A New Trend in Securities Fraud: Punishing People Who Do Bad Things

Joseph T. McClure*

Abstract

In the last few years, data privacy issues have taken center stage. The responsibility of corporations to safeguard personal user data has become a mainstream political issue in the wake of the 2016 presidential election. Social media giants have been repeatedly hauled in front of Congress to explain how the consumer data they have been charged with protecting has ended up in the public domain. But absent a regulatory scheme to punish irresponsibility and encourage vigilance, public floggings in various Congressional hearings is the only major consequence for this conduct. However, because many of these companies are public, the Securities and Exchange Commission, the Department of Justice, and private shareholders all have used federal securities law as a means of recourse when these companies have attempted to hide data breaches or other misconduct. But, as the author notes, this strategy is not limited to data privacy issues, and although the author devotes most of this article to enforcement actions against Facebook, the parallel to many other industries is obvious.

This article seeks to articulate a distinct view of federal securities law as it is increasingly used in non-traditional enforcement actions commenced to punish corporate bad behavior. This paper argues that these non-traditional enforcement mechanisms should be viewed with skepticism. This skepticism should not be misinterpreted as cynicism, as the author believes that these non-traditional enforcement actions are beneficial vehicles to accomplish the admirable governmental objective of "punishing people who do bad things." However, the author recognizes that such use of securities law does not fall into a category of clearly defined criminal law and carries a significant risk of abuse. The author also recognizes the "admirable governmental objective" may be thwarted when it comes to private companies. Finally, the author is uneasy with the societal values conveyed when the government sanctions corporate misbehavior in the name of protecting shareholders from deception.

I. Introduction

What is "securities fraud?" After examining the recent body of investigations and enforcement actions, a cynical (and somewhat facetious) answer could be that everything is securities fraud. Putting aside for a moment the precise legal definition, a slightly more descriptive and straightforward definition is, securities fraud is a convenient and effective, yet imperfect, vehicle for holding public companies accountable for bad behavior. Notable recent investigations and enforcement actions have included opioid manufacturers,[1] data breaches at Target,[2] corporate executives who accepted bribes from or paid bribes to foreign governments,[3] iPhones with slowed performance,[4] climate change skepticism,[5] gun violence,[6] workplace sexual misconduct,[7] and data misuse that enabled manipulation of public opinion leading to a United States presidential election.[8] Without more information, there is no common thread which runs through these actions that were commenced under the premise of enforcing securities law, other than they all seem like instances of people who have done bad things involving very salient issues in public discourse. Yet, the Department of Justice, the Securities and Exchange Commission, private party shareholders, or some combination of the three have determined that in some technical sense, they are all instances of securities fraud.

---

*J.D. Candidate, University of Kentucky College of Law (2019); B.S., University of Kentucky Gatton School of Business & Economics (2016).

[1] Kevin LaCroix, *Securities Suits Hit Opioid Drug Companies*, THE D&O DIARY, (Sept. 5, 2017), https://www.dandodiary.com/2017/09/articles/securities-litigation/securities-suits-hit-opioid-drug-companies.

[2] Dave Michaels, *SEC Chief Wants Investors to Better Understand Cyberrisk*, WALL ST. J (Sept. 6, 2017), https://www.wsj.com/articles/sec-chief-wants-investors-to-better-understand-cyberrisk.

[3] Chad Bray, *Petrobras of Brazil to Pay $2.95 Billion Over Corruption Scandal*, N.Y. TIMES (Jan. 3, 2018), https://www.nytimes.com/2018/01/03/business/dealbook/brazil-petrobras-corruption-scandal.html; Tom Schoenberg, *Michael Cohen, Once of Och-Ziff, Charged With Fraud by U.S.*, Bloomberg Business (Jan. 3, 2018, 4:46 PM), https://www.bloomberg.com/news/articles/2018-01-03/michael-cohen-ex-och-ziff-executive-charged-with-fraud-by-u-s.

[4] Tom Schoenberg, *U.S. Probes Apple Over Updates That Slow Older iPhones*, BLOOMBERG TECHNOLOGY (Jan. 31, 2018, 11:23 AM), https://www.bloomberg.com/news/articles/2018-01-30/u-s-said-to-probe-apple-over-updates-that-slow-older-iphones-jd1yahj7.

[5] Matt Levine, *Coal, Drugs and Lawsuits*, BLOOMBERG VIEW: MONEY STUFF (Nov. 10, 2015, 8:34 AM), https://www.bloomberg.com/view/articles/2015-11-10/coal-drugs-and-lawsuits.

[6] Matt Levine, Rogue Trading and Gun Disclosure, BLOOMBERG VIEW: MONEY STUFF (March 23, 2016, 8:51 AM), https://www.bloomberg.com/view/articles/2016-03-23/rogue-trading-and-gun-disclosure.

[7] Meg James, *CBS hit with shareholder lawsuit over CEO Leslie Moonves' alleged sexual misconduct*, L.A. Times (Aug. 28, 2017, 12:50 PM), http://www.latimes.com/business/hollywood/la-fi-ct-cbs-moonves-shareholder-lawsuit-20180827-story.html.

[8] Matt Levine, *Facebook's Shareholders Are Disappointed*, BLOOMBERG VIEW: MONEY STUFF (March 21, 2018, 10:18 AM), https://www.bloomberg.com/view/articles/2018-03-21/facebook-s-shareholders-are-disappointed.

Matt Levine recently posed an extreme hypothetical[9] that is illustrative of the potential absurdity: Suppose a public company sold a phone that it secretly knew would explode in exactly one year, and millions of people purchased this phone. In one year, millions of people would certainly be killed, and the stock price would certainly sink sharply. The Department of Justice might investigate and (rightly) determine that the company had committed securities fraud. In making that determination, the DOJ would be reaching a judgment that the company had done something bad, but also, that those harmed were *the shareholders of the company*. After all, under federal securities law, shareholders should have been informed the company was making a product it knew would eventually cause widespread harm to consumers, and shareholders should have been given the opportunity to sell their stock before the explosions to prevent loss in share value. If one were to describe the conduct underlying the various investigations and enforcement actions previously mentioned, a lay audience with a general awareness of securities law would likely be deeply confused that the explanation concluded with “and that is why Company X has committed securities fraud.” The audience would not be unjustified in their bewilderment. In some sense, it would not be shocking to find out that these companies or their executives were in *some* kind of legal trouble. After all, each of the aforementioned scenarios involve conduct which is either dishonest, distasteful, or at the very least, inconvenient to those who interact with the company on the consumer level. A Target shopper or an iPhone user may even be delighted that someone is being

[9] Matt Levine, *Sergeant Spoof's Time Has Passed: Also Insider Trading, Securities Fraud, Merger Appraisal, Crypto and Dimon 2024*, BLOOMBERG VIEW: MONEY STUFF (Jan. 31, 2018, 9:46 AM), https://www.bloomberg.com/view/articles/2018-01-31/sergeant-spoof-s-time-has-passed; Matt Levine is a Bloomberg columnist who writes a blog called “Money Stuff.” He has frequently written about the ideas explored in this article, and the genesis of this piece is based on some of his writing.

held responsible for being careless with his data or for slowing down her smartphone. Viewed from this perspective, a reasonable interpretation of federal securities law is that those laws are a convenient way for the government (or shareholders) to punish companies who do things that the market has determined are "bad." On the other hand, with the benefit of a more nuanced analysis, a reasonable person could conclude that while convenient, punishing bad behavior using securities law requires making certain judgments about the identity of the victims, and the selection of those to be compensated for that bad behavior. Such conclusions may depart from conventional understanding or moral sensibility.

