Breaking the Privacy Gridlock: A Broader Look at Remedies

James X. Dempsey
Chris Jay Hoofnagle
Ira S. Rubinstein
Katherine J. Strandburg

April 2021

Berkeley Center for Law & Technology

NEW YORK UNIVERSITY
INFORMATION LAW INSTITUTE

Contents

Executive Summary

Divisions over two enforcement issues—private right of action and federal preemption—have long gridlocked the effort to enact federal consumer privacy legislation. A look at regulatory systems outside the privacy field, however, reveals a complex landscape of enforcement mechanisms and remedies, many of which have not yet received much attention in the privacy debate. Insights from financial services regulation, environmental law, labor law, and other fields may offer ideas for assembling an effective web of enforcement for a federal privacy law.[1]

In the U.S., the dominant model of regulation is based on supervision or monitoring. Under this model, government overseers have routine access to information about the activities of regulated entities, and those monitors can take a variety of actions short of complaint and investigation that change practices of a business. Most large federal regulators have authority for some combination of both supervision and investigations but, for many large agencies, monitoring is the primary form of enforcement. The Federal Trade Commission is an outlier in this regard because it was designed to rely primarily on investigations led by lawyers. Over time, the FTC has developed more supervision-like activities, although their use generally comes only after investigation and complaint, and there are concerns that the third-party assessments the FTC relies on are not very rigorous.

Most monitoring agencies have at their disposal a graduated continuum of enforcement options, and at many agencies, the options most frequently exercised are those outside the court system.

The supervision model may be well-matched with two relatively recent changes in the overall approach to government regulation: the emphasis on public-private collaboration or cooperation and the rise of compliance departments inside corporations.

Information disclosure can also be an effective part of a policy enforcement system. Sometimes, a policy of information disclosure can lead private actors to voluntarily solve a problem in some market-based way. Information disclosure can also support enforcement goals by providing warnings or through admissions of wrongdoing.

[1]Microsoft provides an annual gift to the Berkeley Center for Law & Technology (BCLT), which supports in part the general programming of the center and the salaries of its staff, including Jim Dempsey. Part of Microsoft's 2020-21 gift to BCLT was designated for work on privacy remedies. None of the Microsoft funding supported the salary of, or otherwise directly benefited, BCLT faculty co-director Chris Hoofnagle and none of the BCLT Microsoft funding was redistributed to or otherwise benefitted Ira Rubinstein or Katherine Strandburg. Microsoft had no prior approval over the content of this paper. This report uses François Rozet's Sleek Style LaTeX Template, available at https://github.com/francois-rozet

Environmental law has adopted innovative ways of dealing with small, collective and intangible harms. As a baseline, there are statutory requirements, such as emission limits, that the government enforces with administrative orders and penalties and with civil actions for injunctive relief and monetary penalties. The adoption of specific standards enforced by the government rather than individual plaintiffs overcomes the causality and harm problems that limited traditional tort remedies, because the government does not have to show harm, just that the prescribed limits were violated. Environmental law also includes market-based regulation through, for example, emission fees. The environmental field also relies heavily on self-regulation overseen by regulators.

Another interesting approach in environmental statutes is the concept of natural resource damages. This allows for the measurement of collective and intangible harms, sometimes using contingent valuation methodology.

The citizen suit is a powerful enforcement innovation in environmental law and it is found in almost every federal environmental protection law. These provisions authorize any affected individual to (1) sue any person (including any government agency) alleged to be in violation of a standard or (2) sue the Environmental Protection Agency itself for failure to perform any duty which is not discretionary. Typically, in these proceedings, attorneys fees can be awarded to successful plaintiffs. Under the Clean Water Act, for example, any penalties assessed must be deposited into the U.S. Treasury.

Many regulatory systems rely on private sector enforcers, such as certification bodies, self-regulatory organizations, accountants, lawyers, and other "gatekeepers." In recent years, the use of gatekeepers in the financial services sector has expanded and, moreover, has changed in that the large financial institutions have themselves been enlisted as gatekeepers, regulating the conduct of their third-party service providers. Gatekeeper regimes have become quite explicit and extensive in other key sectors, including information technology, oil, and pharmaceuticals, where regulators in each of these industries have put leading firms on notice about their responsibilities for third-party oversight. As Prof. Rory Van Loo has written, "policymakers have begun relying on third-party enforcement by the real gatekeepers of the economy: the firms who control access to core product markets."

The consumer class action has been hotly debated for decades, with studies on both sides. We cite recent evidence that class actions do generate both specific changes in business practices and general deterrence of wrongdoing. Recent studies have also found value in approaches that ensure monetary relief is actually paid to individual consumers. Some recent privacy and data security class actions have resulted in settlements imposing only injunctive relief (plus attorneys' fees).

Remedies should be tied to policy goals: Before developing a system of remedies, policymakers should define their goals and then any assessment of remedies should consider whether they advance a desired policy goal. Considering remedies through a deterrence theory framework makes it easy to see just how complex and interdependent the remedies necessary to promote even a single policy goal may be. Different policy goals may require different remedies. The experience under the Telephone Consumer Protection Act (TCPA) illustrates the role of intermediaries or other third parties who may be positioned to require regulated entities to respect the asserted policy norms.

1 | Introduction

For years, efforts to enact comprehensive federal privacy legislation have been stymied by all-or-nothing attitudes toward the paired issues of individual enforcement (private right of action) and federal preemption (whether federal law should set a ceiling on state law). As Cam Kerry and John Morris note in one of the leading efforts to advance resolution of the privacy conundrum, the two issues can be "article[s] of faith on both sides" of the debate. To break the gridlock, Kerry and Morris offer a set of proposals intended to finely calibrate a system of private enforcement and preemption.[1]

Fine-tuning private right of action and preemption may indeed be the path forward. But a look at regulatory structures *outside* the field of information privacy shows just how narrow the scope of the privacy debate is. In other regulated fields, from environmental law to financial services, public policy is enforced by mechanisms that go far beyond formal administrative complaints and private lawsuits for damages. These other enforcement options include licensing, permitting and other forms of approval, agency monitoring (as opposed to investigation), citizen suits seeking injunctive relief, information disclosures, creative means of estimating damages, and use of third-party intermediaries or gatekeepers to enforce policy.

In November 2020, we convened two workshops bringing together scholars from fields other than privacy to describe the enforcement and remedies structures in those other fields. In this paper, we offer some insights drawn from those workshops and further research, in the hope that they will generate creative thinking and expand the scope of the remedies and enforcement discussion in the privacy arena.[2]

[1] Cameron F. Kerry, John B. Morris, Jr., Caitlin Chin, and Nicol Turner Lee, *Bridging the gaps: A path forward to federal privacy legislation* (June 3, 2020), https://www.brookings.edu/research/bridging-the-gaps-a-path-forward-to-federal-privacy-legislation/.

[2] For more on privacy remedies, see Lauren Scholz, "*Privacy Remedies*," 94 Indiana L.J. ((2019).

2 | The Supervision Model of Enforcement: Insights from Financial Services Regulation

In the U.S., there are two distinct models of regulatory enforcement: supervision (or monitoring) and investigation. Under the supervisory model, (1) government overseers have routine access to information about the activities of the regulated entities, often obtained on site, where monitors observe what is happening on a continuous, often daily, basis, and (2) those monitors can take a variety of actions short of complaint and investigation that nevertheless result in changes in the practices of the regulated entity. Personnel-wise, the distinction is usually between inspectors and lawyers. Supervision or monitoring (we use the terms interchangeably here) is carried out by inspectors or examiners who often have financial, scientific, or other technical expertise. The EPA, for example, has inspectors who are typically engineers. Investigations, on the other hand, are carried out primarily by lawyers.[1]

One of the key features of supervision is continuous, routine access to information from inside regulated entities. Investigation, in contrast, relies on complaints from the outside or suspicions of wrongdoing, with document demands made after a complaint is received or suspicions are raised. Another characteristic of the monitoring or supervisory approach is the reliance on informal pressures to change corporate behavior.

Supervision or monitoring authority is central to the regulatory structure of many agencies, including the Consumer Finance Protection Bureau (CFPB) and other financial services regulators. (Indeed, as described below in the section on the history of monitoring authority, monitoring is the dominant enforcement model among large regulatory agencies.) Most large regulators have authority for some combination of both supervision and investigations but for many large agencies monitoring is the primary form of enforcement.[2] Certainly for most large agencies, including most regulators of financial services, supervision is the regulatory structure's most powerful enforcement mechanism.

