer transaction costs to some extent. Since they are the only parties who can mitigate this social waste, this internalization of costs is a salutary effect.

b. Manipulation by Targeting Vulnerabilities

Dark patterns that manipulate individuals by targeting certain sorts of vulnerabilities are particularly troubling. Examples of the sort of behavior include the targeting of advertisements based on acute emotional vulnerabilities, such as the recent death of a child, or on specific
health-related vulnerabilities, such as those related to episodes of mania or depression, as well as techniques tailored to exploit vulnerabilities of particular social groups. A person who struggles with bipolar disorder may be susceptible to impulse purchase during a manic episode. These dark patterns are admittedly more difficult to identify and assess than transaction cost dark patterns because differences between individual consumers make it more difficult to distinguish unacceptable targeting of vulnerabilities from more morally benign, or at least long accepted, persuasion tactics of traditional advertising.

To be sure, dark patterns need not be personalized. Some dark patterns are troubling because they target vulnerabilities that are pervasive, rather than particular to subsets of users. Insights from behavioral economics have demonstrated that people also have decision-making vulnerabilities—or cognitive biases. One such bias, called loss aversion, may make consumers feel the harms associated with losses more intensely than they feel the benefits associated with gains. Firms may exploit this bias by falsely indicating that only a few units of the item a consumer is examining remain in stock, so the consumer had better hurry up and make a purchase before they disappear (Mathur et al., 2019). While recognizing that there is a disputed line between consumer protection and paternalism, we put forward a framework for defining legally actionable dark patterns of this sort that we argue will permit courts and regulators to make distinctions that are similarly clear and predictable to those made in other consumer protection law. Each of these factors will be relevant in particular contexts; rarely would one factor be decisive.

Importantly, exploiting cognitive or emotional vulnerabilities does not have a uniform moral or societal salience. Put differently, the moral wrongness and social unacceptability of exploiting vulnerabilities differs based on the type and degree of vulnerability. Some situations or characteristics simply make individuals open to persuasion in morally benign ways. For instance, behavioral data may uncover that a person is usually hungry after getting off work at 11pm. As a result, this person is served ads for restaurants with takeout that are within a 3-mile radius. Similarly, we accept that marketers will exploit some widely held cognitive biases. For example, advertisements often employ the bandwagon effect in order to sell products. If advertisers’ representations about a product’s popularity are truthful and non-misleading, the advertisers’ tactics are not appropriately understood as dark patterns, even though consumers might assign undue weight to the product’s popularity and insufficient weight to expert assessments of its quality. For similar reasons, tactics exploiting many relatively benign and widespread sorts of weaknesses, such as the temptation to eat junk food late at night, have generally been considered morally acceptable.

Exploiting other sorts of vulnerabilities, however, raises graver moral and societal concerns. For instance, exploiting the emotional weakness that comes from losing a child has significantly deeper moral resonance than exploiting late night hunger. Similarly, exploiting
mental health issues or the particular technological unfamiliarity of many elderly individuals is less acceptable than exploiting the bandwagon effect.

One approach for identifying the kinds of vulnerabilities that might rise to the level of liability when manipulated is to identify vulnerabilities revealed through categories of information protected as “sensitive” in positive law. For example, laws treat information about sexual orientation, information about disease and other health matters, and information about children as worthy of heightened protection. Manipulating someone based on information that falls into one of these sensitive classes might be likelier to be deemed worthy of legal action.

c. Hiddenness

Manipulative dark patterns are often designed to undermine a user’s deliberation process covertly, so that users are unaware that their actions are being manipulated (Susser et al., 2019). Often, these sorts of dark patterns involve outright deception, selective disclosure, or misdirection. For example, a number of online shopping sites inform users that “Jane in Anchorage” just purchased the item a consumer is scrutinizing online, but in actuality these updates are bogus—the software randomly generates a list of names and locations to make it appear that other users are buying the items in question. Similarly, shopping sites falsely indicate to consumers that particular items are “in high demand” or “in very low stock” to prompt consumers to purchase them immediately, without further research or deliberation, and it turns out that some web sites describe the vast majority of their inventory in that manner (Mathur et al., 2019). By contrast, persuasion is generally not hidden. Instead, persuasion’s appeals to emotion or reason are overt, even if subtle. The idea that consumers should be generally aware when others attempt to persuade them for commercial purposes is reflected in regulations requiring search engines and media to distinguish between paid advertising and other content. At bottom, hiddenness—or whether a person is aware of the influence—is a factor that weighs in favor of identifying a design feature as a manipulative dark pattern.

d. Vulnerability

Design features aimed at manipulating user choices can now often be targeted based on personal information that goes well beyond the sort of general demographic information previously available to market participants. Targeting heightens concerns about manipulative dark patterns in several ways: It can enhance manipulative power by focusing on the specific vulnerabilities of particular individuals, identify areas of vulnerability that were not apparent to traditional advertisers and, by isolating individuals’ experiences, make it more difficult for them to detect manipulative tactics and account for them in decision-making. Of course, targeting exists on a spectrum of granularity that affects the extent of its impact. At the most specific, dark patterns can be targeted to distinct individuals. Other dark patterns can be targeted to classes of people, such as people living in a certain area.
Targeting can exacerbate the potential for morally and socially unacceptable exploitation of vulnerabilities. Targeting can allow more granular and specific identification of individual vulnerabilities, for example by drilling down to a sub-group of elderly individuals who have been susceptible to manipulative tactics in the past. Targeting can also increase the power of manipulative tactics for particular individuals. For example, if targeting the bereaved based on gathering information from obituaries (or listening to police radio) is distasteful or unacceptable, targeting based on the immediacy and level of personal detail carried by social media is surely more so. Similarly, targeting may allow not only the exploitation of the fact that an individual suffers from bipolar disorder, but also the detection of when that individual is going through a manic or depressive phase.

2. A Data-Driven Approach to Spotting Problematic Dark Patterns

So far, our discussion of dark patterns has been theoretical and anecdotal. Indeed, a significant problem with writing about the topic of dark patterns is the dearth of literature on the subject beyond some very helpful papers that develop typologies or provide examples of dark patterns. (Acquisti et al., 2017; Bösch et al., 2016; Gray et al., 2018; Mathur et al., 2019; Zagal et al., 2013). A helpful taxonomy, developed by Christoph Bösch and co-authors, identifies classic types of privacy dark patterns including bad defaults (which we propose a framework for identifying above, and one example of which is a choice between “Yes” and “Not Now” rather than “Yes” and “No”), privacy zuckering (i.e., providing users options to adjust their privacy settings that are needlessly complex, granular, or confusing), forced account registration (seeming to require registration to use a service), hidden fees or terms added at the end of a long transaction (how did that wind up in my online shopping cart?), forced account preservation (making it impossible to delete accounts once created), and address book leeching (requesting users’ contacts at the time of activation and then spamming users’ contacts with email invitations).

