Tennessee Journal of Law and Policy

Volume 15
Issue 1 *Autumn 2020*

Article 5

September 2020

Schrödinger's Hacker

Eric C. Chaffee

Follow this and additional works at: https://ir.law.utk.edu/tjlp

Recommended Citation
Chaffee, Eric C. (2020) "Schrödinger's Hacker," *Tennessee Journal of Law and Policy*: Vol. 15: Iss. 1, Article 5.
DOI: https://doi.org/10.70658/1940-4131.1029
Available at: https://ir.law.utk.edu/tjlp/vol15/iss1/5

This Article is brought to you for free and open access by Volunteer, Open Access, Library Journals (VOL Journals), published in partnership with The University of Tennessee (UT) University Libraries. This article has been accepted for inclusion in Tennessee Journal of Law and Policy by an authorized editor. For more information, please visit https://ir.law.utk.edu/tjlp.

TENNESSEE JOURNAL
OF LAW AND POLICY

VOLUME 15 AUTUMN 2020 ISSUE 1

ARTICLE

SCHRÖDINGER'S HACKER: INSIDER TRADING AND DATA BREACHES

Eric C. Chaffee[*]

[*] Professor of Law, The University of Toledo College of Law; J.D., University of Pennsylvania Law School; B.A., The Ohio State University. I would like to thank Professor Joan MacLeod Heminway and the editorial board of the *Tennessee Journal of Law & Policy* for inviting me to participate at their symposium and to contribute to this symposium issue. I would also like to thank Christine Gall, Esq. for her encouragement while drafting this work. The views set forth in this essay are completely my own and do not necessarily reflect the views of any employer or client either past or present.

I. A Story of Stories

The current legal framework governing insider trading is a rich fabric of interwoven stories constructed on a loom of law and regulation. Despite securities law at times gaining a reputation for being cumbersome and onerous,[1] the stories underlying insider trading regulation are usually vibrant and engaging.

For example, although Rule 10b-5 is the foundation of insider trading regulation, Milton Freeman has famously and fascinatingly recounted the thinness of its drafting history:

> I was sitting in my office in the S.E.C. building in Philadelphia and I received a call from Jim Treanor who was then the Director of the Trading and Exchange Division. He said, "I have just been on the telephone with Paul Rowen," who was then the S.E.C. Regional Administrator in Boston, "and he has told me about the president of some company in Boston who is going around buying up the stock of his company from his own shareholders at $4.00 a share, and he has been telling them

[1] *See* Donald C. Langevoort, *United States Securities Regulation and Global Competition*, 3 VA. L. & BUS. REV. 191, 192 (2008) ("Various well-publicized, bipartisan blue-ribbon committee reports have criticized U.S. securities regulation for being unduly cumbersome, and, in part, blamed overregulation for a loss of competitiveness in the global capital marketplace."); A.C. Pritchard, *Securities Law in the Roberts Court: Agenda or Indifference?*, 37 J. CORP. L. 105, 106 (2011) ("To outsiders, securities law is not all that interesting. The body of the law consists of an interconnecting web of statutes and regulations that fit together in ways that are decidedly counter-intuitive. Securities law rivals tax law in its reputation for complexity and dreariness.").

> that the company is doing very badly, whereas, in fact, the earnings are going to be quadrupled and will be $2.00 a share for this coming year. Is there anything we can do about it?" So he came upstairs and I called in my secretary and I looked at Section 10(b) and I looked at Section 17, and I put them together, and the only discussion we had there was where "in connection with the purchase or sale" should be, and we decided it should be at the end.
>
> We called the Commission and we got on the calendar, and I don't remember whether we got there that morning or after lunch. We passed a piece of paper around to all the commissioners. All the commissioners read the rule and they tossed it on the table, indicating approval. Nobody said anything except Sumner Pike who said, "Well," he said, "we are against fraud, aren't we?" That is how it happened.[2]

In addition to containing an affirmative fraud by the president of the company, the story also suggests that he might have been trading on some undisclosed inside information about the prospects of the firm as well.[3]

Although the SEC promulgated Rule 10b-5 in 1942, it waited until 1961 in an administrative proceeding, *In re Cady, Roberts & Co.*, to clarify its application to insider trading.[4] The Supreme Court of the United States has adopted and summarized the test for insider trading from this proceeding as follows: "(i) the existence of a relationship affording access to inside

[2] Milton V. Freeman, *Administrative Procedures*, 22 BUS. LAW. 891, 922 (1967).