The FTC is an outlier in this regard because it was designed to rely primarily on investigations led by lawyers.[3] Over time, the FTC has developed more supervision-like activities

[1]This section is based on a workshop presentation by Professor Rory Van Loo, Boston University School of Law.

[2]Monitoring can also follow investigation. A good example is the Department of Justice's monitoring, over an extended period of years, of compliance with final judgments in antitrust cases.

[3]The FTC Act does provide more monitoring authority than the agency exercises. See Rory Van Loo, *The Missing Regulatory State: Monitoring Businesses in an Age of Surveillance*, 72 Vand. L. Rev. 1563, 1617-1618 (2019). Section 6(a) of the Act gives the FTC the power "[t]o gather and compile information concerning, and to investigate from time to time the organization, business, conduct, practices, and management of any person, partnership, or corporation engaged in or whose business affects commerce." In 1978, the U.S. Court of Appeals for the D.C. Circuit noted that the FTC's statute "provides a clear

in connection with its investigations. Currently some of the largest technology companies are under continuing review by the FTC. In the privacy and cybersecurity field, FTC consent decrees often contain provisions requiring companies to undergo regular assessments by a third-party assessor. The goal is to ensure compliance with the consent decree generally and to allow the third party to assess the progress of the security or privacy program. But these assessments are required only in consent decrees negotiated after a case has been pursued through the complaint, investigation, and litigation process. Moreover, there are concerns that these assessments are not very rigorous and typically rely on standards *set by the company* being monitored, unlike an *audit*, which is an inspection based on *a well-defined and commonly accepted standard* of performance. The FTC has made far too little use of this component of its consent decrees.[4]

Within the supervisory model, there are two approaches to the authority of monitors and the imposition of remedies. In one approach, monitors have authority only for information collection and report-writing, in which case enforcement would be handed over to others (lawyers typically). Under the other approach, monitors by themselves have independent enforcement capabilities. In a wide range of agencies, including the CFPB, the SEC and FERC, both approaches co-exist: monitors themselves have autonomous enforcement powers with which they can order corrective action and secure millions of dollars of refunds for consumers and investors, while separately those agencies also have enforcement lawyers who can impose monetary penalties or other remedies through more formal legal processes.

Other agencies are monitor-dominated agencies. The Federal Reserve, for example, has relatively few lawyers, and the monitors, called examiners, have the authority to impose fines on banks, totaling $2 billion annually in recent years. OSHA is another example of a monitor-dominated agency.

A very short history of regulatory monitoring

The monitoring model is not new.[5] It dates back at least to the 1864 creation of the Office of the Comptroller of the Currency (OCC), whose mission included certifying compliance with federal banking laws intended to ensure that banks did not fail and thereby spark bank runs that could collapse the economy. "In pursuing these goals, the OCC's main tool was monitoring. It could not litigate. Although the agency could write rules, it rarely used that authority." Monitoring of the financial services sector expanded substantially over the years with the addition of the Federal Reserve (1913), the FDIC (1933), and, for securities exchanges, broker-dealers and others, the SEC (1933 and 1934). The monitoring model also dominated the regulatory structures created for aviation (FAA),

basis of authority for the Commission to issue orders requiring corporations to submit informational reports to the FTC." *Appeal of FTC Line of Bus. Report Litig.,* 595 F.2d 685, 690 (D.C. Cir. 1978) (per curium). And in *Morton Salt*, the Supreme Court concluded that the FTC Act provides "ample power" to require reports, as well as to send investigators to examine a company's books. *United States v. Morton Salt Co.,* 338 U.S. 632, 649 (1950).

[4]For discussion, *see* Megan Gray, *Understanding and Improving Privacy "Audits" under FTC Orders*, (April 2018); Joseph Jerome, *Can FTC consent orders effectively police privacy?* IAPP Privacy Perspectives (Nov. 27, 2018), https://iapp.org/news/a/can-ftc-consent-orders-police-privacy/.

[5]This section and the next two summarize Rory Van Loo's article, *Regulatory Monitors: Policing Firms in the Compliance Era*, 119 Columbia L. Rev. 369 (2019). Unless otherwise noted, all quotes are from that article, with footnotes omitted.

energy (the FPC, established in 1920 to oversee hydroelectric power plants, now FERC), and telecommunications (FCC). As these financial, transportation, telecommunications, and energy industries have evolved, monitoring statutes have mostly kept pace. The FAA today has monitoring authority over unmanned aerial vehicles, and, in the financial services industry, Congress updated monitoring to reach new financial organizations (such as hedge funds), new products (such as credit cards), and the shadow banking system that by some measures is larger than the traditional banking system (CFPB).

Meanwhile, the monitoring model of regulatory enforcement was extended to many other sectors. "[I]n 1902, Congress authorized federal agents to 'enter and inspect any establishment for the propagation and preparation of any virus, serum, toxin, [or] antitoxin.' Related visitorial statutes soon followed for meat and therapeutic drugs." Initially, these powers "were more limited than those of banking and transportation regulators, since inspectors could not examine documents." In the 1960s, FDA officials were authorized to withhold drug approval and "inspect records, files, papers, processes, controls and facilities" of pharmaceutical companies even without evidence that the drug would be unsafe. "In 2011, after deaths and illnesses from tainted peanut butter, cookies, and ice cream products, Congress gave the FDA broad food-inspection powers." In 1970, Congress created both OSHA and the EPA, with inspection powers.

Only a handful of the largest regulatory agencies—the FTC, the NLRB, and the EEOC—lack strong monitoring groups.[6] Notably, all three are focused on protecting individuals from economic harms. And the EEOC has obtained some monitoring power by using its original statutory authority to write rules that require businesses to submit to the EEOC confidential employee data broken down by race, gender, and other categories.

"[T]he creation of the CFPB in 2011 represented a break with the traditional absence of visitorial authority for regulators focused on protecting against economic harms to individuals." Unlike the FTC, the CFPB was given broad visitorial authority to regularly appear on-site at regulated industries.[7]

In sum: "Across diverse industries and under both Democratic and Republican party leadership, Congress has since the mid-1800s steadily expanded federal agencies' ability to monitor private firms. This historical accumulation of federal authority also spans industries ... governed by small and medium regulators—areas such as offshore oil drilling, liquor stores, and firearm manufacturers. Overall, among the nineteen large federal regulators, only the NLRB is without substantial monitoring authority. Two others, the FTC and the EEOC, have the meaningful ability to collect records but not to conduct on-site inspections. Sixteen of the nineteen largest agencies have both strong visitorial monitoring and record-collection authority."

[6]Those familiar with the FTC may not realize how unusual it is among federal regulatory agencies in its underutilization of monitoring. According to Rory Van Loo, who estimated the total pool of monitors and legal personnel at the 19 largest federal regulatory agencies, at the FTC barely 3% of those employees are monitors, while over 97% are legal personnel (largely conducting investigations). In contrast, at 11 of the 19 agencies, regulatory monitors make up over 85% of the combined regulatory-monitor and legal workforce.

[7]The CFPB has used this authority in its privacy enforcement against financial institutions. Rory Van Loo, *Technology Regulation by Default: Platforms, Privacy, and the CFPB*, 2 Geo. L. Tech. Rev. 531 (2018).

Potential benefits of regulatory monitoring

There are pros and cons to the supervision-based model. It has been criticized for its susceptibility to the development of too comfortable a relationship between supervisors and their regulated entities.[8] Indeed, for such reasons, the FTC abandoned the use of informal settlement agreements decades ago.[9] Where compliance notices are confidential, as they are in some cases, outsiders may have no idea what the regulators are finding in terms of problematic activity and what they are requiring the regulated entities to do in terms of corrective action.

However, the regulatory monitoring model may be well-matched with two relatively recent changes in the overall approach to government regulation of the private sector: the emphasis on collaboration or cooperation with business and the rise of compliance departments inside corporations. Quoting Van Loo (as we do throughout this section except where otherwise noted): "The cooperative model aims to free the parties to focus their energies on fixing mistakes and identifying causes instead of fighting over whether anything was wrong." The rise of compliance departments could be characterized as "self-regulation," but it recognizes that "[f]iscal constraints simply make it impossible to monitor all private actions even for the most dangerous activities." Under the compliance model, instead of examining every product for strict adherence to a code, "the agency 'intervene[s] at the planning stage, compelling regulated organizations to improve their internal management so as to increase the achievement of public goals."'