As useful as this research developing taxonomies and identifying examples of problematic dark patterns has been, independent researchers are hamstrung by a frustrating dynamic. Firms that employ dark patterns know how effective they are. Academics and policy-makers, by contrast, have only limited data on that front. To correct that unfortunate asymmetry, we initiated a new experimental academic study to determine exactly how successful dark patterns are at bending consumer will. This study, Shining a Light on Dark Patterns, to be published separately by Jamie Luguri and Lior Strahilevitz later in 2019, provides eye-opening evidence about the effectiveness and consequences of dark patterns, be they of the subtle or blatant variety.

a. Commissioning a New Experiment on Dark Patterns

Luguri and Strahilevitz created a novel survey instrument that employs various dosages of dark pattern techniques to a large census-weighted sample of Americans (n = 1762). The first
part of the experiment was a survey instrument in which respondents were asked for their preferences or expectations across a host of issues involving privacy and data security. This data was used to inform our analysis of consumeritarian privacy defaults in the above discussion. After respondents completed answering a battery of questions soliciting their views about privacy, every participant in the sample was shown a screen indicating that our software was “Calculating your privacy propensity score. Please wait.” (This was a ruse.) After a short delay, all respondents were informed that our algorithm had identified them as consumers who had a “heightened concern about their privacy.” Respondents were also told that using their IP addresses and other information they had already provided as part of the survey (their phone numbers, etc.) we were able to uniquely identify their mailing address. Experimental subjects were further informed that the researchers had partnered with the nation’s largest data security and credit monitoring firm, which had automatically signed them up for a data protection and credit history monitoring plan. This service would be offered to consumers for free for six months, but after the six-month trial period, consumers would be charged a monthly fee (randomly varied to show either $2.99 per month or $8.99 per month), though they could cancel the service at any time. In other words, we led our experimental subjects to believe that they were about to be signed up for a service that most of them did not seek out. The experiment was carried out after receiving approval from the University of Chicago I.R.B. to engage in this deceptive conduct.

As part of the experimental manipulation, experiment participants were randomly assigned to one of three conditions. The first group (which we will call “easy”) were shown a simple yes-no screen and asked whether they wanted to accept or decline this data protection service from the researchers’ corporate partners. Neither yes nor no was pre-selected. Respondents who selected “Accept” were deemed to have accepted the service.

The second group (which we will call the “mild” dark pattern) were shown somewhat different options. Instead of boxes with the options labeled “Accept” and “Decline” these consumers were shown boxes labeled “Accept and continue (recommended)” and “Other options.” The “Accept and continue (recommended)” box was pre-selected, so a user who wanted to select that option would not need to toggle the cursor position. If respondents selected “Other options” they were shown a screen with two options. Option one read “I do not want to protect my data or credit history.” Option two read, “After reviewing my options I would like to protect my privacy and receive data protection and credit history monitoring.”

Members of this second group who selected “I do not want to protect my data or credit history” were shown one last screen as part of the experiment, in which they were given the prompt “Please tell us why you decided to decline this valuable protection.” They were shown the following options and asked to select one:

- My credit rating is already bad (1)
Even though 16.7 million Americans were victimized by identity theft last year, I do not believe it could happen to me or my family (2)

I’m already paying for identity theft and credit monitoring services (3)

I’ve got nothing to hide so if hackers gain access to my data I won’t be harmed (4)

Other (minimum 40 characters) (5): _______________________

On second thought, please sign me up for 6 months of free credit history monitoring and data protection services (6)

Luguri and Strahilevitz framed these choices to be manipulative in an effort to sway some people to opt for option 6. That is, they tried to identify weak reasons for rejecting our service rather than compelling ones, and some of the options were framed in a way that might make respondents have second thoughts about declining the service.

Respondents who selected “Accept and continue …” on screen one or “After reviewing my options …” on screen two or “On second thought …” on screen three were deemed to have accepted the service. All other respondents were deemed to have declined it.

The third group (which the authors call the “hard” dark pattern condition) were exposed to a litany of interventions in sequence. The first two screens respondents in the “hard” condition saw were identical to those that the “mild” group saw. After those two screens, respondents who were attempting to decline the service were shown a screen with this text:

You indicated that you do not want to protect your data or credit history. We would like to give you a little information so that you can make an informed decision. **What is identity theft?** Identity theft happens when someone steals your personal information to commit fraud. The identity thief may use your information to fraudulently apply for credit, file taxes, or get medical services. These acts can damage your credit status, and cost you time and money to restore your good name. You may not know that you’re the victim of ID theft immediately.

Accept data protection plan and continue (1)

I would like to read more information (2)

There was a countdown timer at the bottom of the screen that prevented respondents from selecting option 2 until ten seconds had passed. Respondents who selected option 2 were shown two more similar screens with text describing the consequences of identity theft and the prevalence of identity theft in the United States, with the same countdown timer and the opportunity to accept the data protection plan on every screen.
Respondents who kept refusing to accept the data protection plan were then shown a confusing prompt, which read as follows:

If you decline this free service, our corporate partner won’t be able to help you protect your data. You will not receive identity theft protection, and you could become one of the millions of Americans who were victimized by identity theft last year.

Are you sure you want to decline this free identity theft protection?

- No, cancel
- Yes

The ambiguity problems with this prompt are significant and intentional. Consumers had to select “Yes” to decline the data protection plan. Selecting “No, cancel” would cause them to be signed up for the service. The reference to the concept of cancellation was designed to trick people who thought they were selecting that box on the mistaken assumption that doing so would decline the data protection service.

Finally, respondents who indicated “Yes” above were shown the same final screen that participants in the “mild” condition saw, asking them why they had declined the service and providing them with one last chance to reverse course.

The dark pattern experiment ended whenever respondents provided either a definitive “Accept” or “Decline” answer, though for obvious reasons declining was more cumbersome than accepting for two-thirds of the sample. At this point, all respondents were asked a few more questions and debriefed on the exercise. First, they were asked to describe their current mood, using a 7-point Likert scale ranging from 1 (“Happy and relaxed”) to 7 (“Aggravated and annoyed”). Second, all respondents were told: “Some survey participants may be contacted to do a follow up survey by the same researchers. Are you interested in potentially participating?” Again, respondents could check a box corresponding to a 7-point scale ranging from 1 (“Not at all”) to 7 (“Extremely interested”). Third, all respondents were asked: “How free did you feel to refuse the offered data protection and identity theft plan?” with choices ranging from 1 (“Not at all free to refuse”) to 7 (“Completely free to refuse”). Two more prompts asked respondents how seriously they took this survey and asked them to share any questions, comments or concerns about the survey. Some respondents used that final prompt to share their displeasure with what the researchers had done, though most left this final prompt blank.

Only after this final prompt were experimental subjects told the truth. The experimenters did not partner with a data protection company. They had not signed participants up for a service. They did not and would not share their responses or demographic information with anybody. Their data would be stored only in de-identified form. Luguri and Strahilevitz told participants exactly why they were interested in dark patterns and required them to click “I understand” in
order to complete the survey. This final page also provided the researchers’ contact information, though none of the participants contacted the researchers.

b. What Story Does the Dark Pattern Data Tell?