[3] *Id.*

[4] *In re* Cady, Roberts & Co., 40 S.E.C. 907 (1961).

information intended to be available only for a corporate purpose, and (ii) the unfairness of allowing a corporate insider to take advantage of that information by trading without disclosure."[5] As a consequence, while no general duty to disclose information exists, the reason why this nondisclosure of information becomes actionable is because of a breach of a fiduciary duty.[6] Importantly, the Court has been careful to clarify that insider trading occurs under Rule 10b-5 only when there is a "manipulation or deception."[7] As a result, in cases of failure to disclose information obtained from a breach of fiduciary duty, one is looking for "secret profits" that result from trading on information from that breach.[8]

Behind each major innovation or clarification of insider trading regulation has been a fascinating story. In *Chiarella,* the story of a "markup man" stealing information from a financial printer revealed the classical theory of insider trading;[9] in *Dirks,* the story of a former business executive and a broker-dealer attempting to expose accounting fraud revealed the regulation of tipper-tippee liability;[10] and in *O'Hagan,* the story of a rogue attorney revealed the misappropriation theory.[11] Even the unrealized watershed opinions in insider trading law offer useful teaching tools in terms of their fact patterns. For example, the stories underlying *Chiarella* and *Carpenter* both provide rich narratives in which the misappropriation theory of insider trading could have

[5] Chiarella v. United States, 445 U.S. 222, 227 (1980).

[6] Dirks v. SEC, 463 U.S. 646, 654 (1983); *Chiarella*, 445 U.S. at 227–29.

[7] *Dirks*, 463 U.S. at 654 (quoting Santa Fe Industries, Inc. v. Green, 430 U.S. 462, 473).

[8] *Id.*

[9] *Chiarella*, 445 U.S. at 224.

[10] *Dirks*, 463 U.S. at 648–49.

[11] United States v. O'Hagan, 521 U.S. 642, 647–48 (1997).

been recognized but was not adopted by the Court.[12]

Of course, insider trading regulation in the United States is not limited to the nondisclosure of information obtained through a breach of fiduciary duty, which is rendered unlawful by section 10(b) and Rule 10b-5. Section 16(b) of the Securities Exchange Act of 1934 renders certain short swing profits by directors, officers, and beneficial owners forfeit to the issuer of the securities.[13] The stories underlying section 16(b) cases tend not to be page-turners based on the complexity of the application of this statute.[14] However, the story behind Rule 14e-3(a)—which places a draconian prohibition on trading on information regarding a tender offer regardless of whether a misrepresentation, deception, or breach of fiduciary duty occurs—is interesting.[15] In the wake of *Chiarella,* a case that the SEC lost, the Commission promulgated Rule 14e-3(a) as a means of ensuring that they would never lose a similar case again.[16] Because the Rule places a very strong prohibition on trading on material non-public information regarding tender offers, it is actually an affront to the underlying theory behind federal securities

[12] Carpenter v. United States, 484 U.S. 19 (1987) (involving a reporter stealing information from the *Wall Street Journal* for purposes of trading in securities impacted by the information).

[13] 15 U.S.C. § 78p(b) (2020).

[14] *See, e.g.*, Foremost-McKesson, Inc. v. Provident Sec. Co., 423 U.S. 232 (1976); Reliance Elec. Co. v. Emerson Elec. Co., 404 U.S. 418 (1972).

[15] 17 C.F.R. 240.14e-3(a) (2019).

[16] *See* Franklin A. Gevurtz, *The Globalization of Insider Trading Prohibitions*, 15 TRANSNAT'L LAW. 63, 81 (2002) ("As a reaction to the Chiarella decision, the SEC used its rulemaking authority under Section 14(e) of the Securities Exchange Act to adopt Rule 14e-3(a)."); Zohar Goshen & Gideon Parchomovsky, *On Insider Trading, Markets, and "Negative" Property Rights in Information*, 87 VA. L. REV. 1229, 1230 n.5 (2001) ("Following Chiarella, in an attempt to narrow the scope of the holding, the SEC enacted Rule 14e-3(a).").

regulation, i.e., full and fair disclosure.[17] The moral of the story: Don't mess with the SEC.