This article seeks to articulate a distinct view of federal securities law as it is increasingly used in non-traditional enforcement actions to punish corporate bad behavior. This paper argues that these non-traditional enforcement mechanisms should be viewed with skepticism. This skepticism should not be misinterpreted as cynicism, as the author believes that these non-traditional enforcement actions are beneficial vehicles to accomplish the admirable governmental objective of "punishing people who do bad things." However, the author recognizes that such use of securities law does not fall into a category of clearly defined criminal law and carries a significant risk of abuse. The author also recognizes the "admirable governmental objective" may be thwarted when it comes to private companies. Finally, the author is uneasy with the societal values conveyed when the government sanctions corporate misbehavior in the name of protecting shareholders from deception. Part II provides a foundation by briefly explaining the relevant basics of corporate structure that convey liability on companies for the conduct of their executives, and builds on that foundation with a short explanation of the technical definition of securities fraud under the 1934 Securities Exchange Act and an abridged journey through traditional cases of securities fraud in the last thirty years. Part III discusses the phenomenon already introduced: the evolving theory of liability in contemporary securities fraud enforcement. Finally, Part IV seeks to evaluate both the positives and pitfalls of adopting this policy of enforcement. The author ultimately concludes that the policy is good, but not unmitigatedly so, and warrants constant scrutiny to avoid abuse.

II. Background

To adequately understand how and why corporate officers may be responsible (or liable) for the conduct of the companies they manage, some background is necessary. Corporate law is premised on the idea that corporations operate to generate profit for their shareholders; thus, all officers have a duty to devote their best efforts to provide that benefit to the shareholders. Part of their duty is ensuring compliance with federal securities law, which imposes disclosure requirements on the company to ensure shareholders are fully apprised of the information necessary to make informed investment decisions.

A. Fundamentals of American Corporate Structure

Corporations occupy a strange space in the American legal system. For some purposes, corporations are collections of people; for other purposes, corporations *are* legally people.[10] The owners, known as shareholders, provide a capital investment in return for an equity interest in the business venture. Shareholders largely have no direct control over the corporation but conduct general oversight through the election of a board

[10] *See* David Ciepley, *Beyond Public and Private: Toward a Political Theory of the Corporation*, 107 AM. POL. SCI. REV. 139, 139–41 (2013).

of directors.[11] The board of directors then makes recruitment and hiring decisions with regard to corporate officers.[12] Top officers, such as the Chief Executive Officer, ("CEO"), the Chief Financial Officer ("CFO"), and the Chief Operating Officer ("COO"), are the people most often associated with the company's public persona.[13] The officers hire the managers, and the managers hire the employees.[14] In this structure, the investor is largely separated from the day-to-day operation and management of the business; those responsibilities are delegated to the officers, managers, and employees.[15] However, because of this separation of ownership and control, the officers owe various duties to the shareholders, including a duty to share information and a duty to operate the company for the benefit of the shareholders.[16] After all, the corporation functions primarily on the shareholders' capital investment.

Most notably, shareholders are owed duties of care and loyalty by the officers and managers.[17] Corporations are run for the benefit of their owners, and as discussed *supra*, the officers, managers, and employees ultimately work for the shareholders. Thus, the officers have an obligation to work to accomplish the objectives of the shareholders, and any deviation from that obligation is a breach of duty that is legally actionable.[18] Prevailing economic and corporate theory suggest that no matter what each individual shareholder's aims may be, all shareholder interests in the business investment are united

---

[11] FRANK H. EASTERBROOK & DANIEL R. FISCHEL, THE ECONOMIC STRUCTURE OF CORPORATE LAW 1-4 (1991).
[12] *Id*.
[13] *See* E. Geoffrey Love, Jaegoo Lim, & Michael K. Bednar, *The Face of the Firm: The Influence of CEOs on Corporate Reputation*, 60 ACAD. MGMT. J. 1462, 1462–81 (2017).
[14] Easterbrook and Fischel, *supra* note 11.
[15] *Id*.
[16] *See* Victor Brudney, *Contract and Fiduciary Duty in Corporate Law*, 38 B.C.L. REV. 595 (1997).
[17] *Id*.
[18] *Id*.

around one single objective: to generate profit.[19] This is a simplified explanation of the shareholder value theory, which essentially suggests that because the shareholders' sole objective is profit, the agents of the corporation (officers, managers, etc.) have a duty to do their best to accomplish that objective, putting aside other considerations.[20] When an officer or manager takes a course of action that deviates from that objective, she is acting to benefit her own personal or social responsibilities, and is not acting on behalf of the corporation.[21] The time and money she spends on accomplishing that objective is her own.[22] If the divergent action taken by the officer or manager causes the company to lose money, that officer or director is responsible to the shareholders for that loss.

B. Securities Fraud

Corporations are primarily animals of state law, but due to the realities of nationwide investment through the sale of securities, they are also subject to federal law.[23] This leads to a patchwork of legal framework to which corporations must adhere. The primary focus of this article is the function of the federal portion of that framework.

Among other functions, the Securities Exchange Act of 1934 created the Securities and Exchange Commission with rulemaking authority; the Commission uses this authority to regulate the dissemination of information to the public.[24] Section 13(a) of the Exchange Act requires all publicly traded securities listed on a national exchange to file and update periodic reports with the SEC as well as other "information and

---

[19] Milton Freidman, *The Social Responsibility of Business is to Increase its Profits*, N.Y. TIMES MAGAZINE (Sept. 13, 1970). *But see* Ciepley, *supra* note 10.
[20] *Id*.
[21] *Id*.
[22] *Id*.
[23] *See*, *e.g.*, Securities Act of 1933, 15 USCS §§ 77a et seq. (2018); Securities Exchange Act of 1934, 15 U.S.C. § 78a et seq. (2018).
[24] 15 U.S.C. § 78 et seq.

documents as the [SEC] shall require."[25] Regulation S–K contains more specific guidance as to other "information and documents" the SEC requires and imposes mandatory disclosure and reporting requirements.[26] Of particular interest, Item 303 requires corporations to include in their financial statements a section known as "Management's Discussion and Analysis" or "MD&A."[27] Item 303 broadly mandates that this section include a discussion of "any known trends or uncertainties that have had or the registrant reasonably expects will have a material favorable or unfavorable impact on net sales or revenues or income from continuing operations."[28]