The results of the study are striking, demonstrating the powerful force that even mild dark patterns can exert on consumer choice. In the easy condition, approximately 11% of respondents accepted the data protection plan and 89% rejected it. This statistic probably overestimates the consumer demand for a product of this kind since respondents were told that they had already been signed up for the service (potentially triggering loss aversion) and a pricing system was employed in which customers would pay nothing for six months but might have the onus of cancelling subsequently to avoid charges (potentially triggering hyperbolic discounting). The researchers had also spent ten minutes priming respondents to think about privacy and security, though that prime likely cut in cross-cutting directions as the researchers simultaneously claimed to be invading respondents’ privacy in order to help protect them against identity theft. Based on the structure of the set-up, 11% is appropriately understood as the ceiling for the percentage of consumers who might be interested in the offered product on its own merits.

What happens when the researchers started employing dark patterns to boost acceptance? Even mild dark patterns proved very effective. In the mild condition, 26% of respondents accepted the data protection plan. This corresponds to a 228% increase in data protection plan acceptance compared to the control group with easy opt-out. Thanks to the experimental design, it is possible to identify the point at which different respondents agreed to the data protection plan. More than three-quarters of accepting respondents accepted the service on screen one (which offered a choice between “Accept and continue (recommended)” and “Other options,” with the former choice pre-selected). Another 23% agreed to accept the data protection plan on screen two. Nearly everyone who made it to screen three (the list of largely bad reasons for declining the service, with one final chance to say yes) selected one of the boxes that amounted to a definitive rejection of the data protection plan. Just three respondents relented “on second thought.”

The effects of the hard condition dark pattern were even more pronounced. A battery of dark patterns convinced nearly 42% of respondents who completed the survey (217 out of 518) to accept the same data protection plan that just over 11% agreed to accept in the easy condition. This figure represents a 371% increase in the percentage of respondents who wound up accepting the plan compared to the easy condition control group. Once again, the first screen did by far the most work, with approximately 65% of the accepting respondents in the hard condition doing so at the outset. The second screen accounted for another 10% of those accepting, and the three screens on which consumers were required to slowly read more information about identity theft combined to peel away another 19% of those who wound up accepting. A confusing “Yes –
“Cancel” prompt seems to have been responsible for another 11% of acceptances. And once again, virtually nobody (just 1 respondent) who made it to the last screen in the hard condition surrendered at that point.

It is worth emphasizing that different populations face varied vulnerabilities to dark patterns. In the Luguri and Strahilevitz “Shining a Light on Dark Patterns” study, there was a significant relationship between education and acceptance. Specifically, more highly educated people were more likely to decline the data protection plan. This relationship was driven by the mild and hard dark pattern conditions. In the easy / control condition, education did not significantly predict whether participants declined the data protection plan. However, when dark patterns were employed in the mild and hard conditions, the more educated the participants were, the less likely they were to accept the data protection plan. This data is suggestive of a troubling prospect—not only do dark patterns prompt consumers to sign up for services they do not really want, but the least educated Americans are most likely to be manipulated successfully.

Before deciding to initiate this project, Luguri and Strahilevitz anticipated that the effects of dark patterns would be significant, but they substantially underestimated the magnitude of the effects. The data tells other surprising stories as well. Recall that Luguri and Strahilevitz randomly varied the cost of the data protection plan, so that half the sample would be signed up to pay $2.99 a month after the six-month trial period ended and the other half would be signed up at $8.99 per month. Raising the stakes made no difference, as the high-stakes and low-stakes conditions are statistically indistinguishable. This result seems to be in some tension with what the neoclassical model of economics would predict, even accounting for the signal of quality that could be sent to consumers by a higher price.

A key consideration in evaluating the wisdom of legal interventions is determining whether a market failure exists. The data that Luguri and Strahilevitz gathered on how annoyed participants felt and how willing they were to participate in future research studies by the same experimenters was designed to gather pertinent information on that front. Here the lesson seems to be that mild dark patterns produce little customer backlash, even while convincing many consumers to sign up for a service they otherwise would not want. Aggressive dark patterns annoy customers who refuse services and whose costs of saying no are increased, but they do not seem to trouble customers who are manipulated into saying yes. Among respondents who wound up accepting the data protection plan, there were not robust significant differences across the easy, mild, and hard conditions. But among respondents who wound up declining it, there were significant differences between the hard condition, on the one hand (4.20 mean, SD 2.06), and the easy (2.88 mean, 1.52 SD) and mild (2.95 mean, 1.65 SD) conditions on the other. The same patterns emerged when researchers asked about willingness to be a repeat customer.

This quantitative data is corroborated by other data collected as part of the experiment. For example, at any stage in the survey, experimental subjects could close their browser window with the survey incomplete. If they opted to do that, they would not get paid by the survey...
research firm the researchers hired. In the mild dark pattern condition, just 9 people opted to do so. In the hard dark pattern condition, that number jumped to 65 people. The questions that forced respondents to read material about identity theft with a countdown timer accounted for the majority of these departing subjects in the hard condition. Moreover, the open-ended question asking for comments and questions generated positive or banal comments in the easy and mild conditions and a barrage of outrage and expletives from a minority of the sample in the hard condition.

These are largely lessons that digital platforms and other sophisticated entities must have learned by now, even if policymakers and academics are only now understanding the magnitude of the manipulation that can occur via dark patterns. From our perspective, it’s the mild dark patterns—like labeling an option that is good for a company’s bottom line but maybe not for consumers as “recommended” or by providing initial choices between “Yes” and “Not Now”—that are most insidious. This kind of decision architecture, combined with the burden of clicking through an additional screen, managed to more than double the percentage of respondents who agreed to accept a data protection plan of dubious value, and it did so without alienating customers in the process. As a result, consumers were manipulated into signing up for a service that they probably did not want and surely did not need. More broadly, we can say the same things of the kinds of dark patterns that are proliferating on digital platforms. These techniques are harming consumers by convincing them to surrender cash or personal data in deals that do not reflect consumers’ actual preferences and may not serve their interests. The harms from dark patterns are akin to those associated with consumer fraud. The case for treating these widely-employed psychological strategies for securing consumer consent as unfair and deceptive practices in trade is quite strong. The case for deeming resigned acceptance under these terms as consent is very weak.

3. Legal Framework

The framework we propose could be implemented via specific federal or state “dark pattern” legislation, by legislatively extending provisions such as the “unfairness” prong of section 5 of the FTC Act or, in some contexts, by interpreting and applying existing consumer protection law.

The call for legal intervention over dark patterns is not a radical break from other consumer protection efforts. Consider, for example, the FTC’s Do Not Call Registry. This registry allows people to designate their telephone numbers so as to place them off-limits to unwanted sales calls. In part, the registry is a response to excessive influence. Marketers would often call during dinner in order to interrupt people and make them more likely to agree to whatever service was being offered, just so they could quickly return to their family. In part, the registry was designed to protect people’s time—few people purchased goods and services over the phone, and continually saying no to telemarketers became a nuisance for consumers.
Historically, regulations also have protected consumers from inappropriate or excessive influence in market transactions, giving consumers “cooling off” periods to cancel transactions that were prodded by high-pressure sales tactics or involve high stakes or might prompt substantial regret on the part of consumers. Federal law generally provides consumers with the right to rescind transactions within three business days under circumstances in which high-pressure sales tactics are likely to be employed, such as door-to-door sales (16 C.F.R. § 429.1), home equity loans (15 U.S.C. § 1635), and student loans (15 U.S.C. § 1638(e)(7)). There are also state laws in various jurisdictions that provide 3-day windows to rescind contracts resulting from door-to-door sales, contracts for gym memberships, or even dance lessons. New York has a mandatory rule that gives consumers rights to rescind transactions resulting from telemarketing. See NY Pers. Prop. Law § 442.