The question that remains is this: what stories are left to be told regarding insider trading regulation? Perhaps, unsurprisingly, many of these stories relate to how this area of law intersects with technology, especially concerns relating to data protection and cybersecurity.

Some of the application of existing insider trading regulation is relatively straight-forward. For example, the SEC charged two former Equifax employees with insider trading based on their alleged trading in the wake of the Equifax data breach that exposed social security numbers and other personal information of approximately 148 million people in 2017.[18] Assuming the allegations are true, such a case in which an employee trades upon material non-public information of a data breach prior to its disclosure offers a relatively easy example of a violation of existing insider trading law.[19] At best, it serves as a cautionary tale that companies need to have policies and procedures in place to ensure

[17] See SEC v. Capital Gains Res. Bureau, Inc., 375 U.S. 180, 186 (1963) ("A fundamental purpose, common to [all federal securities laws], was to substitute a philosophy of full disclosure for the philosophy of caveat emptor and thus to achieve a high standard of business ethics in the securities industry.").

[18] *See* Press Release, SEC, Former Equifax Executive Charged with Insider Trading (Mar. 14, 2018), https://www.sec.gov/news/press-release/2018-40; Press Release, SEC, Former Equifax Manager Charged with Insider Trading (June 28, 2018), https://www.sec.gov/news/press-release/2018-115.

[19] *See* SEC v. Texas Gulf Sulphur Co., 401 F.2d 833, 848 (2d Cir. 1968) ("[A]nyone in possession of material inside information must either disclose it to the investing public, or, if he is disabled from disclosing it in order to protect a corporate confidence, or he chooses not to do so, must abstain from trading in or recommending the securities concerned while such inside information remains undisclosed.").

that employees do not engage in insider trading in the wake of cybersecurity incidents, and to ensure prompt public disclosure of these incidents.[20]

More interesting issues emerge when a hacker obtains and trades on material nonpublic information. Notably, in cases governed by the *Cady Roberts* rule, i.e., matters involving failure to disclose material nonpublic information prior to trading, a breach of fiduciary duty to the source of the information is required, and a hacker in many instances will have no duty to the source. If the hacker uses a deception to gain access to the information, the individual has still violated section 10(b) of the Securities Exchange Act of 1934 and Rule 10b-5 promulgated thereupon, assuming the other elements have been met because fraud has still occurred based upon a material misrepresentation being used for financial gain.[21] However, if a hacker merely exploits a weakness in software to obtain material nonpublic information, the law is unclear whether this is a violation

[20] The SEC has provided guidance to public companies that suggest such an approach to dealing with cybersecurity incidents. *See* Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Securities Act Release No. 10,459, Exchange Act Release No. 82,746, 2018 WL 993646, *2 (Feb. 21, 2018) ("Public companies should have policies and procedures in place to (1) guard against directors, officers, and other corporate insiders taking advantage of the period between the company's discovery of a cybersecurity incident and public disclosure of the incident to trade on material nonpublic information about the incident, and (2) help ensure that the company makes timely disclosure of any related material nonpublic information.").

[21] 15 U.S.C. § 78j(b) (2020); 17 C.F.R. § 240.10b-5 (2020); *see* Stoneridge Inv. Partners, LLC v. Scientific–Atlanta, Inc., 552 U.S. 148, 157 (2008) ("In a typical § 10(b) private action a plaintiff must prove (1) a material misrepresentation or omission by the defendant; (2) scienter; (3) a connection between the misrepresentation or omission and the purchase or sale of a security; (4) reliance upon the misrepresentation or omission; (5) economic loss; and (6) loss causation.").

of section 10(b) and Rule 10b-5.

The current story regarding the intersection of hacking and insider trading is that of Oleksandr Dorozhko, a Ukrainian hacker held liable for violating section 10(b) and Rule 10b-5.[22] Importantly, because that story ended in an unopposed motion for summary judgment against Dorozhko, the law remains unclear as to whether a hacker who merely exploits a weakness in software to obtain material nonpublic information has violated section 10(b) and Rule 10b-5. This essay will present Dorozhko's story and explore possible endings to the legal issues that it left unresolved.