Section 10(b) of the Exchange Act makes it unlawful "[t]o use or employ, in connection with the purchase or sale of any security registered on a national securities exchange or any security not so registered . . . any manipulative or deceptive device or contrivance in contravention of such rules and regulations as the Commission may prescribe as necessary or appropriate in the public interest or for the protection of investors."[29] In other words, corporations are not allowed to make false or misleading statements that investors may rely on in making decisions to purchase or sell securities.[30] This statute is given its effect by Rule 10b–5 which creates a Section 10(b) violation to "make any untrue statement of a material fact or to omit to state a material fact necessary in order to make the statements made . . . not misleading."[31] A "material fact" is any fact that "would have assumed actual significance in the deliberations of the reasonable

[25] 15 U.S.C. § 78m (2018).
[26] 17 C.F.R. § 229 et seq.
[27] 17 C.F.R. § 229.303.
[28] *Id*.
[29] 15 U.S.C. § 78j (2018).
[30] *Id*.
[31] 17 C.F.R. § 240.10b-5.

shareholder."[32] Viewed in context with Regulation S–K, corporations have an obligation to be truthful in their required disclosures and any other disclosures they make voluntarily, and if circumstances arise that make a previous statement untrue, the corporation has an affirmative duty to issue a correction or clarification of that statement.[33] As a technical matter, corporations, as legally fictional entities, are incapable of committing fraud because they are not persons, so when the officers acting on behalf of the company commit the fraud, that improper action is attributed to the company.[34] To that end, the Supreme Court has recognized both a public and a private right of action under Rule 10b–5 against both the corporation and the corporate officer who violate the rule.[35]

As part of the normal course of running a business, the corporation (through its officers) constantly makes public statements and releases other less formal information with regard to its business ventures. Naturally, investors use each of these bits of information to make a decision whether to buy or sell the securities offered by that corporation, so much so that each small piece of information becomes compounded into the price of the security.[36] Because of this inherent reliance, all disclosures must be truthful and complete, and any false or misleading statements must be corrected.[37] According to former enforcement official John Reed Stark, the founder of the SEC's

[32] TSC Indus., Inc. v. Northway, Inc., 426 U.S. 438, 449 (1976).
[33] In re Time Warner Inc. Sec. Litig., 9 F.3d 259, 267 (2nd Cir. 1993) (if prior statements become untrue "as the result of intervening events," a duty to correct or update may arise); City of Edinburgh Council v. Pfizer, Inc., 754 F.3d 159, 176 (3rd Cir. 2014) (duty to update when "subsequent events produce an extreme or radical change in the continuing validity of the original statement").
[34] Stephen Choi and Adam Pritchard, *SEC Investigations and Securities Class Actions: An Empirical Comparison*, 13 J. EMPIRICAL LEGAL STUD. (Issue 1) 27–49 (2016).
[35] Stoneridge Inv. Partners, LLC v. Scientific-Atlanta, Inc., 552 U.S. 148, 165 (2008).
[36] Basic, Inc. v. Levinson, 485 U.S. 224, 241–42 (1988) (explaining the "fraud on the market" theory for public securities).
[37] *Id*.

Office of Internet Enforcement, "Wherever you are talking, you are talking to investors. There is no place where you have immunity. . . . When you're a public company official, you have to be careful at all times."[38] Any omission can later become a false or misleading statement when other statements do not correct the omission because investors or potential investors rely on the fact that a disclosure is complete, so any new undisclosed information which makes a previous statement something less than fully truthful is a misstatement.[39]

Traditional Section 10 securities fraud cases involve either a voluntary or mandatory disclosure that turns out to be untrue or misleading if it induces investors to buy or sell. These investors can lose money because of the decision they made based on the misleading information. Although a violation of Section 10 is not the only way to commit securities fraud, Section 10 (along with Rule 10b–5) creates the most common and generic form of securities fraud under federal law. Therefore, this note will refer to violations of those provisions simply as "securities fraud."

The most famous cases of securities fraud in the last 30 years have centered on this basic framework. One such example is WorldCom. Near the end of the 1990s, the telecommunications industry began to decline.[40] In 1999, WorldCom began inflating earnings from its telecommunications operations to meet aggressive growth goals the corporation had set for itself.[41] Instead of disclosing WorldCom's failures to meet

---

[38] Renae Merle and Elizabeth Dwoskin, *How the SEC could target Facebook*, WASH. POST BLOGS (July 3, 2018 9:45 PM), https://www.washingtonpost.com/news/business/wp/2018/07/03/how-the-sec-could-target-facebook/.
[39] In re Time Warner Inc. Sec. Litig., 9 F.3d at 267.
[40] Ken Belson, *WorldCom Chief Is Given 25 Years for Huge Fraud*, N.Y. TIMES (June 14, 2005), https://www.nytimes.com/2005/07/14/business/worldcom-chief-is-given-25-years-for-huge-fraud.html.
[41] Barnaby J. Feder and Kurt Eichenwald, *Corporate Conduct: The Overview; Ex-WorldCom Chief Is Indicted by U.S. In Securities Fraud*, N.Y. TIMES (March 3, 2004),

performance goals, CEO Bernard Ebbers directed the preparers of WorldCom's financial statements to use non-GAAP accounting methods to manipulate and exaggerate the corporation's earnings,[42] thereby artificially inflating the price of its stock.[43] After investigations, the SEC and DOJ pursued civil and criminal enforcement actions against Ebbers and other WorldCom executives.[44] The indictment of Ebbers alleges his statements made on behalf of the corporation "falsely described WorldCom's true operating performance and financial condition, and omitted to disclose facts necessary to make those statements complete, accurate, and not misleading" in violation of Rule 10b–5.[45] Ebbers was eventually tried, convicted, and sentenced to 25 years in prison on nine counts relating to securities fraud.[46]

In the early 2000s, the scandal involving Enron Corporation rocked the financial world and permeated into popular culture.[47] By capitalizing on favorable natural resources regulations of the time, Enron was recognized as the most innovative company in the year 2000 by *Fortune* magazine's "Most Admired Company" survey.[48] Less than a year later, following multiple SEC and DOJ investigations and enforcement actions, Enron was left disgraced and essentially worthless.[49] The target of the investigation and

---

https://www.nytimes.com/2004/03/03/business/corporate-conduct-overview-ex-worldcom-chief-indicted-us-securities-fraud.html.

[42] *Id*.

[43] Belson, *supra* note 40.

[44] Press Release, U.S. Dept. of Justice, U.S. Charges Ex-WorldCom CEO Bernard Ebbers (March 24, 2004), https://web.archive.org/web/20060809122629/http://www.fbi.gov/dojpressrel/pressrel04/world030204.htm; Litigation Release No. 19301, Securities and Exchange Commission, SEC Files Civil Fraud Action Against Bernard J. Ebbers, WorldCom's Former Chief Executive Officer (July 13, 2005), https://www.sec.gov/litigation/litreleases/lr19301.htm.

[45] Indictment ¶34, United States v. Ebbers, (No. S3-02-Cr.-1144) 2004 WL 1263386 (S.D.N.Y. 2004).

[46] Belson, *supra* note 40.

[47] Paul M. Healy and Krishna G. Palepu, *The Fall of Enron*, 17 J. ECON. PERSP. 3 (2003).

[48] *Id*.