Both the Do Not Call Registry and “cooling off” laws have the effect of insulating vulnerable people from undesirable pressure in sales transactions. The Do Not Call Registry protects people from confusing sales pitches that happen over the phone. Similarly, “cooling off” laws protect people by giving them a mechanism to cancel transactions after the fact. In particular, many vulnerable people may not feel comfortable declining a sales pitch that happens at their residence, especially if they live alone. At bottom, both consumer protection efforts dilute some sales pressure in ways that are particularly beneficial for vulnerable people.

In this section, we are concerned with a subset of dark patterns—ones that warrant legal intervention, yet may be deemed non-deceptive and thus arguably fall outside of existing consumer protection regimes. Some user interfaces may be inconvenient for some users but fail to cross a threshold of manipulation that we would argue should be considered legally actionable dark patterns. For example, suppose that most users of a software program want the application to be rendered in full color, but a small subset of users who are colorblind prefer that it be rendered in a format that enhances its usability for users who have reduced sensitivity to green light. There should be no legal liability if a company renders its application in full color by default and then makes a user who has deuteranomaly (green light colorblindness) navigate through several screens in order to toggle on an option that makes the application easier to read for that subpopulation. That is a defensible choice, given the preferences of the user base and existing technologies. If the option to change the way the application appears is made too prominent, it is likely that users who are not colorblind will opt out of the default setting unintentionally and be less satisfied with their experience using the application as a consequence. Therefore, the user interface described above would not be categorized as a dark pattern, and no legal sanctions should attach to such a design.

At the other end of the spectrum, some dark patterns fit neatly within current regulatory strictures against misrepresentations and deceptive practices. The FTC, in particular, has a legislative mandate to police unfair or deceptive trade practices and has pursued enforcement actions against deceptive dark patterns. The FTC has had the most success invoking section 5’s
prohibition on deceptive practices in trade when consumers were tricked into signing up for goods or services. In three federal court of appeals cases, the courts have accepted the Commission’s arguments that companies appropriately characterized as employing dark patterns had behaved in an unlawfully deceptive manner (F.T.C. v. AMG Capital Management, 910 F.3d 417 (9th Cir. 2018); F.T.C. v. LeadClick Media, LLC, 838 F.3d 158 (2d. Cir. 2016); Fanning v. F.T.C., 821 F.3d 164 (1st Cir. 2016)). The Commission and courts did not use the dark patterns terminology, and the record lacked the kind of empirical evidence revealed by the Luguri and Strahilevitz study, so the judges relied on sensible intuitions to conclude that the trade practices being challenged were deceitful.

There is, admittedly, less case law surrounding the FTC’s use of section 5 from which to construct a profile of what conduct is “unfair.” In the overwhelming majority of enforcement actions, companies choose to settle with the commission, entering into binding settlement agreements, rather than challenge the commission in court or administrative proceedings. (Solove & Hartzog, 2014). In the absence of judicial decisions, however, these widely-publicized consent decrees provide significant guidance to regulated entities. In 1980, the FTC laid out the test still currently utilized to find an act or practice “unfair” due to unjustified consumer injury under section 5. Per this test, an unfair trade practice is one that 1) causes or is likely to cause substantial injury to consumers, 2) is not reasonably avoidable by consumers themselves, and 3) is not outweighed by countervailing benefits to consumers or competition. This three-part test is now codified in section 5(n) of the FTC Act.

Generally, the “substantial injury” prong is seen as the linchpin of a section 5 unfairness analysis. Overwhelmingly, the substantial harm asserted by the FTC has been monetary; however, unwarranted health and safety risks have also been the backbone of some actions (Hartzog & Solove, 2015). Monetary harm can come from the coercion of consumers into purchasing unwanted goods, or from other incidental injuries that come as a result of the unfair action, such as financial harm from identity theft due to improperly secured data. Notably, a harm’s substantiality can come from its collective effect on consumers, as the FTC notes “an injury may be sufficiently substantial, however, if it does a small harm to a large number of people” (FTC Policy Statement on Unfairness). The harm need not be “certain” under section 5, only likely. Thus actions can be brought before the damage is fully realized, as long as it is more likely than not to occur.

The next prong of the three-part unfairness test is that the injury must not be one which the consumer could have reasonably avoided. This prong is grounded in the belief that the market will be self-correcting and that consumers should, and in general will, avoid those companies that utilize unfair practices. Those practices that “prevent consumers from effectively making their own decisions” run afoul of this prong, even if they merely hinder free market decisions and fall short of depriving a consumer of free choice. In order for consumers to reasonably avoid harm, particularly in the case of a nonobvious danger, they must also be aware
of the possible risk. Thus it is imperative that a company disclose risks to consumers so that they can make informed decisions with knowledge of the relevant potential harms.

The cost-benefit analysis prong of the unfairness test ensures that companies are only punished for behaviors that produce “injurious net effects.” There are, as the Commission notes, inevitable trade-offs in business practices between costs and benefits for purchasers and consumers, and as such certain costs may be permissibly imposed on consumers, provided they are justified and balanced by legitimate benefits. Broader societal burdens are also accounted for in this equation as are the potential costs that a remedy would entail. Additionally, the Commission looks to public policy considerations during this analysis in helping to establish the existence and weight of injuries and benefits that are not easily given a concrete value.

The FTC has previously regulated the use of unfair designs and unfair default settings that are varieties of dark patterns. In FTC v FrostWire, LLC, (FTC Matter No. 112-3041, 2011), the commission brought action against the producers of a file sharing application designed in a manner that caused a significant number of consumers to "unwittingly share files stored on those devices." Relevantly, the FTC pointed to the obstructionist defaults of the program, which made it exceptionally burdensome for a consumer to prevent all of her files from being shared. As described in the complaint, "a consumer with 200 photos on her mobile device who installed the application with the intent of sharing only ten of those photos first had to designate all 200 … as shared, and then affirmatively unshare each of the 190 photos that she wished to keep private.” Similarly, in In re Sony BMG Music Entertainment (FTC Matter No. 062-3019, 2007), content protection software was required to be installed on consumers computers in order for them to listen to purchased music CDs. This software was then almost impossible to remove for the average consumer, and those in the minority who were able to uninstall the software found their CD-ROM drive no longer operable as a result. The FTC, in a similar rationale to FrostWire, found the design of the program unfair.

Additionally, The FTC has a long history of regulating the targeting of vulnerable consumers, whether those vulnerabilities come from inherent cognitive biases or particularized individual or group vulnerabilities (Solove & Hartzog, 2014). The FTC, in its statement on unfairness, distinguishes between legitimate salesmanship and techniques that "prevent consumers from effectively making their own decisions." The Commission properly bans practices that "undermine[…] an essential precondition to a free and informed consumer transaction,” such as the “exercise [of] undue influence over highly susceptible classes of purchasers” like “promoting fraudulent ‘cures’ to seriously ill cancer patients.”