The remainder of this essay will be structured as follows. Part II will provide an overview of Oleksandr Dorozhko's story including the allegations against him and the subsequent litigation. Part III discusses the uncertainty in the law created by Dorozhko's story in terms of what is covered by insider trading regulation and section 10(b) and Rule 10b-5 generally regarding hacking. Finally, Part IV discusses various solutions to this uncertainty including common law created by the courts, congressional legislation, or rulemaking by the SEC. Further, Part IV argues that although congressional legislation is most desirable, SEC rulemaking is likely the most feasible means for resolving how section 10(b) and Rule 10b-5 interface with hacking. This Essay also contains a sample rule that could be adopted by the SEC.

II. The Story of Oleksandr Dorozhko

Perhaps unsurprisingly, the information regarding Dorozhko, an accused foreign-born hacker, is relatively thin. Most of the available information relating to his story comes from the litigation itself. In addition, because Dorozhko exercised his Fifth Amendment right

[22] *See infra* Part II (providing the story of Oleksandr Dorozhko).

against self-incrimination and did not testify during the case, some of the underlying facts likely remain open to dispute.[23] Although the District Court did ultimately grant the SEC's unopposed motion for summary judgment in civil court, Dorozhko was not convicted in a criminal proceeding, and as a result, he remains innocent until proven guilty. Nevertheless, the allegations that can be pieced together do tell a compelling story that presents an unresolved and complex issue regarding the types of behavior rendered unlawful under section 10(b) and Rule 10b-5.

A. A Hacker's Tale

At the time of the alleged unlawful activity, Oleksandr Dorozhko was a Ukrainian citizen in his early fifties residing in Uzhgorod, Ukraine.[24] He worked as a self-employed engineering consultant in the energy industry, and he had an income of approximately $45,000 to $50,000 per year.[25] His net worth was between $100,000 to $250,000.

Although Dorozhko invoked his Fifth Amendment right against self-incrimination and did not testify during the case, the SEC presented evidence suggesting that the following events occurred during October 2007. On October 4, 2007, Dorozhko transferred $42,500 to Interactive Brokers LLC, a registered broker-dealer in Greenwich, Connecticut, to open an online trading account.[26] Beginning at 8:06 am on October 17, 2007 and continuing throughout that morning and the early afternoon, a hacker began probing a website of IMS Health, a publicly-traded company headquartered in Norwalk, Connecticut.[27] The website was hosted by

[23] SEC v. Dorozhko, 606 F.Supp.2d 321, 322 (2008).
[24] *Id.* at 324.
[25] *Id.* at 325.
[26] *Id.*
[27] *Id.*

Thompson Financial, a division of Thompson Corporation, that assisted many Fortune 500 companies with investor relations matters.[28] IMS Health had stated publicly as early as October 9 that it would announce its third quarter earnings on October 17, 2007 around 5:00 pm.[29] At 2:01 pm, in preparation for the announcement, IMS Health sent slides containing its earnings report to Thompson Financial.[30] Thompson Financial formatted the slides and uploaded them to a secure server with the intent that they be kept confidential until the announcement later that day.[31] At 2:15 pm, the hacker probed the Thompson Financial network and located the slides.[32] By 2:18 pm, the hacker had downloaded and viewed the slides containing the IMS earnings report.[33]

According to the SEC, beginning at 2:52 pm, Dorozhko for the first time began using the online trading account that he had established with Interactive Brokers LLC. By 3:06 pm, he had acquired $41,670.90 of put options that would expire on October 25 and 30, 2007.[34] At 4:33 pm, after the close of market, IMS Health released its disappointing third quarter earnings information to the public.[35] At 9:30 am on October 18, 2007, the market opened, and IMS Health's stock plunged 28%.[36] At 9:35 am, Dorozhko began selling the put options that he had purchased using the online trading account.[37] By 9:41 am, he had sold all of the options that he purchased the previous day at a net profit of $286,456.59.[38]

[28] *Id.*

[29] *Dorozhko*, 606 F.Supp.2d at 325 (2008).

[30] *Id.*

[31] *Id.* at 325–26.

[32] *Id.* at 326.

[33] *Id.*

[34] *Id.*

[35] *Dorozhko*, 606 F.Supp.2d at 326 (2008).

[36] *Id.*

[37] *Id.*

[38] *Id.* at 327.