[49] *Id*.

prosecution was Jeffrey Skilling, President, CEO, and COO of Enron.[50] Skilling was tried and convicted on twelve counts of securities fraud, including violations of Section 13(a) and Rule 10b–5.[51] The SEC Complaint alleged, *inter alia*, that Skilling made false or misleading statements to promote a new Enron product at an analyst conference in order to manufacture earnings and thereby boost Enron's stock price.[52] The Complaint further alleged that Skilling filed false or misleading financial statements with the SEC as part of the corporation's federally required reports.[53] Skilling was convicted by a jury and ultimately sentenced to 168 months in federal prison.[54]

In the 1960s, Bernie Madoff founded Bernie Madoff Investment Securities ("BMIS").[55] Sometime during the 1980s, BMIS ceased operating as a legitimate investment company, and in December of 2008, Madoff confessed to two senior BMIS employees, "It's all just one big lie." He further acknowledged that BMIS was ". . . basically, a giant Ponzi scheme."[56] In November of 2008, BMIS reported managing over

---

[50] Litigation Release No. 23422, Securities and Exchange Commission, Court Grants Summary Judgment To Conclude Civil Case Against Former Enron CEO (Dec. 8 2015), https://www.sec.gov/litigation/litreleases/2015/lr23422.htm.

[51] Complaint ¶67–69, SEC v. Skilling et al., No. H-04-0284 (S.D. Tex. 2004), https://www.sec.gov/litigation/complaints/comp18582.htm; DOJ Skilling Indictment, U.S. v. Skilling, (Cr. No. H-04-25 (S-2)) 2004 WL 1553217 (S.D. Tex.) (July 7, 2004); Alexei Barrionuevo, *Enron Chiefs Guilty of Fraud and Conspiracy*, N.Y. TIMES (May 25, 2006), https://www.nytimes.com/2006/05/25/business/25cnd-enron.html.

[52] Press Release 2004-18, U.S. Securities and Exchange Commission, SEC Charges Jeffrey K. Skilling, Enron's Former President, Chief Executive Officer and Chief Operating Officer, With Fraud (Feb. 19, 2004), https://www.sec.gov/news/press/2004-18.htm; DOJ Skilling Indictment, *supra* note 51 (the indictment echoes these allegations made by the SEC).

[53] Press Release 2004-18, *supra* note 52.

[54] Press Release, U.S. Dept. of Justice, Former Enron CEO Jeffrey Skilling Resentenced to 168 Months for Fraud, Conspiracy Charges (June 21, 2013), https://www.justice.gov/opa/pr/former-enron-ceo-jeffrey-skilling-resentenced-168-months-fraud-conspiracy-charges; Enron CFO Andy Fastow and Enron Founder/Board Chairman Kenneth Lay were also convicted of the fraud. Fastow was sentenced to six years in prison plus two additional years of court-supervised home confinement. Lay died of a heart attack before sentencing. Kate Murphy and Alexei Barrionuevo, *Fastow Sentenced to 6 Years*, N.Y. TIMES (Sept. 27, 2006), https://www.nytimes.com/2006/09/27/business/27enron.html.

[55] Complaint at ¶12, SEC v. Madoff, 08-CIV-10791 (S.D.N.Y. Dec. 11, 2008).

[56] Complaint at ¶23, *supra* note 55.

$64.8 billion in client assets.[57] At the time of his confession, Madoff stated the business was insolvent with estimated losses of approximately $50 billion.[58] The SEC charged Madoff (and BMIS) with violations of Section 10(b) of the Exchange Act and Rule 10b–5, in addition to violations of other securities laws.[59] On March 12, 2009, Madoff pleaded guilty to a Criminal Information that outlined various violations of securities law, including Section 10(b) and Rule 10b–5, based on Madoff's fraudulent filings with the SEC and his communications with clients and prospective clients.[60] Madoff was later sentenced to 150 years in federal prison.[61]

The common thread of these major enforcement actions is that it makes some intuitive sense that these are violations of securities law. In each case, the offending company or officers did something for the purpose of affecting the financial analysis and investment decisions of their shareholders or potential investors; the crimes were *financial* in nature. The underlying facts in these instances are somewhat complicated in terms of violating securities laws that involved the offender performing some sort of accounting gimmick or moving numbers around, followed by false or misleading representations about the accuracy of the books. Of course, this is what most people would expect out of a securities fraud case. They accept not understanding the exact transactions that comprise the elements of the crime, but they assume the violation concerns fraud in the numbers or the financial statements.

[57] Sentencing Memo at *5, United States v. Madoff, 09-CR-213, (S.D.N.Y. June 26, 2009).
[58] Complaint at ¶23, *supra* note 55.
[59] Complaint at ¶36–39, *supra* note 55.
[60] Criminal Information, United States, v. Madoff, No. 09-CR-213, 2009 WL 772903 (S.D.N.Y. Mar. 10, 2009).
[61]Sentencing Hearing Transcript at *49, United States v. Madoff, 09-CR-213, (S.D.N.Y. June 29, 2009).

This stands in stark contrast to some of the more recent major investigations and enforcement actions. The government has found a new use for federal securities law, employing it where the underlying conduct is both intuitively bad and easy for any lay person to understand. Instead of simply "cooking the books," the underlying bad act is a data breach, or a faulty product, or a sexual assault allegation. The criminal liability flows from not telling the shareholders and conducting business as if the stock price accurately reflects the absence of any skeletons in the company closet. This marks a new trend in securities fraud: punishing people who do bad things beyond just faulty accounting practices or distorted financial records.

III. The Emerging Theory of Liability in Current Securities Fraud Enforcement

As discussed briefly in Part II (B), securities fraud has traditionally been employed to penalize *financial* crimes. Recently, however, there has been a noticeable interest in chastising other conduct that is not inherently a crime of a *financial* nature. The underlying bad behavior might not be technically illegal, but we know it is bad because the value of the company drops when the public finds out about that behavior.[62] As a result, the open market becomes the judge of what is bad and what is good and accordingly adjusts the stock price to reflect public judgments.[63] The government, or even private parties, can then use the all-purpose tool of securities fraud to impose penalties on the company for misconduct. However, the company is only penalized when it fails to admit the mistakes at the time the officers realize the mistakes. As Matt Levine explains, "If a company does a bad thing—or even has a bad thing done to it—and doesn't contemporaneously disclose it, and if the market eventually finds out and the

[62] Levine, *supra* note 8.
[63] *Id*.

stock drops, then the act of keeping it secret initially was securities fraud. Companies are supposed to tell their shareholders about material news, so that the shareholders can make informed trading decisions."[64]

A prime example of this emerging phenomenon is Facebook. In March 2018, a series of articles in the *New York Times* and other publications revealed that Facebook had allowed a data firm named Cambridge Analytica to harvest user data without permission from more than 50 million user profiles (later estimated to be as many as 87 million users)[65] for controversial use by a campaign during the 2016 United States presidential election.[66] Although there were credible reports of egregious Facebook data misuse as early as March 2017,[67] Facebook vaguely denied or otherwise refused to acknowledge any issues until March 16, 2018, when the company published a press release after the close of the Friday trading session.[68] Among the myriad of problems Facebook faced following this revelation was its failure to disclose this issue to its shareholders prior to the March 16th press release. As early as 2015, the company was aware that "information had been harvested on an unprecedented scale" yet the company

---

[64] Matt Levine, *Google Is Big and Google+ Was Small*, BLOOMBERG VIEW: MONEY STUFF (Oct. 9, 2018, 11:14 AM), https://www.bloomberg.com/view/articles/2018-10-09/google-is-big-and-google-was-small.