In the privacy field, the emergence of chief privacy officers and the build-out of corporate privacy compliance structures have been major, even revolutionary developments. In the private sector in the US, they evolved largely without being required by statute or regulation and without even acknowledgement in the sectoral legal framework.

In other fields, the rise of self-regulation/internal compliance is linked to increased reliance on third-party gatekeepers, discussed further below. "[T]hird-party certification is used in a wide array of domains, including food safety, pollution control, product safety, medical devices, and financial accounting." Regulatory monitors shift their emphasis from examining the details of paperwork or safety valves to making sure that the in-house compliance unit and third-party gatekeepers do their jobs. "In other words, the firm's compliance team essentially serves as the regulatory monitors' agents."[10]

Likewise, the move to compliance management may be associated with a greater reliance on best practices as opposed to rules. "In the Clean Water Act, Congress mandated that states and the EPA identify 'best management practices' for tackling the biggest source of water pollution: runoff from cities and farms. The EPA then shares 'success stories' that can be adopted elsewhere. ... [I]n a world of best practices, there are often multiple ways to satisfy the mandate. A best practices regime thereby allows agency regulatory

[8] Agency capture is a serious issue and may lead to tragic results, as it seems to have in the two fatal crashes of the Boeing 737 MAX. See David Shepardson, *U.S. House report blasts failures of Boeing, FAA in 737 MAX certification*, Reuters (Sept. 16, 2020).

[9] See Concurring and Dissenting Statement of Commissioner J. Thomas Rosch Regarding Google's Search Practices, *In the Matter of Google Inc.,* FTC File No. 111-0163 (Jan. 3, 2012). Commissioner Rosch noted, "The Commission has, at times, permitted respondents to avoid an enforcement action by terminating the offending conduct, but only when the underlying conduct was promptly corrected upon notice of a possible violation and the risk of a future violation was remote."

[10] The GDPR addresses codes of conduct and certifications in Chapter IV, Section 5, but these tools are still relatively new and underused.

monitors not only to identify the best practices in the first place but also to assess whether a given firm's practices come close enough to 'best."'

A monitoring approach is also responsive to certain market changes, including the greater sophistication of modern businesses, the pace of innovation, and the ubiquity of information technologies. Even monitors who operate inside regulated firms can fail to understand rapid, complex developments in an industry, but, in contrast to agency lawyers, monitors are more likely to have the expertise necessary to keep up. In general, the supervision-based model is designed to promote the free flow of information. That may be all the more true in the age of big data, as monitoring agencies may have access to huge amounts of data and the capability to analyze it for indicators of wrongdoing or other relevant trends. Remote monitoring devices can continuously transmit data to the regulatory monitors. Every day, data on millions or even billions of reports on conditions or transactions flow from energy companies to FERC and from securities firms to the SEC.

The graduated enforcement continuum available to monitors

Most monitoring agencies have at their disposal a graduated continuum of enforcement options, ranging from warning letters to civil litigation or criminal prosecution. When monitoring activities detect wrongdoing, the monitors—EPA inspectors, bank examiners, and others—exercise influence over a regulated industry through multiple means, ranging from informally requesting that businesses change behavior to mandating the suspension of business activities. At many agencies, the options most frequently exercised are those outside the court system.

The ultimate power of a monitor, available in many agencies, is the power to take away a business's freedom to operate. Monitors can shut down dangerous workplaces or polluting factories or offshore drilling operations. In at least eleven of the nineteen largest federal agencies, regulatory monitors exercise the authority to prevent business operations ex ante or to suspend market access ex post. Federal regulators can recall toys, automobiles, and food based on health or safety concerns. Environmental inspectors can shut down companies that are discharging hazardous chemicals. Bank monitors can revoke a bank's license. In reality, monitors rarely stop a business from operating, but the fact that that remedy is hanging over the relationship smooths the transfer of information and encourages agreement on lesser sanctions and remedial actions.

Short of closing a plant or revoking a bank's license, monitors can obtain corrective action merely by recommending it. For example, bank supervisors may just ask a bank to refund incorrect fees or fix whatever compliance problem was identified without ever having a publicly available enforcement action. These actions are called "matters requiring attention" or MRAs, and their content is confidential.

FERC monitors possess a similar authority to issue public "noncompliance" notifications and direct nonpublic settlement agreements. For instance, in fiscal year 2016, the FDA's inspections group issued 14,590 warning letters, while its legal division took only twenty-one enforcement actions. In terms of behavioral impact, these recommendations can be far-reaching. Compliance varies across time and agencies, but there are indications that in diverse industries companies cooperate when informally advised to take a course of action.

In other contexts, these notices of noncompliance are public. Public shaming can have a powerful effect. Quoting Van Loo, "Given that a few thousand dollars in fines is insignificant to a large company, the public posting of monitoring violations enables some regulatory monitors to have greater enforcement power over businesses."

The act of supervision itself may also be an enforcement tool. Supervisors can also impose costs on regulated companies by ramping up inspections, or, as a carrot, they can lighten their supervisions, as a reward for compliance.

Warning letters and recommendations can also have an impact far beyond the specific entity that receives the letter. They may constitute a body of law, closely followed by regulated entities, even in the absence of rulemaking. Inspection manuals, although binding only on the employees carrying out the inspections, serve also as compliance guides: These manuals give instructions as to what information the regulatory monitors should collect and how they should analyze the data they observe, and firms meticulously study these texts to adjust their behavior.

3 | Information Disclosure to Support Market-based Enforcement

Sometimes, a policy of information disclosure can force private actors to voluntarily solve a problem in some market-based way.[1] Overall, information disclosure may have proved disappointing as an enforcement mechanism, but those targeted at digital intermediaries may have the most promise among this category. "Travel websites such as Expedia and Travelocity benefitted from government mandates that airlines release flight prices and times online. These intermediaries help to regulate by enabling a marketplace filled with informed consumers, thereby deterring undesirable business practices. Although legal authority made the information available, it did not require any private actor to use that information to regulate."[2]

Another successful example is an Israeli law from 2015 that requires stores to release their price and product information in machine readable form. The intent of that law was for online price comparison tools to spring up and allow shoppers to go online and figure out in advance where they should buy what products at the lowest prices. And that is what actually happened. Researchers have concluded that that one intervention caused prices to lower by 4—5%. In other words, to solve the problem of consumers being harmed by high prices, the legislature took the route of leveraging information disclosure and digital intermediaries, which then put market pressure on stores.

Disclosure as warning and as admission

Since its inception, the National Labor Relations Board has used the remedy of remedial notice posting.[3] "This remedy typically requires that a transgressor employer or labor union post physical (or more recently, electronic) notice in a conspicuous place for the affected employees to read. ... [T]he remedial notice remedy seeks to provide employees with the information they need to ameliorate the coercive effects of past unfair labor practices, and spot future unfair practices when they occur. Further, notice-posting requirements also have a deterrent component ... ."[4] In egregious cases, the NLRB orders employers to read the notice aloud to employees, although several appeals courts have rejected that practice.[5]

[1] Section based on Prof. Van Loo's workshop presentation.

[2] Rory Van Loo, *The New Gatekeepers: Private Firms as Public Enforcers*, 106 Va. L. Rev. 467, 477 (2020).

[3] Drawn from the workshop presentation of Prof. Aditi Bagchi, Fordham University Law School.

[4] Thomas C. Barnes, *Making the Bird Sing: Remedial Notice Reading Requirements and the Efficacy of NLRB Remedies*, 36 Berkeley J. of Emp. and Labor Law 351 (2015).

[5] See *Sysco Grand Rapids, LLC v. NLRB*, 825 Fed. Appx. 348, 359-60 (6th Cir. 2020) (denying enforcement of the remedy of a public notice reading). The limits of such notices were illustrated,

Traditionally, FTC privacy settlements have gone in the opposite direction, containing no finding of wrongdoing and containing a clause stating that the respondent neither admits nor denies the allegations. They generally have not required notice to the consumers affected by the allegedly unfair or deceptive practice. However, in January 2021, the FTC announced a settlement that required the respondent to affirmatively notify its customers of what data disclosure the company had made and that the company had recently entered into a settlement with the FTC "to resolve allegations that sharing this information was inconsistent with the promises we made to you."[6] Commissioners Slaughter and Chopra filed a separate opinion stating that the Commission had never before ordered such notice of a privacy action and, moreover, stating their view that the FTC should presumptively seek notice provisions in privacy and data security matters, especially in matters that do not include redress for victims.