Alternatively, to the extent that dark patterns emerge in the financial services and banking sectors, the Consumer Financial Protection Bureau (CFPB) has the authority to regulate "abusive conduct.” The CFPB abusive conduct definition is arguably more expansive than the “unfair” conduct regulable by the FTC and, as such, is a powerful tool for regulation. An abusive practice, per 12 U.S.C. § 5531, is one that:
(1) materially interferes with the ability of a consumer to understand a term or condition of a consumer financial product or service; or

(2) takes unreasonable advantage of -

   (A) a lack of understanding on the part of the consumer of the material risks, costs, or conditions of the product or service;
   (B) the inability of the consumer to protect the interests of the consumer in selecting or using a consumer financial product or service; or
   (C) the reasonable reliance by the consumer on a covered person to act in the interests of the consumer.

This provision covers the exploitation of the cognitive biases of consumers in order to manipulate or pressure the consumer into making a decision that may not be in their own best interest. Adding such a broad provision to the FTC Act would be ideal for the protection of consumers insofar as the FTC would be able to restrict the use of dark patterns in all the industries subject to the Commission’s jurisdiction.

a. Dark Patterns as Unfair Practices

The manipulative dark patterns we discuss here might seem natural targets for regulation aimed at “unfair” practices. We would support the interpretation of existing unfairness provisions to include them, but we acknowledge that there may be some barriers to doing so. Recall that, as currently interpreted, section 5 of the FTC Act defines an unfair practice as one which, at a minimum, (1) “causes or is likely to cause substantial injury to consumers” that (2) “is not reasonably avoidable by consumers themselves,” and is (3) “not outweighed by countervailing benefits to consumers or to competition.” Arguably, the manipulative dark patterns we describe here should meet all three of these prongs, but there are possible hurdles as to the first two. Previous cases based on the privacy or security of personal data have sometimes stumbled on the “substantial injury” requirement because courts have found increased risk of harm insufficient to constitute “substantial injury.” A case premised on dark patterns might fare better, however, if the alleged injury was stated in terms of consumers being manipulated into entering into transactions that they would otherwise have avoided, rather than in terms of any privacy or security risks associated with those transactions. Where the dark pattern is not technically deceptive, there might also be a question of whether the injury was “reasonably avoidable by consumers themselves,” though we think unfairness should encompass the sorts of manipulative dark patterns we describe here if it is to mean anything beyond deceptiveness. Favorable interpretations of unfairness could be pressed in litigation. Alternatively, or in addition, Congress could empower the FTC to engage in rulemaking on these issues—a change that would be desirable for other reasons as well.
In our view, a quantitative approach to identifying dark patterns could be workable and offers many of the benefits of bright-line rules in general. More precisely, where the kind of A/B testing that we discuss above reveals that a particular interface design or option set more than doubles the percentage of users who wind up “consenting” to engage in a consumer transaction, the company practice at issue could be deemed presumptively an unfair or deceptive practice in trade. In the scenarios developed by Luguri and Strahilevitz, both the mild dark patterns and the hard dark patterns made it more likely than not that consumers were electing not to decline a service on the basis of the choice architecture employed rather than on the basis of innate demand for the service at issue. The “more likely than not” standard is widely employed in civil litigation over torts and other kinds of liability, and it could work well in this context too, ideally with the FTC and academics working hand in hand to replicate high-quality research that quantifies the effects of particular manipulations. As a statistical matter, each individual research subject in the study who was signed up for the data protection plan was more likely than not to have done so because of the dark pattern rather than because of underlying demand for the service being offered.

What’s more, it may be appropriate for courts to deem instances in which the “more likely than not” test is satisfied as instances in which consumers have not actually consented to the contractual terms at issue. To hold otherwise runs the risk of treating consent as a legal fiction, rather than an indication of mutual assent. Numerous legal settings require individuals to consent to have their information processed or shared, or to incur a legal obligation to pay for a good or service. Where this consent is procured through a manipulative exchange between the consumer and the digital platform it should be treated by courts as a legal nullity (Hartzog, 2018).

In embracing a “more likely than not” rule, we do not mean to rule out the development of multifactor standards that can complement a rule-based approach. For example, the “more likely than not” test works very well when the innate preference for a product among consumers stands at 10 or 20%. But when 40 to 50% of consumers would want to sign up for a service or purchase a product, the “more likely than not” test is likely to let too much manipulative conduct survive. In our view, a situation where 40% of consumers opt to buy a service because of innate demand for it and 20% of consumers opt to buy because of a manipulative interface or choice architecture may still be legally problematic. We consider how the law should address those kinds of situations below, in the section labeled “Questions of Intent and Proof.”

In considering the interpretation of fairness requirements, it may also be useful to consider the EU’s approach to “fair processing” under the GDPR. The UK’s Information Commissioner’s Office has issued guidance to data processors stating they should be able to affirm that:

- We have considered how the processing may affect the individuals concerned and can justify any adverse impact.
We only handle people’s data in ways they would reasonably expect, or we can explain why any unexpected processing is justified.

- We do not deceive or mislead people when we collect their personal data.

This approach would seem to capture the manipulative dark patterns we have in mind.

b. Questions of Intent and Proof

However implemented, the framework we propose here lends itself well to a two-step approach for purported dark patterns that do not satisfy the “more likely than not” bright line rule proposed above, beginning with a prima facie allegation that a manipulative dark pattern based on either transaction costs or vulnerability has been deployed. The prima facie barrier for discovery or investigation should not be too high because such patterns will often be the result of intentional design choices or, at a minimum, of willful blindness to design implications that will be readily apparent from internal documentation and behavior. We do not support a standard that requires intent or willful blindness for liability, however. Though such a standard might capture many of the most problematic dark patterns, particularly of the transaction cost strand, increasing use of artificial intelligence approaches to targeting suggests that system designers should have a duty to avoid implementing manipulative dark patterns that rise to the level that would be actionable under our framework.

To be more explicit about how enforcement might proceed, a consumer protection agency might identify illegal dark patterns on the basis of a two-step process. First, the agency would identify evidence that a particular design appears to impose unnecessary transaction costs or to exploit vulnerabilities associated with particular individual or group characteristics. Once this prima facie threshold is met, the consumer protection agency would further investigate the procedure underlying the design choices for this interface, thus potentially uncovering further evidence that the manipulation is intentional or willfully blind or, alternatively, that there is a non-manipulative justification for the design. For example, when a company is rolling out a new product or service to its existing customers, it may need to disclose a healthy quantum of information to describe the new opportunity, and that process of persuasion will entail transaction costs for consumers. To the extent that the company is offering arguments designed to appeal to consumers’ System 2 decision-making processes, it should not get into any trouble with regulators. It is only when the choice architecture employs cognitive tricks that are designed to exploit quirks of human System 1 decision-making that the line separating unlawful dark patterns from constitutionally protected persuasive commercial speech is crossed. Admittedly, there may be some close cases involving judgment calls about the precise line between permissible and impermissible, and evidence of intent will be illuminating where it is available. Regulators charged with policing dark patterns should focus on the blatant cases at the outset, while the development of “common law” principles along the way will permit the eventual differentiation of disputes closer to the margin.
Suppose that elderly consumers have been complaining that a user interface manipulated them into purchasing something that they did not want or into unintentionally giving over personal information. An investigation might uncover evidence that the designers engaged in A/B testing aimed at elderly people or were willfully blind to data showing the design’s disproportionate effects on the elderly. Information about design processes may often be sufficient to confirm the identification of a manipulative dark pattern. Sometimes, however, the results may have emerged from an AI targeting algorithm and will have to be demonstrated by other sorts of evidence, perhaps including statistical testing.