[65] Georgia Wells, *Facebook Reveals Apps, Others That Got Special Access to User Data*, WALL ST. J. (July 1, 2018), https://www.wsj.com/articles/facebook-reveals-apps-others-that-got-special-access-to-user-data-1530454712.

[66] Matthew Rosenberg, Nicholas Confessore & Carole Cadwalladr, *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. TIMES, (Mar. 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

[67] Mattathias Schwartz, *Facebook Failed to Protect 30 Million Users From Having Their Data Harvested by Trump Campaign Affiliate*, THE INTERCEPT, (March 30, 2017, 2:01 PM), https://theintercept.com/2017/03/30/facebook-failed-to-protect-30-million-users-from-having-their-data-harvested-by-trump-campaign-affiliate.

[68] Press Release, Facebook, Suspending Cambridge Analytica and SCL Group From Facebook (Mar. 16, 2018), https://newsroom.fb.com/news/2018/03/suspending-cambridge-analytica/.

did little to protect users or address the issue.[69] In August 2016, Facebook officers verified the breach[70] and sought to contain it by reaching out to Cambridge Analytica.[71] The reporting from the *New York Times* and others detailing the nature of the breach and the failure of Facebook to disclose it to its users (or shareholders) sparked a firestorm of public outrage. Debate quickly turned to the propriety of Facebook's conduct both in allowing Cambridge Analytica to violate the company's policies and in the decision not to disclose the violations to its users (and shareholders). In the ten days following the March 16 press release, shares of Facebook plunged almost 20% in response to the disclosure and the ensuing public debate.[72] Anecdotally, the market recognized that Facebook had done something bad, and the company lost roughly $80 billion in market value to mark this recognition.[73]

Even before the sell-off concluded, a group of Facebook shareholders filed suit in San Francisco, alleging securities fraud (among other claims) under Rule 10b-5.[74] By July 2018, multiple federal agencies had taken interest in Facebook's conduct from various angles. By July 2, 2018, the Department of Justice, the FBI, the SEC, and the Federal Trade Commission (FTC) were each conducting probes into Facebook regarding

---

[69] Carole Cadwalladr and Emma Graham-Harrison, *Revealed: 50 million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach*, THE GUARDIAN (Mar. 17, 2018), https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.
[70] Facebook maintains that data was "misused" in violation of its policies rather than admitting the company suffered a "data breach." Whatever the factual and technical differences may be, the author uses the term "breach" when discussing all events related to Cambridge Analytica's use of Facebook data because the distinctions are only semantical to this article. *See* Elizabeth Dwoskin & Tony Romm, *Facebook's Rules for Accessing User Data Lured More Than Just Cambridge Analytica*, WASH. POST (March 19, 2018), https://www.washingtonpost.com/business/economy/facebooks-rules-for-accessing-user-data-lured-more-than-just-cambridge-analytica/2018/03/19/.
[71] Rosenberg, *supra* note 66.
[72] Paul R. La Monica, *Facebook has Lost $80 Billion in Market Value Since its Data Scandal*, CNN Money (March 27, 2018), https://money.cnn.com/2018/03/27/news/companies/facebook-stock-zuckerberg/index.html.
[73] *Id*.
[74] Complaint, Yuan v. Facebook Inc., 3:18-cv-01725, 2018 WL 1400036 (S.D. Cal., Mar. 20, 2018).

the company's failure to appropriately manage its consumers' data.[75] At the core of each probe was essentially one question: Why didn't Facebook disclose the breach to its users and investors?[76]

The FTC took particular interest in whether Facebook violated a 2012 settlement which required the company to give its users "clear and prominent notice and obtain their express consent before sharing their information beyond their privacy settings."[77] In light of the aforementioned duties requiring public companies to disclose material facts to its shareholders,[78] the SEC was interested in which executives knew what about the breach when they made various statements, ultimately bringing charges "for making misleading disclosures regarding the risk of misuse of Facebook user data."[79] Working from the day Facebook officials became aware of the 2015 breach, SEC officials reviewed Facebook's financial statements for their MD&A of business risks, specifically the risk of data breaches, as well as any public statements Facebook officers made to the media or to Congress.[80]

Following the *New York Times* story, the value of Facebook dropped substantially, as was reflected in its share price. The financial market recognized

---

[75] Craig Timberg, Elizabeth Dwoskin, Matt Zapotosky & Devlin Barrett, *Facebook's Disclosures Under Scrutiny as Federal Agencies Join Probe of Tech Giant's Role in Sharing Data with Cambridge Analytica*, WASH. POST (July 2, 2018), https://www.washingtonpost.com/technology/2018/07/02/federal-investigators-broaden-focus-facebooks-role-sharing-data-with-cambridge-analytica-examining-statements-tech-giant.
[76] Timberg, *supra* note 75.
[77] Wells, *supra* note 65.
[78] See Part II(B), *supra* note 23–61 and accompanying text.
[79] Press Release 2019-140, U.S. Securities and Exchange Commission, Facebook to Pay $100 Million for Misleading Investors About the Risks It Faced From Misuse of User Data (July 24, 2019), https://www.sec.gov/news/press-release/2019-140.
[80] In the first 10-K filed after knowledge of the breach (2016), Facebook's MD&A included: "Security breaches and improper access to or disclosure of our data or user data, or other hacking and phishing attacks on our systems, *could* harm our reputation and adversely affect our business" (emphasis added). This clause was also included in Facebook's subsequent quarterly reports.

Facebook's conduct was bad, but it was not clearly criminal, or even *obviously* a violation of securities law. The sell-off was likely influenced, at least in part, by the negative publicity the company would endure and the embarrassment of the inevitable congressional hearings and media coverage in response to the breach. Facebook's failure to keep data safe did not itself make the company less valuable in terms of assets and revenues, but the breach lessened Facebook's value in the eyes of the public at large, or rather the market at large. The financial market punished Facebook for conduct the public considered reprehensible, and thus punished Facebook's shareholders. But in the absence of disclosure, the shareholders were not in a position to know about the data breach; that was the officers' responsibility. In not disclosing the data breach to allow shareholders to make informed investment decisions, the officers likely abandoned their legal duties to the shareholders. This abdication allows the shareholders to pursue legal action against the officers to recoup their losses. Thus, under federal securities law, the parties responsible for the loss in company value are the officers, and courts could enter a judgment against them for this financial damage.[81] In fact, Facebook has already reached a settlement agreement with the SEC in which it has agreed to pay a $100 million penalty and submit itself to an injunction "permanently enjoining it from violating Sections 17(a)(2) and 17(a)(3) of the Securities Act of 1933 and Section 13(a) of the Securities Exchange Act of 1934, and Rules 12b-20, 13a-1, 13a-13, and 13a-15(a) thereunder."[82]