This harkens to earlier decades of false advertising enforcement, where the FTC has ordered "corrective advertising," that the advertisers affirmatively run a marketing campaign disabusing the public of the falsehoods.[7] While corrective advertising is seen as an extreme remedy, it is not at all clear that it works: consumers may not hear the message, consumers may misinterpret it, or consumers might hear the message and generalize a negative attitude to a class of companies instead of the wrongdoer. One major counter-advertising effort, the anti-tobacco "Truth" campaign, has been shown to reduce intent to smoke, but it did so by provocatively and loudly elucidating the deceptive marketing of an entire industry.

The promotion of policy goals can also be served by ex ante disclosures, in the form of impact assessments intended to (a) inform decision-makers of the potential adverse effects of a project, policy, or action and (b) identify ways to mitigate those impacts. The concept originated in the environmental field, where Environmental Impact Assessments (EIAs) have long played a role. Federal agencies have been required to perform Privacy Impact Assessments (PIAs) since the E-Government Act of 2002. Article 35 of the EU's General Data Protection Regulation requires regulated businesses to conduct PIAs of any data processing that is likely to result in a high risk to the rights and freedoms of natural persons, and regulations to be issued under the new California Privacy Rights Act will likewise require PIAs. There seems to have been little evaluation in the U.S. of the effectiveness of EIAs or the PIAs required under the E-Government Act. Effectiveness data seems to be more readily available for health impact assessment (HIAs), which governments at all levels began using about 20 years ago to determine the potential

anecdotally, in a recent news report. Five years ago, an employer was compelled by the NLRB to post a notice to employees at one of its facilities, promising not to engage in certain anti-union behavior. However, the employer is now alleged to be engaging in the very same behaviors at other facilities. "The employee notice was a hollow victory for workers. The National Labor Relations Board, the federal agency that negotiated the settlement with Amazon, has no power to impose monetary penalties. Its enforcement remedies are few and weak, which means its ability to restrain anti-union employers from breaking the law is limited. The settlement [requiring the notice] was not publicized, so there were not even any public relations benefits." David Streitfeld, *How Amazon Crushes Unions*, The New York Times (Mar. 16, 2021).

[6] *In the Matter of Flo Health, Inc.*, FTC File No., 1923133 (Jan. 13, 2021), https://www.ftc.gov/system/files/documents/cases/flo_health_order.pdf

[7] *See Warner-Lambert Co. v. FTC*, 562 F.2d 749 (D.C. Cir. 1977), *cert. denied*, 435 U.S. 950 (1978) (Listerine was compelled to run ads stating, "Listerine will not help prevent colds or sore throats or lessen their severity").

health effects of proposed policies, plans, programs, or projects..[8] Studies have found that HIAs can be effective, although a lot depends on the receptiveness and flexibility of the decision-maker.[9] A 2011 report by a National Research Council committee assumed that HIAs could be effective and called for their greater use.[10]

Like all of the enforcement measures discussed here, disclosure alone is not sufficient. Consider cybersecurity: California's breach notification law became effective in 2003, and by at least 2010, breach notification was de facto a national standard. Breach notice has probably changed corporate behavior by reducing unnecessary collection and storage of sensitive data such as Social Security Numbers, but few if any would claim that a decade of breach notices has created sufficient incentives for information security.[11]

[8]While the HIA, popular in some other countries, is not yet widely used in the United States, one study found that more than 390 HIAs had been completed or were in progress in the United States as of early 2016. Andrew Dannenberg, *Effectiveness of Health Impact Assessments: A Synthesis of Data From Five Impact Evaluation Reports.* Prev. Chronic. Dis. 2016;13:150559, https://www.cdc.gov/pcd/issues/2016/15_0559.htm.

[9]See Justicia Rhodus, Florence Fulk, Bradley Autrey, Shannon O'Shea, and Annette Roth, *A Review of Health Impact Assessments in the U.S.: Current State-of-Science, Best Practices, and Areas for Improvement* (EPA, 2013) (of those HIAs for which measures of effectiveness could be obtained (n=50), 60% show direct effectiveness, 32% showed general effectiveness, 6% showed no effectiveness, and 2% showed opportunistic effectiveness). See also Pew, *Health Impact Assessments Can Help Improve Decision-Making* (Nov. 2020); Dannenberg, supra.

[10]National Research Council Committee on Health Impact Assessment, *Improving Health in the United States - The Role of Health Impact Assessment* (2011).

[11]A study published in 2011, based on data from 2002-2009, concluded that adoption of data breach disclosure laws reduced identity theft caused by data breaches, on average, by 6.1%. Sasha Romanosky, Rahul Telang, and Alessandro Acquisti, *Do Data Breach Disclosure Laws Reduce Identity Theft?,* Journal of Policy Analysis and Management, 30 (2), 256—286 (2011). However, the laws' effect on ID theft may have faded as individuals and companies have become habituated to them and cyber-criminals have continued to innovate: During the years covered by the study, identity theft reports to the FTC were running at about 250,000 a year. In 2020, two years after every state in the nation had a data breach notice law, the FTC logged 1.4 million ID theft reports; in 2019, the number was 650,523.

A more recent article, probing the often unarticulated justifications for breach notification laws, is very skeptical that the current laws are well-suited to achieve any of their goals. See Mark Verstraete and Tal Zarsky, *Optimizing Breach Notification* (July 14, 2020), U. Ill. L. Rev. (forthcoming 2021), available at SSRN: https://ssrn.com/abstract=3650724.

4 | Diffuse and Intangible Harms: Lessons from Environmental Law

One way to view environmental law statutes is that they try to address characteristics of tort law that fit poorly with a modern economy.[1] There have been toxic spills, pollution, and other environmental harms for a long time, and for much of our legal history, these were governed by nuisance law and other tort doctrines. For a relatively simple economy, basic tort law worked. But it does not work for a large scale, complex industrial economy, for a number of reasons: The harms are long term, and they may be synergistic in that there may be multiple pollutants that cause health damage. As a result, there may be difficulties in showing causation. The harms are often very diffuse, affecting a lot of people in a small way, leading to collective action and free rider problems. Tort law tends to be individualized, while many environmental harms are not to individuals, but rather are collective harms, such as to public lands or water resources used by all. And some environmental harms are intangible, like the damage to a pristine wilderness from an oil spill, raising problems of valuation.

How does environmental law seek to overcome the limits of tort law through enforcement and remedies? As a baseline, there are statutory requirements, such as emission limits under the Clean Air Act, that the government enforces. Under the Clean Air Act, the government can issue an administrative order, requiring a person to come into compliance, it can issue administrative penalty orders, and it can bring a civil action in court for injunctive relief and monetary penalties. 42 U.S.C. § 7413. This overcomes the collective action problem: the government does the enforcement rather than individual tort law plaintiffs. And it also overcomes the causality problem to some extent because the government does not have to show harm, it just shows that the emission limit or other statutory or regulatory limits were violated. Specifically in terms of penalties, the Clean Air Act establishes penalties of up to $25,000 per day per violation for statutory violations, including for violation of reporting obligations.

The Superfund law (officially known as the Comprehensive Environmental Response, Compensation, and Liability Act of 1980) offers some interesting innovations. It addresses the problem of old hazardous waste sites that many parties contributed to, where there would be huge costs in trying to figure out who is responsible and who contributed to the harm to what degree. To solve this problem, the Superfund law has a rule of joint and several liability, which essentially puts all the burden of investigating and apportioning blame on any one of the potentially responsible parties. The government can sue just

[1] Unless otherwise noted, this section is based on a workshop presentation by Professor Dennis Hirsch, Ohio State University Moritz College of Law, and on Dennis Hirsch, *Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law*, 41 Ga. L. Rev. 1 (2006) https://ssrn.com/abstract=1021623.

one party for the entire cost of cleanup, which incentivizes that party to investigate and find the other responsible parties (or else pay the whole bill).

The Superfund law redefines tort doctrines in another way to make these lawsuits possible. In order to succeed in a lawsuit against a potentially responsible party that may have disposed of hazardous substances at a site, the government does not have to show harm. It only has to show that the defendant disposed of hazardous substances at the site. The government doesn't have to show the specific harm the defendants individually caused since they are jointly and severally liable if they can be tied to the site.

The environmental field also uses incentives for good behavior. Both the federal EPA and many state EPAs have leadership programs that recognize environmental excellence. In some cases they might give regulatory flexibility in exchange, sometimes they just give recognition.[2]

There is also market-based regulation through, for example, emission fees, which give emitters an incentive to figure out ways to reduce their emissions for less than the cost of the fee, and those who do enjoy a competitive advantage over others who cannot.