C. Institutional Implementation Considerations for Default Rules and Dark Pattern Regulations

Once the content of default rules and the non-manipulative way in which they should be offered to consumers are determined, there is the regulatory question of how such rules should be implemented. There are several models for doing so, and the optimal implementation choice should consider the issues regarding the problems of fine print and consumer contracts, where it is the sellers that write and present the contracts in the first place and consumers may remain uninformed about some or all of the terms in the contracts.

Unlike the case of dark patterns, where there is already a regulatory structure capable of incorporating enforcement actions against such practices, there are currently no all-encompassing default rules in the information privacy space. One approach towards implementation of default rules is through a principles project with the American Law Institute, or, less likely in this context, a restatement project, if there is enough case law to “restate” and steer the rules in a normatively appealing direction. In practical terms, principles project ideas are generated by the director and the projects committee, who also take suggestions from members. The director then develops a project proposal and potential reporters, which is then considered by the project committee for advice and recommendation to the council. While restatements are directed to judges, the principles projects are addressed to legislatures and administrative agencies, or also to judges when the law in that particular area is scant. The benefit of a principles project is that the consumertarian-rule creating process could result from robust exchanges among experts in industry, judges, consumer advocates, and practicing lawyers, all of whom would give thoughtful advice to the reporters, thus ensuring all interests are well represented in the final product. The drawbacks of such approach are that it might take considerable time to obtain approval by the ALI members, the final product might not be optimal but rather reflect compromises made to ensure a final vote, and legislatures might ignore it. At the end of the day the ALI process may not be nimble enough to respond to rapid changes in technology and corporate practices unless the end product is written in a way that is open-ended enough to empower those charged with enforcing the law but also still clear enough to provide fair notice to regulated entities. Given industry participants’ need to comply with the laws of
multiple jurisdictions, an effective default rule regime would have to be adopted wholesale by all states or at the federal level to ensure uniformity.

Other projects take the form of codes, which are drafted with an eye toward legislative enactment. An example of this is the Uniform Commercial Code, which does not have legal effect until and unless adopted by state legislatures, which can, of course, modify the proposed code as they see fit. Codes might take longer to get buy in from the relevant bodies and might suffer some of the same concerns raised with principles or restatements. Alternatively, private bodies can create model rules that can also later be adopted by legislatures. For example, The Principles of European Contract Law (PECL) is a set of model rules, created by the Commission on European Contract Law, led by Professor Ole Lando (the Lando Commission). Like the restatement, the PECL is “soft law,” and, without some legislative or judicial action, not legally enforceable.

Finally, Congress could grant the FTC or a newly established federal agency some rule-making authority and charge the agency with the task of creating default rules and limits on dark patterns, or at least involve the agency in the process of creating such rules.

One dynamic should be relatively clear from our analysis above, which is that waiting for market forces to solve the problems we have identified is unlikely to lead to satisfying results. Even if markets for online services were perfectly competitive, many of the impediments to market privacy and security solutions we identified in section I.A. would remain. Namely, when privacy breaches occur it is often hard to tie subsequent harms to any particular breach, since the same personal information may be replicated in many different proprietary databases. These dynamics give rise to substantial negative externalities. (See Ben-Shahar, 2018). Companies that wanted to differentiate themselves on the basis of investments in privacy and security or the development of enlightened policies would face challenges in communicating their choices to unsophisticated consumers, given the complex and technical subject matter at issue and the danger that consumer-facing advertising will spook consumers about entire product lines. For example, consumers presently have no understanding of various ways in which dark patterns are being used to manipulate their choices, and the subtlety of successful strategies would make it costly for a firm that eschewed the dark patterns strategy to run a campaign condemning their competitors in an effort to gain market share. In that sense, we can contrast dark patterns with a more blatant and easier to understand strategy like extra fees for checked luggage, a pricing strategy Southwest Airlines has criticized in its “Bags Fly Free” ad campaign. Digital platforms also have incentives not to publicize many of their investments in data security in detail because describing those investments to consumers (or shareholders) necessarily alerts hackers to the same information, which in some cases could create new vulnerabilities. Finally, perfect competition is unlikely to internalize the externalities associated with one consumer’s decision to expose personal information about friends and family. We do not mean to suggest that it is impossible for consumer-facing firms to differentiate themselves on the basis of privacy and
security precautions. Some have done so successfully. But those efforts represent an incomplete strategy for addressing the thorny range of problems highlighted herein.

**D. Mitigation for Security Threats Caused by Data Breaches**

To mitigate attacks that leverage passwords stolen in a data breach to compromise accounts on other services, minimizing the role of passwords in authentication would seem an obvious solution. Unfortunately, efforts to eliminate passwords entirely are unlikely to fully succeed in the near term. One reason for widespread password reuse is that users are asked to make dozens, or even hundreds, of different accounts, falling back on password reuse as a coping mechanism. The idea of federated identity or single-sign-on systems, which entail using a single identity provider (e.g., Google) to authenticate many different services, would obviate having so many different accounts. However, adoption of such systems has been limited for a number of reasons, including users’ concerns about sharing data with companies like Google and Facebook that offer to serve as identity providers, as well as concerns about creating a single point of failure. While password manager software installed on a user’s device does not raise the same privacy concerns, password managers are again a single point of failure and also enable new kinds of attacks. Furthermore, current password managers do not fully prevent users from continuing poor practices like password reuse due to design decisions their creators have made (Ur et al., 2015).

Techniques like multi-factor authentication often layer a password with a second line of defense (e.g., possession of a smartphone configured in a particular way). While doing so substantially lessens accounts’ vulnerability following a data breach, it again does not eliminate passwords. Recent efforts by the World Wide Web Consortium to standardize the WebAuthn specification for authentication using public-key cryptography (often enabled by USB tokens from manufacturers like Yubico) have been heralded as a new way to eliminate passwords. However, the inconvenience of users needing to carry additional hardware for authentication (at least in the near term) prevents WebAuthn from being a silver-bullet solution. As a result, passwords are unlikely to disappear completely anytime soon. Furthermore, rearchitecting authentication systems would, at best, only solve problems related to reused passwords stolen in a data breach, not to any other types of information stolen.