But whatever pecuniary harm Facebook's lack of care or disclosure caused its shareholders, the injury inflicted on Facebook users and arguably, on American

---

[81] *See*, *e.g.*, Matrixx Initiatives, Inc. v. Siracusano, 563 U.S. 27 (2011).
[82] Press Release 2019-140, *supra* note 79.

democracy, is much more salient. Darren Robbins, a prominent securities law attorney[83] remarked, "[Facebook has] potential culpability in a number of areas . . . whether liability from users, government regulators, or investors follows, there are implications for our society given the unique position Facebook occupies in the daily lives of Americans."[84] Thus, securities law may ultimately provide the best instrument to reprimand this sort of conduct. The actual detriment that Facebook users suffered through Cambridge Analytica's use of their data is uncertain, and the argument regarding the damage the data misuse did to American society is more political than legal. But the shareholders definitely suffered a concrete and provable harm. To put it simply, "Facebook's shareholders were definitely . . . victims of all of this: They bought the stock at a high price not knowing about the Cambridge Analytica breach, and then when they found out about it the stock price fell, and they lost money."[85] That harm is a violation of federal securities law that is both simple to prove and easy to measure.

Facebook's fate is not without precedent. In late 2014, Yahoo learned Russian hackers had successfully stolen user names, email addresses, birthdates, telephone numbers, and various other personal data from 500 million users, but failed to disclose the breach until 2016.[86] The SEC investigated, and fined Yahoo $35 million.[87] In the agreed settlement order, the SEC found that Yahoo's financial statements, specifically its

[83] Darren J. Robbins, *Robbins Geller Rudman & Dowd LLP*, https://www.rgrdlaw.com/attorneys-Darren-J-Robbins.html.
[84] Christie Smythe and Kartikay Mehrotra, *Facebook Sued by Investors Over Voter-Profile Harvesting*, BLOOMBERG TECHNOLOGY (March 20, 2018, 5:10 PM), https://www.bloomberg.com/news/articles/2018-03-20/facebook-sued-by-investors-over-voter-profile-harvesting.
[85] Matt Levine, *AT&T Time Warner Will Get Another Look*, BLOOMBERG VIEW: MONEY STUFF (July 13, 2018, 11:06 AM), https://www.bloomberg.com/view/articles/2018-07-13/at-amp-t-time-warner-will-get-another-look.
[86] Order, In re Altaba Inc., f/d/b/a Yahoo! Inc., (Release No. 3937) 2018 WL 1919547 (April 24, 2018).
[87] *Id*.

MD&A, "were materially misleading in that they claimed the company only faced the *risk* of potential future data breaches [that might cause financial loss] . . . without disclosing that a massive data breach *had in fact already occurred*."[88] (Emphasis added.) Steven Peikin, co-director of the SEC's enforcement division, issued unambiguous remarks following the first-of-its-kind enforcement action, warning the fine "should serve as a message to other companies," and "to the extent that reasonable investors would view the information as material, the concept of omitting to disclose a material fact is part of the language of the anti-fraud law."[89] With two high-profile examples of this brand of nontraditional enforcement, the SEC has put public companies on notice that failure to affirmatively disclose data breaches or misleading the public as to the nature and severity of such breaches is likely to draw significant enforcement attention likely to result in fines and other sanctions.[90]

Elsewhere, one state court in New York established an outer limit to the use of securities law as a blunt object.[91] In a suit against Exxon, the New York attorney general alleged the company inconsistently presented "proxy costs" used to measure the environmental impact and cost of regulation.[92] The lawsuit alleged Exxon's internal figures did not match those disseminated to the public, which mislead with respect to Exxon's financial exposure to climate change.[93] The trial court in New York dismissed

[88] *Id.*
[89] Merle & Dwoskin, *supra* note 38.
[90] In February 2018, the SEC issued new guidance on when a company must disclose a data breach. See SEC Press Release 2018-22, Securities and Exchange Commission, SEC Adopts Statement and Interpretive Guidance on Public Company Cybersecurity Disclosures (Feb. 21, 2018), https://www.sec.gov/news/press-release/2018-22.
[91] *See generally* Joseph McClure, *Securities Fraud: Not Just for Policing Financial Markets*, DUKE LAW FINREG BLOG (May 2019), https://sites.duke.edu/thefinregblog/2019/05/02/securities-fraud-not-just-for-policing-financial-markets/.
[92] *Id.*
[93] *Id.*

the suit, finding the internal and public proxy costs were different metrics.[94] Of course, this is a state-level case based on The Martin Act, a statutory scheme unique to New York, so this decision has no bearing on the federal system or other states. However, a similar lawsuit is currently pending in Massachusetts.[95] State attorneys general have obviously taken their cues from the SEC in pursuing these nontraditional enforcement actions. Whether this trend leads to an expansion or contraction of the practice remains to be seen.

IV. Weighing the Consequences

This basic structure does not stop with data breaches, but could extend to countless areas of corporate misconduct: Company A does a bad thing; Company A does not disclose that bad thing; some time later, the public finds out and the stock price falls; the government decides to impose a penalty for defrauding public shareholders who are a proxy for the public at-large. This rough framework for punishing bad behavior is certainly convenient for government enforcement agencies. A decline in share value that is proximately caused by nondisclosure of material information is a clear violation of securities law. The ease with which enforcement actions can state this uncontroversial legal principle makes reliance on it tempting. This is especially true in circumstances which present intricate and disputed fact patterns which may complicate the application of more conventional legal tools to punish bad behavior. In some circumstances, like that of Facebook, it may be unclear if the underlying bad behavior is even illegal due to either unsettled application of legal principles or a dearth of regulation. Enforcement agencies

[94] Decision, State v. Exxon Mobil Corp., (No. 452044/2018) (Sup. Ct of NY, Monroe County, Dec. 10, 2019)

[95] Complaint, Commonwealth of Massachusetts v. Exxon Mobil Corp., (No. 19-3333) (Sup. Ct of Mass., Oct. 24, 2019).

rarely have an appetite for prolonged legal battles where the law is unclear, often preferring a negotiated settlement imposing a fine. In light of such difficulties, the ease of prosecuting violations of securities law is attractive and comes with some certainty that enforcement will be successful. Simply put, applying securities law to detestable conduct may be attractive because engaging those laws frequently does not require legal massage or logical gymnastics to find the purported violation.

It is also a convenient remedy for the consumers or users who themselves are unable to practically pursue legal action, but who nonetheless want to see some sort of punishment inflicted on the companies that have caused them harm. This framework can be utilized for all kinds of corporate conduct that does not fit neatly into the government's toolkit of criminal and civil laws and penalties. However, corporate non-disclosure of a material risk to company value *does* fit neatly within the government's power to punish companies for violations of federal securities law. The deterrent effect is likely the same as if the company were actually punished for the underlying conduct. The company cares not whether it is paying a fine for allowing massive data misuse or for simply failing to tell people about the massive data misuse. To be sure, the solution to avoid enforcement actions and civil penalties is not to be more careful in orchestrating a cover-up. The solution is to be more careful to avoid doing anything that is likely to be viewed as severely harmful, but in the case of an accident, to timely disclose it so as to prevent further harm. Of course, both would be ideal; but the latter is much easier to control. Once the conduct is disclosed, public debate can shift to the adequacy of the company's response, but at least those affected can judge for themselves whether further individual action is required for self-protection. The rationale of using securities law to punish companies that fail to disclose is the *ex ante* deterrent effect to covering up serious misconduct, to promote transparency, and to encourage responsiveness. This is the "message" the SEC is presumably trying to send.