The environmental field also relies heavily on self-regulation overseen by regulators: "EPA rules, for example, require companies producing hazardous chemicals to build a risk management plan and perform inspections of their equipment. Companies must regularly submit the documentation to authorities, listing all incidents that have occurred. Environmental agencies then audit those internal reports, which may result in a "determination of necessary revisions" to the company's systems."[3]

Using surveys to measure damages

Another interesting approach, found in the Superfund law and also in the Oil Pollution Act, is a concept called natural resource damages.[4] This approach addresses problems of collective and intangible harms. It works this way: Under the Oil Pollution Act, if a company spills oil, it is liable to individual landowners for whatever damage is caused them and it may be liable under the Act to conduct a cleanup. However, in addition to cleanup costs, the company is also liable for natural resource damages, which is the cost of restoring the resource once the cleanup has been completed, and the lost use values during the time that the resource was damaged and was unavailable to fishermen and

[2]See, for example, EPA Press Office, *U.S. EPA Recognizes Freight Industry Leaders for Environmental Performance* (11/05/2020) https://www.epa.gov/newsreleases/us-epa-recognizes-freight-industry-leaders-environmental-performance; Ohio EPA, *Encouraging Environmental Excellence (E3) Program* https://www.epa.state.oh.us/ocapp/ohioe3.

[3]Rory Van Loo, *Regulatory Monitors: Policing Firms in the Compliance Era*, 119 Columbia L. Rev. 369 (2019). Along similar lines, U.S. export control law encourages voluntary self-disclosure of export violations by treating it as a mitigating factor in determining administrative sanctions. See 15 C.F.R. § 764.5.

[4]"When a spill or release of contaminants into the environment results in injuries to natural resources, Natural Resource Damages (NRD) are sought from the party or parties legally responsible in order to restore the injured natural resources and compensate the public. The goal of an NRD claim is the restoration, replacement, or acquisition of the equivalent of the injured resources, and compensation for past and future lost services that the injured resources would have provided had they not been injured by the release." NY State Dept. of Environmental Conservation, *Natural Resource Damages* (NRD) https://www.dec.ny.gov/regulations/2411.html. See US EPA, *Natural Resource Damages: A Primer* https://www.epa.gov/superfund/natural-resource-damages-primer.

others who might have wanted to use it. There is a trustee who brings the action on behalf of the public and manages the damages.

This takes into account the intangible value of the resource, using something called contingent valuation methodology. The contingent valuation method is applied through conducting a survey in which people are directly asked how much they would be willing to pay (WTP) to enjoy a specific natural resource.[5] Surveys may use the travel cost methodology, asking how much people pay to travel to get to a particular natural site as a way of estimating what the value of the resource is to an individual. Surveys are a way of valuing both collective damage to collective goods and intangible harms.[6]

[5]See Environmental Justice, Contingent Valuation http://www.envjustice.org/2012/12/contingent-valuation/. Although CVM has been used in cost-benefit analysis and environmental impact assessment for several decades, it has been subject to many critiques.

[6]See Daniel R. Petrolia, Dennis Guignet, John Whitehead, Cannon Kent, Clay Caulder, Kelvin Amon, *Nonmarket Valuation in the Environmental Protection Agency's Regulatory Process, in* Applied Economic Perspectives and Policy (15 October 2020) https://doi.org/10.1002/aepp.13106. Parties have also used surveys in patent infringement cases to show the monetary value consumers place on a particular feature. "Long a staple of trademark, false advertising and antitrust cases, consumer surveys are now de rigueur in patent cases as well." *Sentius Int'l, LLC v. Microsoft Corp.*, No. 5:13-cv-00825-PSG, 2015 U.S. Dist. Lexis 8782, at *2 (N.D. Cal. Jan. 23, 2015). A commonly used method is known as a conjoint survey. In a conjoint survey, an expert attempts to quantify customer preferences for certain product attributes, which enables the expert to estimate the "market's willingness to pay" for a particular, patented feature. John D. Luken and Lauren Ingebritson, *Recent Trends in Reasonable Royalty Damages in Patent Cases in in Remedies in Intellectual Property Cases* (Defense Research Institute 2018) https://www.dinsmore.com/content/uploads/2018/11/2018_02_Remedies_01_Patents_A_Royalty_Damages.pdf.

5 | Gatekeepers and Other Third Parties

For some time now, regulatory systems have relied on private sector enforcers,[1] such as certification bodies, self-regulatory organizations, accountants, lawyers, and other "gatekeepers."[2] For instance, under the SEC's disclosure-based system of regulation, a publicly traded company must obtain the signoff of a certified accountant before releasing its annual reports. Bank regulation likewise has long relied on gatekeepers who could withhold approval of required statements or audits if the company was out of compliance. In the environmental field, agencies also enlist private third-party monitors to assess compliance. Rather than directly conducting inspections, a regulator may instead write a rule requiring certification from an accredited third-party inspector. Statutes and court orders compel businesses in diverse industries to hire third-party monitors. The FTC already requires independent assessments in its data security settlements although—as noted above—this falls far short of formal audits.

This has been called "audited self-regulation." "For example, the Federal Aviation Administration certifies individuals to conduct inspections, tests, and training in various areas of pilot and aircraft certification, and the Department of Agriculture certifies veterinarians to make various inspections, examinations, and certifications under animal health statutes and regulations."[3]

Of course, gatekeepers may fail miserably, as illustrated by the sudden and very costly collapse of Enron after years of accountants' audit reports showing huge profits

More recently, the use of gatekeepers in the financial services sector has expanded and the large firms have themselves been enlisted as gatekeepers. The Consumer Financial Protection Bureau requires large financial institutions to make sure that their third-party service providers comply with consumer protection laws, essentially anointing the banks as regulators. The regulated third parties include mortgage servicers, call centers, debt collectors, software developers, and real estate lawyers. This goes one step beyond making

[1] This section is based on Rory Van Loo, *The New Gatekeepers: Private Firms as Public Enforcers*, 106 Va. L. Rev. 467 (2020), available at SSRN: https://ssrn.com/abstract=3498042. Unless otherwise noted, all quotes are from that article, footnotes omitted.

[2] Even "[i]ndependent of any legal influence, firms monitor other firms solely out of self-interest. For instance, when land is the collateral for a loan, banks may inspect the property periodically to ensure that the borrowing firm is not releasing hazardous chemicals or otherwise damaging that collateral. Insurance companies also monitor the businesses that they insure to prevent legal violations that would cause the insurer to make large payouts under the policy. The prospect of reducing costs motivates such monitoring, but the monitoring advances the public interest. ... In recent decades, private entities increasingly regulate to advance social causes for reasons beyond protecting their direct investments or members. For example, Walmart imposes recycling and energy conservation requirements on its vendors, and Nike and Apple audit their manufacturing facilities to prevent child labor and other abuses."

[3] Douglas C. Michael, Federal Agency Use of Audited Self-Regulation as a Regulatory Technique, 47 Admin. L. Rev. 171, 179 (1995).

the banks vicariously liable for the conduct of their third-party service providers. Instead, the bank regulator spells out specific steps that the banks must take to control the third parties. The regulator may require banks, in their contracts with third parties, to include a cancellation clause that allows the bank to cancel its contract to punish a provider of call center services if it has violated the law. Or the regulator may require the banks to develop mechanisms to monitor their third parties. Then the regulator can sanction the bank not because the regulator proves that the third party did anything wrong, but because the bank didn't adequately have a monitoring system in place for that third party. Under this arrangement, banks actively audit the contracts between their third parties and consumers, because the banks know that if that a third party (such as a mortgage servicer) is imposing fraudulent contracts on the third party's customers, the bank is going to be liable, even just for that contract existing with the consumer. The banks even listen in on customer service calls of their third-party service providers to make sure they don't violate the law.

Other large firms at the center of the economy have been enlisted as enforcers. Again quoting Van Loo, "The world's largest businesses must routinely police other businesses. By public mandate, Facebook monitors app developers' privacy safeguards ... and Exxon reviews offshore oil platforms' environmental standards. Firms thus enlisted in regulatory schemes must write rules in their contracts that reserve the right to inspect third parties. When they find violations, they must pressure or punish the wrongdoer."