Accepting the persistence of the password in the authentication ecosystem, another approach to mitigating the security threats of data breaches would be to involve the affected users more directly, notifying them in greater detail about what information has been breached and how it could be used. Currently, data-breach notifications provide limited, often vague, information to consumers. As such, it is not surprising that consumers are often not sure how to respond when either their account credentials or their personal information is reported stolen. (Ablon et al., 2016; Golla et al., 2018). As a result, even after major, widely publicized breaches like those of Equifax or LinkedIn, many consumers have not taken action in response. In contrast, automated systems could potentially have taken some action on their behalf.
Fully empowering the user to act would likely require a radical redesign of the data-breach notifications companies send to consumers. These notifications would need to be more detailed and actionable. Laws might also need to be amended. Current legal requirements for data-breach notifications vary by jurisdiction, yet no jurisdictions require notifications that are as detailed as might be needed. Further complicating these efforts is the necessity to authenticate the recipients of such detailed notifications; sending detailed information about information that was stolen to an unauthenticated recipient is, in a way, its own data breach. However, this approach increases, rather than decreases, the burden on users. The redesign of data breach notifications could conceivably provide greater agency and transparency to users, yet it would be unlikely to change this desolate scenario of widespread inaction. Increased transparency would only make an imperfect system even more burdensome. As mentioned above, users could easily resort to password managers to mitigate many of the risks discussed herein. That they do not do so demonstrates the need to develop alternative solutions that shift the focus from the user to other parties.

An interesting alternative may be to encourage companies to share the data stolen in a data breach directly with other companies, including their competitors. That is, following a data breach, companies would send the precise information identified as stolen to any other companies that request that information. Given that some larger companies already buy this breached information from hackers themselves, in some sense such a system would simply remove hackers as the middlemen. Two key challenges stand in the way of a system like this becoming practical. First, it is ethically questionable for a company that has experienced a data breach to further disseminate their users’ personal information and credentials to any other company that asks. On one hand, disseminating this information that had been given specifically to only one company can violate users’ privacy. That a further violation of privacy may be necessary follows from the breached company’s negligence in protecting the data in the first place. On the other hand, given that other companies might be purchasing this information from hackers anyway to protect their own users, it might cause further harm if this information is not disseminated for defensive purposes. Complicating this calculus, though, are questions about how a company might want to handle the dissemination of data that has been breached by hackers but has not yet been released publicly.

The idea of competing companies working together to stave off computer security threats has some conceptual similarities to controversial efforts for sharing threat intelligence as part of the Cybersecurity Information Sharing Act of 2015 (CISA). This law established processes and legal safeguards for private companies to share information on computer security threats (e.g., details of attempted attacks) with the US federal government or with other private companies. The legal safeguards provided by CISA minimize potential liabilities related to the disclosure of privileged information, and they also protect shared information from FOIA requests under certain circumstances. While CISA has been presented as facilitating voluntary sharing of cybersecurity threats, rather than mandating such sharing, some of the act’s many critics have questioned whether
sharing truly is voluntary (Stepanovich, 2015). Other critics of the act have pointed out that CISA potentially broadens federal surveillance under the guise of warding off hackers (Krebs, 2015). In the end, only a few companies have chosen to share data with CISA thus far. These past experiences with CISA raise important questions about how to structure any future processes for companies to share information stolen in data breaches with other entities.

Given concerns users might have with their data being shared with particular other companies or with government agencies, as well as how such a sharing infrastructure could create perverse incentives in favor of data breaches, the architecture of such an inter-entity sharing agreement, and the role of the government in such an agreement, requires care and thought. One possible direction to mitigate these tensions could be a process for consumers to opt in to having their data shared with other companies when notified of a data breach. In contrast, though, one could consider establishing a consumertarian default rule. Outlining a default rule that establishes terms that most individuals in a data breach would agree to, yet could be overridden upon the request of each impacted user, would likely require empirical grounding. That is, empirical research would be needed to document what specific types of information (e.g., usernames, credentials, contact information, social contacts) users would want other unrelated companies to be told were stolen in a given data breach. Consumers would likely view such transfers as akin to data sharing or data selling, practices that they often view negatively, even though in this case the transferred data could perhaps be constrained legally to allow only for threat mitigation. Empirical research would also need to answer questions about consumers’ perception of which companies or entities should receive this data. Consumers' opinions might dictate that each consumer should establish a personalized whitelist of companies to which information could be shared. The empirical work might instead suggest that a more global, non-personalized whitelist is appropriate, dictating that only a particular list of trusted companies or entities should be permitted to receive data.

Beyond a consumertarian default rule, one can envision two other possible solutions to increase coordination and data sharing amongst companies for the purposes of increased data security. This system must be designed in a way that promotes the sharing of this sensitive and critical information while at the same time protecting user privacy, providing proper incentives for companies to participate (in contrast to CISA) and complying with laws and regulations on data sharing amongst companies (both data protection and antitrust laws).

The first possibility one could consider is to further strengthen a CISA-like system by making participation in a government-controlled database mandatory, alleviating some of the free-riding problems that currently impair CISA (companies receive reports even if they do not participate). Such imposition, however, would probably face even more opposition than the initial, voluntary CISA-style system did. Indeed, as seen above, CISA was perceived as a violation of user privacy and as an expansion of what is already an intrusive federal surveillance apparatus. These are some of the reasons why the CISA legislation stalled in Congress for many years and why
current voluntary participation is low. As a result, such an expansion is unlikely. It is also probably undesirable.

A second, preferred, alternative may be to use technological tools to design a “data-breach clearinghouse,” where companies may share information about breaches and passwords in a secure and privacy-preserving manner. Companies could query the clearinghouse to determine whether a given user on their service had used the same, or a similar, password on another service. Enabling companies to insert data stolen from them into the clearinghouse removes hackers as the middleman who stand to profit from selling this data to other companies, and it also facilitates coordination among competing companies for the overall benefit of the authentication ecosystem. It can also minimize the additional financial incentives for hackers. Before they make stolen data public, they attempt to sell the data to others who weaponize it to compromise other accounts. Enabling other companies to defend against these attacks could substantially lessen the value of this non-public data.

Two methods can provide incentives for companies to participate. First, data-breach laws could be amended to mandate a company’s participation in the clearinghouse shortly after it learns of a data breach. Second, data-breach laws or courts could establish that not querying their own users’ records in the clearinghouse is prima-facie evidence against data-security protocols, potentially increasing liability in the event of a data breach. Finally, by being privately run and having a sole objective of enhancing data security, the clearinghouse would not be the equivalent to CISA in enabling further surveillance by the government (assuming they are protected from government backdoors).

A couple of security and privacy design considerations are crucial for such a clearinghouse to be feasible. First, the clearinghouse must not become a new single point of failure for the authentication ecosystem in the event that it is compromised. Second, the clearinghouse must minimize the potential for brute-force querying to leak private information. However, current cryptographic techniques can enable more privacy-preserving approaches to data sharing and can partially mitigate concerns about how such data sharing impacts privacy. Broadly, the sub-field of cryptography studying secure multi-party computation focuses on techniques that can meet these assumptions. More specifically, recent work has engineered new techniques for decentralized private set-membership testing. These techniques enable one website to query other websites about whether a user's password is the same across sites (Wang & Reiter, 2018). The key innovation is that this work uses advanced mathematics to perform this testing without negatively affecting the privacy of a user's password, subject to certain assumptions. While these techniques are not yet at a point of engineering maturity sufficient for a data-breach clearinghouse like the one we imagine, they are an important step toward such a design.