But this new theory of liability in securities law does not come without perils. One obvious potential critique of this approach is that using securities law as an all-purpose sword subverts the process of developing more precise legal tools. The ease of fitting this kind of punishment into the same box as more traditional violations of securities law effectively short-circuits a broader debate and delays use of the democratic process to address corporate bad behavior. A law that specifically regulates data use, sexual harassment, climate change, or gun violence would undoubtedly be more effective at punishing misconduct and certainly would appear more logically related to deterring corporate bad behavior. If securities law is regarded as a sufficient remedy for all corporate misconduct, the public may be deprived of a robust public discussion required to stimulate the political will necessary to enact precise legislation. Securities law is designed to regulate capital markets, not to function as the government's catch-all legal net for policing the conduct of public companies.

We must also consider whether this use of the government's enforcement mechanisms in this way is consistent with the intent of Congress, and whether there exists a potential for abuse. Congress is constitutionally responsible for legislating, and our laws should punish the conduct the government deems reprehensible if our system is to make sense. Opponents may argue that employing securities law to punish bribery,[96]

[96] Bray, *supra* note 3.

defective products,[97] or climate change skepticism[98] treats the operation of securities law as unmoored from any original Congressional intent. The primary purpose of securities law is to ensure the public maintains faith in the integrity of the market.[99] Contrary to popular belief, federal securities regulation was not "dreamed up precipitously in the nightmare which followed the dramatic stock market collapse of 1929,"[100] but rather was implemented as part of a consolidation and an upgrade of state "blue sky" laws in order to promote disclosure and transparency and thus, to improve trust in financial markets.[101] In 1933, two months before the passage of the Securities Act (a precursor and compliment to the Exchange Act passed just months later), President Roosevelt made clear the purpose of creating federal securities law was not to guarantee value of the securities, but to ensure "full publicity and information, and so no essentially important element attending the issue is concealed from the buying public."[102] The overall goal remains the promotion of the free sharing of information from corporate executives to their shareholders and other potential investors. But the implied intent is that the shared information is *financial* in nature: the nuts and bolts of how the security works, what assets and debts are behind the company that issued it, and an estimation of what events may change the value of those assets.

---

[97] Schoenberg, *supra* note 4.
[98] Levine, *supra* note 5.
[99] *See* JOEL SELIGMAN, THE TRANSFORMATION OF WALL STREET 3 (1982).
[100] Edward Gadsby, *Historical Development of the S.E.C.–The Government View*, 28 GEO. WASH. L. REV. 6 (1959).
[101] Rutheford B Campbell, Jr., *Federalism Gone Amuck: The Case for Reallocating Governmental Authority over the Capital Formation Activities of Businesses*, 50 WASHBURN L.J. 573, 578 (2010) (explaining the overlap of blue sky laws and the 1933 Act, and noting the emphasis on disclosure and transparency in the federal regime).
[102] Address to Congress by Franklin D. Roosevelt (March 1933), *reprinted in* M. PARRINO, TRUTH IN SECURITIES 23 (1968).

With information more accessible than ever before, what constitutes *material information* may have transformed somewhat. As information is exchanged over the Internet with increasing speed, shareholders' expectations regarding information to which they are entitled may have also evolved. For example, in 2011, the share price of Apple was significantly affected by news of CEO Steve Jobs's deteriorating health.[103] Additionally, in 2018, Tesla shares dropped sharply when CEO Elon Musk appeared on a podcast smoking marijuana.[104] These examples are analogous only in that they both involve the private lives of the top corporate officers. CEOs and other officers are agents of the corporation, and arguably embody the public persona of the company,[105] but they are also human and surely entitled to some measure of privacy. The contemporary financial market apparently does not agree. Even minor details about elements of officers' private lives such as health and social habits move share prices of companies in a material way. These seemingly private matters constitute material information in the minds of shareholders; thus, the shareholders believe they must be entitled to disclosure. These anecdotes illustrate the extent to which modern investors view the importance of new information, however tortuously connected to the financial health and required reporting of the company. It is hard to imagine that in the depths of the Great Depression, Congress could have intended to ensure shareholders be appraised of information such as the private lives of corporate officers. Nonetheless, under modern construction of these laws, it remains that owners of a corporation should be apprised of *all* material operations

---

[103] Heather Struck, *Steve Jobs' Sick Leave Could Slow Down Apple Stock*, FORBES (Jan. 17, 2011), https://www.forbes.com/sites/heatherstruck/2011/01/17/steve-jobs-sick-leave-could-slow-down-apple-stock.

[104] Sarah Salinas, *Tesla Stock Closes Down 6% After Top Executives Resign and Elon Musk Smokes Weed on Video*, CNBC (Sept. 7, 2018), https://www.cnbc.com/2018/09/07/tesla-sinks-8percent-after-bizarre-musk-podcast-appearance-cao-exit.html.

[105] Love, *supra* note 13.

of their company, whether the news is positive or negative, so that they may make ownership decisions that may reflect their own values as individuals. As shareholders' expectations of materiality broaden, so will this element of securities law.

We must bear in mind that this remedy is currently only available against public companies; the implications of employing securities fraud as a catch-all remedy for corporate misconduct could influence changes in decisions about corporate structure and participation in the public markets. Companies may decide that if it is impossible to predict what sort of conduct could subject them to liability under the securities law, the shareholders' interests may be better served by the business remaining or going private where the most stringent disclosure requirements are avoided.[106] Operating privately, companies can continue their activities as before, with less scrutiny from governmental agencies, but also with restricted access to capital. The potential negative consequences to economic growth of such a shift are both uncertain and far beyond the scope of this article. But there is no reason that the provisions of federal securities law discussed in this article could not be extended to private companies. Leadership of the SEC has recently discussed the merits of allowing private companies easier access to capital by cutting restrictions on issuers to allow more "mom-and-pop" investors to participate in private securities investments.[107] Certainly, the periodic and mandatory reporting requirements may impose severe burdens on private companies. However, it cannot be unreasonable to require truthfulness in all voluntary disclosures, and to impose a duty to correct

[106] *See* Patrick Muldoon, *Remaining, or Going, Private: Traditional and New Rationales* (forthcoming 2019).
[107] Dave Michaels, *SEC Chairman Wants to Let More Main Street Investors in on Private Deals*, WALL ST. J. (Aug. 30, 2018), https://www.wsj.com/articles/sec-chairman-wants-to-let-more-main-street-investors-in-on-private-deals-1535648208.

misstatements similar to that required under Rule 10b-5. This proposal is currently in its infancy, but if it receives serious debate, discussions about expanding the public reporting required of privately held companies and about imposing increased legal exposure for false or misleading public statements should occur.