Gatekeeper regimes have become quite explicit and extensive in key sectors. As of 2018, the ten largest American companies by valuation operated in information technology, finance, oil, and pharmaceuticals. A regulator has put leading firms in each of these industries on notice about their responsibilities for third-party oversight. "[T]he Environmental Protection Agency (EPA) ... requires BP Oil and other energy companies to audit offshore oil platform operators for environmental compliance. The Food and Drug Administration (FDA) expects Pfizer and other drug companies to ensure suppliers and third-party labs follow the agency's health and safety guidelines The Consumer Financial Protection Bureau (CFPB) orders financial institutions, such as American Express, to monitor independent debt collectors and call centers for deceptive practices."

Traditionally, the gatekeepers (accountants, for example) were hired by the parties they were supposed to regulate. If the gatekeeper did not sign off on the activity or filing of its client (the regulated entity), the regulated entity could hire a new, more accommodating gatekeeper. In contrast, in the newer model, the enforcer-firm is usually the client—or at least a crucial business partner—of the third parties it regulates. Its main sanction is to cease doing business with those third parties, which can prove devastating. "The client relationship that weakens traditional gatekeepers thus strengthens the enforcer-firm. In short, policymakers have begun relying on third-party enforcement by the real gatekeepers of the economy: the firms who control access to core product markets."

For example, after the Cambridge Analytica scandal, the FTC privacy settlement with Facebook required Facebook to safeguard what happened to users' data even after it reached a third party's custody. So now, if an app developer is not behaving, Facebook is expected to bring it into line or shut the gate, meaning cutting off the app's access to Facebook. This type of requirement dates back at least to the 2011 Resellers case, in which the FTC required data brokers to oversee the security practices of the mortgage companies to which they sold consumer data.[4]

The trend towards enlisting major companies as enforcers offers some hope for improving upon prior regulatory models' accountability. Because enforcer-firms often sell directly to consumers, they may prove more responsive to public concerns when compared to traditional gatekeepers, which interact most closely with regulated entities. And because the enforcer-firm is itself a prime target of public regulation, it would be easier for an administrative agency to oversee it than to add a whole new category of firms as required for oversight of traditional gatekeepers.

Gatekeepers in the tech sector

In the internet and information technology sector, there are a number of areas where intermediaries regulate functions by imposing rules on business users. (Note: These tend to be of the older model, where the regulated entity gets to choose its gatekeeper, and the gatekeeper, unlike the enforcer-firms discussed above, does not have a direct relationship with the consumer.) For instance, under the Children's Online Privacy Protection Act (COPPA), the FTC approves "seal" programs for companies that promise adherence to self-regulatory guidelines; companies that comply with an approved program shall be deemed compliant with the Commission's COPPA regulations.[5] Outside seal programs, IT companies have developed other voluntary measures to effectuate consumer laws. For instance, large scale SMS text services automatically recognize "stop words" (words such as "stop" or "unsubscribe" that indicate that a person no longer wishes to receive messages from a sender) and refuse to send text messages from their clients (businesses seeking to communicate with consumers) to those consumers.[6] On a high level, this is because the TCPA and other marketing laws impose advertiser and platform liability for violation of consumer rights.

In its administrative orders and settlements, the FTC has long required respondent companies to hire third party assessors to certify compliance. In that arrangement, refusing to sign off on the respondent's mandated reports to the FTC constituted the assessor's main sanction. As noted above, the regulated company could, however, respond to that sanction by bringing its business elsewhere. Increasingly, the FTC has limited respon-

[4]Lesley Fair, *Data Resellers Liable for Downstream Security Failures*, FTC Business Blog (Feb 16, 2011), https://www.ftc.gov/news-events/blogs/business-blog/2011/02/data-resellers-liable-downstream-security-failures.

[5]The safe harbor is mandated by 15 U.S.C. § 6503. The rules for the program provide that, in considering whether to initiate an investigation or bring an enforcement action against an entity covered by COPPA, the Commission will take into account the history of the entity's participation in the safe harbor program. 16 C.F.R. § 312.11. See FTC, *COPPA Safe Harbor Program*, https://www.ftc.gov/safe-harbor-program. See also, for example, FTC, *Letter from the Commission Approving kidSAFE Seal Program* (Feb. 11, 2014) https://www.ftc.gov/system/files/attachments/press-releases/ftc-approves-kidsafe-safe-harbor-program/140212coppa-safeharborapp.pdf.

[6]See, for example, Twilio, Twilio support for opt-out keywords (SMS STOP filtering); Tenyx, *SMS Opt-Out Keywords and Stop Words*,

dents' choice in selection of assessors because of a fear that respondents were choosing assessors strategically.

Also, U.S. privacy and data security laws have for some time required data controllers to impose contract terms on their third-party vendors forcing them to adhere to the same standards as the controllers: HIPAA, before it was amended to directly regulate third parties processing covered health data, required covered entities to bind their business associates to protect data. Likewise, the data security "common law" of the FTC requires entities to exercise control over the security practices of service providers to whom any data flows, as do the "reasonable security" laws of many states.

6 | Compensation Versus Deterrence

In many fields, including, for example, contracts, intellectual property, and consumer protection, the law of remedies draws a distinction between compensation and deterrence.[1] In some schemes, such as commercial contracts, remedies are focused on compensation for breaches, not their deterrence. Indeed, one view of contract law is that its remedies structure allows, even encourages, "efficient breaches," so long as the injured party is compensated for the harm it suffered. However, consumer contracts are treated differently. In the consumer context, both the common law of fraud and false advertising and the statutes on unfair and deceptive trade practices have remedies structures that are designed to deter wrongdoing.

Intellectual property law relies on multiple types of remedies, with different goals:

- Injunctions, to prevent future infringement and stop irreparable harms;
- Actual damages, to compensate for harms to the plaintiff;
- Disgorgement of profits, to prevent unjust enrichment and deter wrongdoing;
- Statutory damages, to provide some compensation when it is difficult to prove actual damages;
- Enhanced damages, to punish willful infringers.

Across the branches of IP law (utility patents, design patents, copyright, trademarks, and trade secrets), there are nuanced variations in how these remedies are deployed and under what standard. Burdens of proof can be very important: If the burden is on the plaintiff, it may be very difficult to prove, for example, lost sales. Statutory damages offer a way of setting compensation when harm is difficult to measure or prove. However, the experience from intellectual property law is that it is very hard to set the right amount: depending on the circumstances, statutory damages may over-compensate or under-compensate.[2]

The overarching point that emerges from a consideration of damages in these fields is that the remedies must be linked to the goals. The first question must be whether the goal of the system is compensation or deterrence. A compensation-based regime will probably not be effective in deterring undesirable conduct.

[1] This section is based on workshop presentations by Prof. Gregory Klass, Georgetown University Law Center; Prof. Pamela Samuelson, UC Berkeley Law School; and Ted Mermin, UC Berkeley Law School.

[2] For more on remedies in the intellectual property field, see Pamela Samuelson and Mark P. Gergen, *The Disgorgement Remedy of Design Patent Law,* 108 Calif. L. Rev. 183 (2020); Pamela Samuelson, John M. Golden, and Mark P. Gergen, *Recalibrating the Disgorgement Remedy in Intellectual Property Cases,* 110 Boston U. L. Rev. 1999 (2020); Pamela Samuelson and Tara Wheatland, *Statutory Damages in Copyright Law: A Remedy in Need of Reform* 51 William & Mary L. Rev. 439 (2009).

7 | Class Actions, Citizen Suits, and Injunctive-Only Relief

The consumer class action has been hotly debated for decades, with studies on both sides, arguing for or against the merits of class actions, criticizing or defending the percentage of settlements or other recoveries that go to plaintiffs' attorneys instead of plaintiffs, and contesting the fundamental question of whether class actions actually produce meaningful change in corporate behavior. (On the latter concern, specifically in the context of privacy and data security matters, it has been noted that many apparently high-stakes cases were settled for less than $10 million, a sum too low to create general or specific deterrence.[1])

Aside from damages, discovery is an important element of class action lawsuits, as discovery often helps plaintiffs understand how data are actually collected and used. Several high-profile cases in recent years became more credible as a result of the discovery process unearthing practices that differed from companies' public statements. We cannot resolve all the controversies surrounding class actions, but it may be helpful to cite some of the more recent research in favor of class actions.