Shortly thereafter, Interactive Brokers LLC froze Dorozhko's account to conduct an internal investigation that led the matter to be referred to the SEC.[39] On October 29, 2007, the SEC filed for and received in the United States District Court for the Southern District of New York a temporary restraining order to freeze the proceeds from Dorozhko's trades and for other related relief.[40]

B. SEC v. Dorozhko

The district court ultimately granted the SEC's unopposed motion for summary judgment against Dorozhko for violating section 10(b) and Rule 10b-5 because of his activities.[41] However, the path to this outcome was not as easy as easy as it sounds.

Initially, the district court denied the SEC's motion for a preliminary injunction on the basis that the allegations against Dorozhko did not constitute insider trading under section 10(b) and Rule 10b-5 because of the lack of a breach of fiduciary.[42] Writing for the court, Judge Naomi Reice Buchwald held:

> Dorozhko's alleged 'stealing and trading' or 'hacking and trading' does not amount to a violation of § 10(b) and Rule 10b–5 because Dorozhko did not breach any fiduciary or similar duty "in connection with" the purchase or sale of a security. Although Dorozhko may have broken the law, he is not liable in a civil action under § 10(b) because he owed no fiduciary or similar

[39] *Id.*
[40] *Id.*
[41] *SEC Obtains Summary Judgment Against Computer Hacker for Insider Trading*, SEC Litigation Release No. 21,465 (Mar. 29, 2010), https://www.sec.gov/litigation/litreleases/2010/lr21465.htm.
[42] SEC v. Dorozhko, 606 F.Supp.2d 321, 324 (2008).

> duty either to the source of his information or to those he transacted with in the market.[43]

In essence, the court held that Dorozhko could not be held liable under section 10(b) and Rule 10b-5 because he did not violate the *Cady Roberts* rule that governs insider trading regulation.[44] Notably, the district court also denied Dorozhko's motion to dismiss to allow the SEC time to conduct discovery to determine whether Dorozhko's trading was the result of a tip from a corporate insider.[45]

The United States Court of Appeals for the Second Circuit reversed the district court and held that a hacker could violate section 10(b) and Rule 10b-5 in the absence of a breach of fiduciary duty if the hacker traded upon material nonpublic information obtained through a deception.[46] The Second Circuit held that a breach of fiduciary duty is only required to establish a deception for purposes of a violation of section 10(b) and Rule 10b-5 in cases involving nondisclosure in trading based upon material nonpublic information.[47] The court held that misrepresenting one's identity to gain access to information would be enough to constitute a deception for purposes of a violation of section 10(b) and Rule 10b-5.[48] However, the court also held that it is less clear as to whether "exploiting an electronic code to gain unauthorized access is 'deceptive,' rather than being mere theft."[49] Consequently, the Second Circuit remanded the case to determine whether Dorozhko's behavior was "deceptive" under section 10(b) and Rule

[43] *Id.*
[44] *Id.*
[45] *Id.*
[46] SEC v. Dorozhko, 574 F.3d 42, 43–44 (2009).
[47] *Id.* at 46–49.
[48] *Id.*
[49] *Id.*

10b-5.[50] As a result of this remand, when Dorozhko stopped participating in the litigation, the district court granted the SEC's unopposed motion for summary judgment against him for violating section 10(b) and Rule 10b-5 because of his activities.[51]

III. Schrödinger's Hacker

Dorozhko's story is fascinating because whether or not he committed the acts necessary to violate section 10(b) and Rule 10b-5 remains unclear. As discussed previously, Dorozhko exercised his Fifth Amendment right against self-incrimination, and the District Court ultimately granted the SEC's unopposed motion for summary judgment, which casts doubt upon how he gained access to IMS Health's earnings information. Manipulative or deceptive conduct is required to violate section 10(b) and Rule 10b-5, and such conduct may or may not have actually occurred in Dorozhko's case. Hinging liability under section 10(b) and Rule 10b-5 on such nuanced factual determinations is problematic for the risk that it creates to the stability of capital markets in the United States.

To understand why the Second Circuit's holding in *Dorozhko* is troubling, one should consider the following two hypotheticals. In hypothetical one, a hacker sends a company executive a phishing email that appears to be from the company's information technology department, and as a result, the hacker is able to obtain the executive's username and password. The hacker uses the username and password to gain access to the company's online electronic document system and trades based upon an earnings report that has not been released

[50] *Id.*

[51] *SEC Obtains Summary Judgment Against Computer Hacker for Insider Trading*, SEC Litigation Release No. 21,465 (Mar. 29, 2010), https://www.sec.gov/litigation/litreleases/2010/lr21465.htm.

to the public. In hypothetical two, a hacker discovers a weakness in the design of a company's online electronic document system. As a result, the hacker trades based upon an unreleased earnings report that the hacker is able to obtain because of the weakness.