For a number of reasons, such a clearinghouse is strongly preferable to companies directly sharing plaintext information with each other, or buying that information from hackers. For example, directly sharing plaintext data would have major ramifications for user privacy. In
addition, depending on how the structure is designed, the direct sharing of information among competitors may run afoul of antitrust laws—in particular if this information is essential and if the trust requirement restricts the system to only a handful of already established companies. This scenario could be a variation of the Supreme Court’s *Associated Press v. United States* decision (326 U.S. 1 (1945)).

Recent pushes to bring more centralized notifications of data breaches to consumers are related to a potential data-breach clearinghouse, yet operate on slightly different assumptions and fulfill different use cases. The website *Have I Been Pwned* focuses on notifying users when data associated with a particular email address or user name is part of a data breach. However, because it does not attempt to communicate the data itself (i.e., the exact password that has been stolen), it does not solve the same problem as a potential data-breach clearinghouse. Mozilla’s recently released Firefox Monitor for the Firefox browser brings the *Have I Been Pwned* functionality to a wider user base. Google’s recently released Password Checkup extension has similar goals and uses some related technologies. The Password Checkup extension aims to tell a user if the credentials they are trying to create for an account match those that Google knows to be compromised from prior data breaches (e.g., those Google’s security team has collected from hacker forums) without revealing the user’s password to Google. It does so, in part, by sending an encrypted version of a short prefix of the username and password of interest to Google, sending back to the user all entries in the database matching that prefix. While such a system is ideal for when the credentials have already been leaked publicly, this approach does not solve the problem of permitting the data-breach clearinghouse to handle credentials that have potentially been stolen by hackers but not yet released publicly. These credentials have much higher security requirements lest the data-breach clearinghouse inadvertently increase harm by leaking information about them.

**E. Privacy-Preserving Measurement and Coordination**

There are several components of the Committee’s different reports that call for greater measurement of technology sector business practices or coordination between firms. The Market Structure and Antitrust Subcommittee, for instance, recommends routine collection of market transaction data to understand the competition dynamics of major technology platforms. The reports on the News Media Industry and on Political systems also call for data collection and disclosure. This Subcommittee’s own report envisions a system for sharing stolen user credentials in the event of a data breach.

In considering the virtues of greater information transparency, it is vital to acknowledge that market measurement and sectoral coordination can involve confidential personal data. Public-sector agencies and private-sector businesses participating in these information sharing programs should adhere to principles of data minimization, avoiding bulk data dumps in favor of more targeted disclosures. Participants should also implement appropriate security safeguards, including technical precautions such as encryption and access controls, as well as security.
policies such as employee training. Promoting competition, protecting consumers and even understanding the impacts of platforms on political systems should not come at the expense of significant additional privacy impositions.

We also note that there is a range of privacy-preserving computational techniques that may implement the Committee’s measurement and coordination recommendations while mitigating privacy consequences. One promising direction is differential privacy, a family of techniques that enables performing computation on a dataset without revealing an individual’s personal information. Unlike prior approaches to privacy-preserving dataset analysis (e.g., k-anonymity), which are appealing in theory but prone to vulnerabilities in practice, differential privacy is designed to provide strong probabilistic guarantees. The technology sector is increasingly implementing differential privacy for user analytics, and software libraries for differential privacy are quickly reducing the costs of and barriers to further adoption.

It would be (relatively) straightforward, for example, to apply differential privacy to market surveillance. A regulator could issue queries to regulated firms to understand long-term trends in technology sector competition, and meanwhile, the firms could have confidence that they were not disclosing the details of specific transactions or business partners.

Another promising direction is secure multiparty computation, which enables multiple entities to collaborate on data analysis while limiting the data that each entity discloses. Secure multiparty computation could, for example, enable regulators to conduct market surveillance using data held across multiple firms while minimizing information flows to regulators and preventing competitors from learning each other’s sensitive business details. In the context of data breach information sharing, as noted above, secure multiparty computation could enable firms to compare user credentials without ever disclosing the credentials themselves.

The Subcommittee is not recommending any specific technology for privacy-preserving computation, but we encourage bearing these opportunities in mind for the subcommittees’ recommendations and future recommendations on technology competition, the media landscape, politics, and privacy.
Conclusion

The law and the marketplace, as they presently exist, simply expect too much of consumers. They expect each consumer to read terms of service and privacy policies and to opt out of problematic practices. Such an expectation might be realistic if there were one entity that handled consumers’ data, but it becomes absurdly impractical when scores of such entities interact with the typical consumer. The law expects consumers to be vigilant against dark patterns, and it often treats sneaky and manipulative tactics that are designed to confuse or badger consumers into accepting privacy intrusions as tantamount to authentic consent. Consumers are also expected to keep track of dozens of different passwords and other authentication tools, and to do so in a way that will not itself expose those passwords to the possibility of breach. It is little wonder, then, that password reuse and the use of inadequate passwords have become widespread problems. In short, in many privacy and security domains, consumers who face time constraints, cognitive constraints, or situations that seem low-stakes at first glance, and who then act rationally in response, are left unprotected by legal doctrines. We can and ought to do better.

In our report, we have endeavored to identify three key areas where fundamental problems of privacy and security emerge, and where the existing legal and regulatory toolkit has failed consumers. As a result, consumers are stuck with product features that they do not understand or do not want. They are manipulated into making choices that conflict with their preferences and values. And their data is being exposed to unnecessary threats of leakage and misuse resulting from the failures of platforms to coordinate in ways that would serve the collective interests of both customers and shareholders. Our effort here has been to summarize the state-of-the-art academic research where it exists and to supplement it in important instances where we have found the literature wanting. Having consulted the research, new and old, we have proposed three ambitious ideas to enhance the privacy and security of Americans’ interactions with the digital platforms that have become important, ubiquitous, and unfortunately sometimes frustrating parts of life in the modern world.

The Privacy and Data Protection Subcommittee has not raised all the important issues concerning privacy and data security that relate to digital platforms. There are other efforts underway—in legislatures, within firms and industry groups, in academia, and within bodies like the ALI—that aim to be more comprehensive than this one and that stand to accomplish much good if their ideas are implemented. We hope those efforts succeed because the privacy and security problems confronting the users of digital platforms are substantial and urgent.
References


Bakos, Yannis et al., Does Anyone Read the Fine Print? Consumer Attention to Standard Form Contracts, 43 J. Legal Studies 1 (2014).


Bösch, Christoph et al., Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns, Proceedings on Privacy Enhancing Technologies (2016).

Calo, Ryan, Against Notice Skepticism in Privacy (and Elsewhere), 87 Notre Dame L. Rev. 1027 (2012).


Golla, Maximilian et al., “What was that site doing with my Facebook password?” Designing Password-Reuse Notifications. In Proc. CCS, 2018.


Hartzog, Woodrow, Privacy’s Blueprint (Harvard Univ. Press 2018).