In 2016, Deborah Hensler concluded that "the available evidence is too incomplete to determine the general effectiveness of private class actions in regulating different sectors of the economy. The inadequacy of the evidence demonstrates that policy makers should be cautious about popular assertions about both the benefits and costs of class actions." However, from this she drew the conclusion that, "[u]ntil better data are available on the relative contribution of public and private mechanisms to the enforcement of economic regulation, ... we should craft regulatory policies that promote redundancy."[2]

In an intensive investigation of the outcomes of six consumer actions arising out of provision of services rather than products, Hensler et al. found that defendants agreed to change their practices in all six.[3] Brain Fitzpatrick of Vanderbilt Law School concluded that, "There is no doubt that class actions generate specific deterrence."[4] When Fitzpatrick examined every single class action settlement in federal court over a two year period, he found that almost one-quarter of the time the settlement included a provision requiring the defendant to change its behavior in some way. In some types of class action

[1]The too-low settlement trend could end. Consider that, in a recent case where the defendant argued there was no injury to the plaintiff class, it nevertheless eventually settled for $650 million.

[2]Deborah Hensler, *Can private class actions enforce regulations? Do they? Should they? in* Comparative Law and Regulation: Understanding the Global Regulatory Process (Francesca Bignami and David Zaring, eds., 2016).

[3]D. Hensler, N.M. Pace, B. Dombey-Moore, B. Giddens, J. Gross and E.K. Moller, Class Action Dilemmas: Pursuing Public Goals for Private Gain 145-73 (2000).

[4]Brian Fitzpatrick, The Conservative Case for Class Actions 100 (2020).

lawsuits, he found behavior modification provisions as often as 75% of the time.[5] Fitzpatrick also found that class actions have a general deterrence effect—that is, they deter potential wrongdoers:

> [T]here is indeed evidence. It is not reams and reams of evidence, but there are now several studies, they span different time periods, they involve different types of class actions, and, with one exception, they all say the same thing: class actions deter misconduct.[6]

As to consumer compensation, Fitzpatrick and Robert Gilbert concluded that, under certain circumstances, consumer class actions can indeed serve a meaningful compensatory role: when they eschew claim forms in favor of automatic distributions, and when they rely on standard-sized checks (rather than the cheaper, postcard-sized variety) and especially when they use direct deposits to make those distributions.[7]

Citizen suits

One interesting characteristic of environmental laws are the citizen suit provisions.[8] Under these provisions, any affected individual can vindicate the public's rights.[9] Under the Clean Water Act, for example, two types of citizen suits are authorized: (1) against any person, (including any government agency) who is alleged to be in violation of an effluent standard, or (2) against the EPA Administrator where there is alleged a failure of the Administrator to perform any act or duty under this chapter which is not discretionary with the Administrator. 33 U.S.C. § 1365. This is not about seeking compensation for an individual or even for a class of individuals. (Under the Clean Air Act, for example, any penalties assessed by the court must be deposited into a special fund in the U.S. Treasury; small amounts may be used for beneficial mitigation projects which enhance the public health or the environment. 42 U.S.C. § 7604(g).) Instead, it is about enforcing the statute where the EPA or relevant regulator has not done so. It is a private right of action to vindicate public rights. The process often requires notice to the regulator and, if the regulatory body proceeds, then the private suit cannot proceed. (Under the Clean Water Act, if the EPA does initiate a lawsuit in federal court, "any citizen may intervene as a matter of right." 33 U.S.C. § 1365(b)(1)(B).)[10]

---

[5] Id.

[6] Id. at 109.

[7] Brian T. Fitzpatrick and Robert Gilbert,, *An Empirical Look at Compensation in Consumer Class Actions* (March 6, 2015), https://ssrn.com/abstract=2577775.

[8] Based on a workshop presentation by Professor Dennis Hirsch, Ohio State University Moritz College of Law.

[9] Citizen suits remain subject to the standing requirements of Article III. See *Lujan v. Defenders of Wildlife*, 504 U.S. 555 (1992) (no standing), and *Friends of the Earth, Inc. v. Laidlaw Environmental Services, Inc.*, 528 U.S. 167 (2000) (standing).

[10] But for a very few exceptions, every federal environmental statute authorizes citizen suits. See Sections 304 and 307 of the Clean Air Act, 42 U.S.C. §§ 7604 (suits against violators of the Act) and 7607 (suits against the EPA); Section 505 of the Clean Water Act, 33 U.S.C. § 1365; Toxic Substances Control Act, 15 U.S.C. §§ 2618, 2619; Ocean Thermal Energy Conversion Act, 42 U.S.C. § 9124; Comprehensive Environmental Response, Compensation, and Liability Act, 42 U.S.C. § 9659; Section 105(g) of the Marine Protection, Research, and Sanctuaries Act, 33 U.S.C. § 1415(g); Section 12 of the Noise Control Act, 42 U.S.C. § 4911; Section 11(g) of the Endangered Species Act, 16 U.S.C. § 1540(g); Section 16 of the Deepwater Port Act, 33 U.S.C. § 1515; Section 7002 of the Resource Conservation and Recovery Act, 42 U.S.C. § 6972; Section 20 of the Toxic Substances Control Act, 15 U.S.C. § 2619; Section 1449 of the Safe Drinking Water Act, 42 U.S.C. § 300j-8; Section 520 of the Surface Mining Control and Reclamation

One key element: The process allows for attorneys' fees where "appropriate,"[11] which makes public interest litigation possible. For example, there are some organizations that fund their lawyers through attorneys' fees and play an important role in enforcing the Clean Water Act.

Injunctive relief only class actions

It may not represent a trend yet, but it is worth noting that some recent privacy and data security class actions have resulted in settlements imposing only injunctive relief (plus attorneys' fees). For example, in three cases consolidated under the caption *McDonald v. Kiloo A/S*, the Northern District of California approved an injunctive relief only settlement, finding that it would meaningfully change defendants' practices in ways that should improve privacy protections for children. "As one illustrative example, ... the settlements will 'place strict limitations on thousands of child-directed apps so that, at minimum, only contextual [*i.e.*, not behavioral] advertising is served to children under age 13."' McDonald v. Kiloo A/S, Case No. 17-cv-04344-JD; Case No. 17-cv-04419-JD; Case No. 17-cv-04492-JD, 2020 U.S. Dist. LEXIS 175865 (N.D. Cal. Sept. 24, 2020). While the settlements did not provide any monetary relief to class members, they did not release damages or other monetary claims for any class members or their children, except for the class representatives and their children, so that class members are free to pursue those claims against defendants in future actions.

Likewise, in *Adkins v. Facebook*, Case No. CV-18-05982 WHA (N.D. Cal. Nov. 15, 2020), the court approved a settlement imposing "a battery of security commitments to prevent future similar attacks." Compliance with these commitments will be assessed annually by an "unbiased, independent third-party vendor selected by Facebook," though with class counsel's approval. The results will be shared with the Court and an expert retained to verify compliance, but otherwise will remain confidential. "Given Facebook has already voluntarily implemented the security measures, this external oversight becomes the real value for the class."

Additionally, a preliminary order in *In Re Facebook Biometric Information Privacy Litigation*, No. 15-CV-03747-JD, Dkt. No. 456 (N.D. Cal. June 4, 2020), denied settlement approval because, inter alia, the settlement required no additional changes to Facebook's business practices and left unclear what specific changes Facebook would be making. The order re final approval, *In Re Facebook Biometric Information Privacy Litigation*, No. 15-CV-03747-JD, (N.D. Cal, Feb. 26,2021), noted several such changes in Facebook's policies including the company setting its "Face Recognition" default user setting to "off" for all users who have not affirmatively opted in or consented to biometric scans; deleting all existing and stored face templates for class members unless Facebook obtains a class member's express consent after a separate disclosure about how Facebook will use the face templates; and deleting the face templates of any class members who have had no activity on Facebook for three years.

Act of 1977, 30 U.S.C. § 1270; and Section 23 of the Outer Continental Shelf Lands Act, § 23, 43 U.S.C. § 1349(a).

[11] For example, the Clean Water Act provides, "The court, in issuing any final order in any action brought pursuant to this section, may award costs of litigation (including reasonable attorney and expert witness fees) to any prevailing or substantially prevailing party, whenever the court determines such award is appropriate." 33 U.S.C. § 1365(d).