Finally, we must consider the judgments this new theory of liability inherently makes about the victims of corporate conduct, the victims who the government seeks to protect through its enforcement. Criminal law is inherently an expression of society's values.[108] If millions of users' personal information is disseminated without their knowledge, and misused to their detriment, it seems inequitable to find that *the shareholders of the company who violated their own users' confidence* deserve recompense for this harm. Consider the allegations of sexual harassment at CBS that have prompted a shareholder lawsuit alleging securities fraud.[109] If the court were to find in favor of the plaintiffs, the court would be finding that CBS's non-disclosure of pervasive sexual harassment (and possibly assault) by its CEO inflicted harm *on the shareholders*, rather than on the women who were sexually harassed. To put a finer point on it, "the claim that workplace-based sexual harassment damages shareholders through the misallocation of human capital might be interpreted to imply that the female employees of publicly traded corporations are themselves corporate assets."[110]

But at least in the case of Facebook, maybe shareholders, not consumers, *actually are* the victims. Consumers of Internet-connected products and social media *must* have at

[108] *See* Robert Cooter, *Expressive Law and Economics*, 27 J. LEGAL STUD. 585, 596-97 (1998) *and* Cass R. Sunstein, *On the Expressive Function of Law*, 144 U. PA. L. REV. 2021, 2024–26, 2045 (1996).
[109] James, *supra* note 7.
[110] Daniel Hemel & Dorothy Lund, *Sexual Harassment and Corporate Law*, 118 COLUM. L. REV. 1583 (2018).

least some awareness their data is being collected and shared with other parties. There have been various reports of phone manufacturers allowing access to users' text messages,[111] mobile apps tracking and storing user location data without users' permission,[112] and mobile apps potentially even listening to users while the app is in use.[113] All this to say nothing of the data that users *voluntarily* provide to social media and other websites like Facebook. The continued use of these products and services is at least some evidence consumers do not really care about safeguarding their data. Anecdotally, perhaps people use these services despite commonly known faults because they are convenient and users have made an economically rational judgment, whether consciously or unconsciously, that the convenience is worth more than their individual privacy. A proponent of this philosophy might ask, "How can consumers turn around and claim harm when they have ignored the risks for their own convenience? Doesn't this suggest the consumers do not *really* care about how their data is being used? Or does it just reflect an inability to do anything about it?" All of these seem true, but the latter suggestion of powerlessness seems *more true*. If a consumer could do something to protect his or her data without incurring substantial costs for the chance at nominal recovery, the consumer may be more likely to take action against the responsible entity. It

[111] Tom Warren, *Facebook Has Been Collecting Call History and SMS Data From Android Devices*, THE VERGE (March 25, 2018), https://www.theverge.com/2018/3/25/17160944/facebook-call-history-sms-data-collection-android.
[112] Associated Press, *Google Found to Track theLlocation of Users Who Have Opted Out*, NBC NEWS (Aug. 13, 2018), https://www.nbcnews.com/tech/tech-news/google-tracks-your-movements-it-or-not-n900106.
[113] Andrew Griffin, *iPhones are Not Listening in on Their Users, Apple Says – but Third-Party Apps Could Be*, THE INDEPENDENT (Aug. 9, 2018), https://www.independent.co.uk/life-style/gadgets-and-tech/news/iphone-apple-listening-data-privacy-security-apps-facebook-instagram-a8484256.html; Contrary to some of the most feverish speculation, Facebook CEO Mark Zuckerberg has testified to Congress that Facebook and Instagram do not collect user data via mobile device microphones, see CNBC, Zuckerberg Senate Joint Committee Testimony, YOUTUBE (April 11, 2018), https://www.youtube.com/watch?v=pI_6we-nqBk.

is unrealistic to suggest that consumers have a Hobson's choice between allowing companies to expose dossiers of user data and living disconnected. That is no choice at all!

People have both personal and professional responsibilities that require them to stay connected with other people through the Internet, which inherently requires some disclosure of data. Perhaps the bottom line is that "[m]ore than a decade into the era of prevalent social networks and smartphones, people still have no way to make informed choices about how to safely conduct their lives online."[114] While consumers may be willing to interact with a company despite not fully comprehending the value of their own data they are putting at risk, shareholders who otherwise have no consumer connection to the company hold no such data interest. Consumers may willingly trade their data for the convenience of a product, but shareholders have made no such trade. Shareholders' interests are purely financial. In exchange for providing capital, shareholders are entitled to be informed of all material information, including whether the company is using consumers' data in a way that would be reputationally toxic. Stated another way, consumers use a product the company produces, and are entitled to remuneration if the product itself causes injury. To shareholders, shares of the company itself are the product; if through its operations, the company causes injury to the owners of those shares, the shareholders are entitled to be compensated. For shareholders, the recoverable injury is always the decline in value of the company's stock caused by the release of previously undisclosed material information.

---

[114] Shira Ovide, *No, Google, We Did Not Consent to This*, BLOOMBERG OPINION: TECHNOLOGY & IDEAS (Oct. 8, 2018, 3:05 PM), https://www.bloomberg.com/view/articles/2018-10-08/google-privacy-glitch-no-we-did-not-consent-to-this.

By failing to disclose material information when the company has engaged in conduct that may harm consumers, the company has not inherently violated any obligation to its consumers. But this nondisclosure clearly violates the covenant it made with shareholders. Moreover, it robs the shareholders of the ability to decide whether to make more socially responsible (or financially advantageous) decisions with their capital. Viewed this way, shareholders clearly *are* the victims of corporate misconduct that can be punished by enforcement of securities law. When presented with comprehensive information, shareholders may decide against investing in companies that misuse consumer data, accelerate climate change, contribute to gun violence, or violate some other social virtue. But investors can only make these decisions if they are fully informed about the companies they research. Essentially, if investors had known about the Cambridge Analytica debacle in 2015, they may have decided that Facebook was not worthy of their capital investment, and looked to invest in some other company. Transparency itself may deter corporate impropriety, or it may perhaps incentivize some measure of corporate social responsibility. The best way to promote transparency is the vigorous enforcement of securities law to protect the shareholders' right to be fully informed.

V. Conclusion

Whether in response to data breaches, irresponsible climate change skepticism, gun violence, the opioid epidemic, or workplace sexual misconduct, federal securities law is a convenient but imperfect vehicle for punishing bad corporate behavior. This tool, whether utilized by shareholders or government agencies, is useful for disciplining the entities who are culpable, yet elusive to reprimand, under traditional civil and criminal law. However, given the looseness with which they may apply to a broad range of malfeasance, federal securities laws have a significant potential for abuse when used to correct non-traditional financial crimes in this way. In addition, the victims of corporate misconduct which are identified by these laws and the societal values expressed by their enforcement are neither complete, nor absolute. Liability under securities law may not make victims whole, or even satisfy a thirst for conventional justice; but it can deter silence and increase transparency especially from corporations that receive substantial public trust in the form of sensitive user data or common product use. As suggested, the enforcement regime described is not perfect, but it is better than allowing amorphous corporate misconduct to go unchecked. Sometimes, better is good.