8 | Enforcement and Remedies: An Options Matrix

To illustrate the discussion of remedies, we developed a set of questions that could be used to map the remedies landscape for any system of public policy rules, including privacy. The matrix or framework is informed by deterrence theory as applied in international relations.[1] (Thinking of remedies within a deterrence framework surfaces the idea of over-deterrence, a concern that may be under-represented in the privacy debate.) One purpose of the matrix is to show that the range of remedies options—the means to encourage good behavior and deter bad behavior—is not limited to punishment. Thus, the range of remedies also includes:

- cost imposition,
- cost internalization (a concept drawn from classic tort theory),
- denial of benefits,
- carrots or safe harbors that can be offered to regulated entities and that will compel them to act in a certain way and that can be taken away from them if they don't conform to the desired norm,
- transparency, which can incentivize good behavior as well as deter bad behavior,
- intermediaries or third parties, and
- enforcement agencies committed, and credibly signaling that they are committed, to enforcement

Remedies options can be thought of as controlled through a set of dials that can be tuned to achieve optimal outcomes. In this and in other ways, the matrix echoes classic deterrence theory from criminal law, which focuses on punishment and detection in a context where increasing one or the other or both can achieve the desired discouragement of criminal activity. For example, lower penalties but higher detection may serve as much of a deterrence role as higher penalties with lower detection. However, our main goal here is not to fine tune but rather to expand the scope of imaginable remedies and to tie them to policy goals. Dialing up or down on a particular remedy or enforcement mechanism may become easier (or less crucial) if the number and type of remedies and enforcement tools is expanded.

To illustrate application of the matrix, we applied it to a specific law, the Telephone Consumer Privacy Act. In some ways, the TCPA has been an effective statute. It highlights several key points with respect to remedies.

[1] See Michael J. Mazarr, *Understanding Deterrence*, RAND (2018) https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE295/RAND_PE295.pdf. There is also a form of deterrence theory in tort law.

The link between remedies and policy goals

The first of these points is that a system of remedies should be tied to policy goals: any assessment of remedies must consider whether they advance a policy goal.

Under some privacy laws, such as the TCPA, the policy goal is clear and fairly unitary. In the case of the TCPA, it is to eliminate unwanted telemarketing calls to consumers. So far, however, it is uncertain whether there is such a clear goal in the current debate over comprehensive federal privacy legislation. Is the purpose of privacy legislation to better implement the system of notice and choice, which is widely acknowledged to be inadequate? Is it to give individuals "control" over their information, through rights of access, correction, portability and deletion? Is it intended to prevent discrimination against protected classes or other harmful uses of data? Is it intended to fundamentally change the profiling-based, attention-capture business model of free online services? Are the goals the same for an offline business, an online store, and a social networking site?

As policymakers think about remedies, it is important to ask whether the policy goals have been identified. Not until policy goals have been identified is it possible to embrace and calibrate remedies.

The value of multiple types of remedies

Moreover, the application of our matrix to the TCPA suggests that it is likely that no one remedy can successfully promote even a fairly simple goal. The deterrence theory framework makes it easy to see just how complex and interdependent may be the remedies necessary to promote even a single policy goal (reducing unwanted telemarketing calls or texts to consumers). To achieve the goal of reducing unwanted telephone calls, the TCPA regime uses regulatory enforcement with monetary penalties (FCC); private right of action with injunctive relief, damages (including statutory damages) and attorneys' fees; safe harbors; and gatekeepers. All the more, a single remedy is unlikely to advance the multiple goals that comprehensive consumer privacy legislation may seek to achieve. Different policy goals may require different remedies.

The power of intermediaries

Another point that TCPA application of our deterrence framework illustrates is the role of intermediaries or other third parties who may be positioned to require regulated entities to respect the asserted policy norms. In the eco-system addressed by the TCPA, where the policy goal is to reduce marketing calls, junk texts and other unwanted communications, there are intermediaries that make telemarketing possible and that serve an enforcement role. These intermediaries will refuse to do business with companies violating the law because the intermediaries themselves face liability. There are many instances of intermediary liability being used to carry out policy goals. For example, it is illegal for publishers to publish discriminatory housing ads. The policy goal is to eliminate discrimination in residential housing. A more controversial form of intermediary enforcement is the role of ISPs in takedowns of copyright-infringing material. The privacy debate may benefit from a consideration of the role of intermediaries.

The remedies matrix: a framework for assessing remedies

Remedies framework: elements and questions	Applied Example: Telephone Consumer Protection Act (TCPA)
What are the highest-level policy goals of the regime?	
Policy goals	To reduce unwanted telemarketing, particularly to wireless phones, while allowing individuals to consent to advertising messages; to prevent abusive forms of calling; to protect certain kinds of callsystems, such as lines to emergency services and retirement homes
Deterrence: How does the regime seek to deter bad behavior? Options may include direct punishment (fines), redress of harms (compensation), denial of benefits (disgorgement of profits or other benefits), and cost imposition (e.g., a tax or fee).	
Direct punishment, such as fines paid to the government	FCC can pursue a "forfeiture penalty," calculated under a statutory formula (not based on illegal gain or profit)
Redress remedies to individuals (which may include restitution or other money damages)	Private right of action for "actual monetary loss" or liquidated damages of $500/call; triple damages for knowing violations
Denial of benefits (such as disgorgement of profits or data deletion)	Not available under TCPA. In other contexts, for instance, in most FTC cases, companies get to keep the data they (arguably) wrongfully acquired
Cost imposition (including taxes or fees)	Under the TCPA, there is no systematic and intentional cost imposition. In telemarketing more generally, however, all callers are required to pay a fee to the FTC to access the Do Not Call database.
Does the regime include a mechanism to hold the bad actors' assets at risk?	In some states, callers have to post a bond so that their assets can be seized quickly
Does the regime contemplate the problem of over-deterrence?	There are no mechanisms, such as ceilings on potential damages, in the statute, although some jurists have contemplated substantive due process limits on statutory damages
Is there a market for non-compliance?	Senders can take advantage of technical features of the telephone system that give them anonymity; subscribers have no real tools to quickly identify or complain about callers; overseas callers are not subject to deterrence mechanisms
Are attorney fees available to successful plaintiffs?	Yes
How does the regime seek to compel good behavior (carrots or sticks)?	
Preapprovals (permits, licenses)	None
Injunctive relief	If awarded by courts

Safe harbors	FCC defines multiple safe harbors that are treasured by industry, and that typically require documentation data collection to enjoy the liability shield, for instance, damages can be reduced in cases where the caller has implemented a documented system for reasonable compliance. In some states, callers have to post a bond so that their assets are held at risk by the regulator
Role of Gatekeepers and Third Parties	
Does the ecosystem for the sector/practice include gatekeepers (e.g., third party service providers) who regulate conduct?	Most advertisers use a third-party calling service to actually send messages. Most of these, like Twilio, hard code in TCPA requirements. Increasingly, insurance plays a role in compliance, as insurers have had to cover mega-fines for illegal calling
How does the regime address third parties who are involved in the underlying unwanted behavior?	Advertisers who hire telemarketers intending to break the law have vicarious liability
Other Issues	
How does the regime address the problem of guile?	Burden to show consent imposed on caller; lack of calling documentation results in loss of safe harbor
How does the regime address collective wrongs (small injuries to many people)?	Class action
How does the regime address power differentials among victims and wrongdoers?	Jurisdictional grant to state courts (small claims courts); class action
How does the regime respond to technological change?	FCC oversees the TCPA and has extended its definitions to address text messaging and advances in calling infrastructure. However, TCPA definitions tend to be highly technology-specific and it is not clear whether they address media convergence. The Supreme Court recently clipped the wings of the TCPA by visiting the definition of "autodialer" in *Facebook Inc. v. Duguid et al*, No. 19–511 (SCT 2021)
Regulatory Structures	
Is the regime complemented by an agency and what are that agency's powers?	FCC has broad powers to investigate, to update rules, and to punish wrongdoers. Some overlapping authority with FTC for Telemarketing Sales Rule
Monitoring or investigation?	Investigation

Overall Assessment of Efficacy	
Does the regime achieve desired policy outcomes?	Legitimate companies genuinely try to comply with the TCPA, and most use some kind of third-party, such as Twilio, that uses practices and procedures to encourage compliance. There are regular, 8-figure settlements in TCPA litigation against major brands that failed to comply. However, the regime does not deter swindlers and con artists. Some senders cannot be deterred because they are ideologically motivated (e.g., candidates and non-advertising issue messages). Weakening the TCPA is a major goal of the Chamber of Commerce. The whole regime may fall apart because of Congress' technology-specific definition of "autodialers." The Supreme Court, in April 2021, interpreted the definition of autodialers such that many forms of calling and text message marketing may now be legal even without consent. First amendment challenges could clip the regime.