Despite the fact that both hypotheticals involve trading upon material nonpublic information that was obtained in morally questionable ways, under the Second Circuit's holding in Dorozhko's case, the coverage of section 10(b) and Rule 10b-5 remains uncertain. Neither hypothetical fits within nondisclosure insider trading under section 10(b) and Rule 10b-5 because although the hacker has likely breached a number of laws, the hacker has not breached a fiduciary duty. However, insider trading regulation extends beyond nondisclosure insider trading.[52] The affirmative misrepresentation found in the phishing email in hypothetical one is likely enough for it to be rendered unlawful based on a traditional securities fraud analysis under section 10(b) and Rule 10b-5. In the absence of a misrepresentation, hypothetical two is probably not a violation of these provisions. As Milton Freeman's story at the beginning of this Essay reveals, Rule 10b-5 is only designed to render fraud unlawful. In the absence of a deception, fraud cannot exist.[53] Regardless, both hypotheticals are equally troubling in regard to investor protection and market stability.

With that said, however, the result is not absolutely certain. Assuming the matter eventually reaches the Supreme Court, the Court could hold that the behavior in hypothetical two constitutes a "deception" for purposes of section 10(b) and Rule 10b-5. However, such a result is unlikely based on the Roberts Court's unwillingness to innovate and expand the limits of federal securities regulation.[54] This is especially true

[52] *See supra* notes 13–17 and accompanying text.
[53] *See supra* note 2 and accompanying text.
[54] *See* Eric C. Chaffee, *The Supreme Court as Museum Curator: Securities Regulation and the Roberts Court*, 67 CASE W. RES.

because the Second Circuit, which decided Dorozhko's case, is no longer viewed as the "Mother Court" for innovations in securities regulation.[55] The Court could even decide that hypothetical one is not a violation of section 10(b) and Rule 10b-5 because the deception is not closely enough connected with the purchase or sale of a security.

Beyond the uncertainty and inconsistent results created by hacking in hypotheticals one and two, hacking creates other concerns relating to tampering with stock prices. Consider the following two additional hypotheticals. In hypothetical three, a hacker engages in a spoofing attack, which is a specific type of denial of service attack that allows the hacker to deceptively appear to be a large number of different users to overwhelm and shut down a website. The hacker chooses to shut down a publicly traded web-based company's website and causes the website to be offline for a week. Prior to undertaking the attack, the hacker purchases put options based on the material non-public information that the website is vulnerable. In hypothetical four, a hacker chooses to shut down a publicly traded web-based company's website and causes the website to be offline for a week, after the hacker discovers that entering certain information into the company's website will stop it from functioning. Prior to undertaking the attack, the hacker purchases put options based on the material non-public information that the website is vulnerable.

L. REV. 847, 854 (2017) ("[T]he Roberts Court is playing the role of museum curator in regard to securities regulation by preserving the artifacts created by Supreme Court precedent. . . . [T]he days of an activist Court in the area of securities regulation have long past.").

[55] *Id.* at 879–80 ("Justice Harry Blackmun famously referred to the United States Court of Appeals for the Second Circuit as the 'Mother Court' in the field of securities regulation. . . . The Roberts Court has ended the Second Circuit's role as the 'Mother Court' and the lower court laboratories approach in regard to the development of securities law . . . .").

Hypothetical three and four present similar concerns as hypothetical one and two. Hypotheticals one and three are likely violations of section 10(b) and Rule 10b-5, and the result in hypotheticals two and four are highly uncertain. However, all of the hypotheticals demonstrate that hacking poses a danger to the stability of capital markets in the United States.

These hypotheticals display an interesting parallel with the thought experiment, known as "Schrödinger's cat," posed by Austrian physicist Erwin Schrödinger in 1935 to demonstrate his issue with the Copenhagen interpretation of quantum mechanics.[56] Specifically, he was concerned about this interpretation's reliance on quantum superpositions, in which a quantum system such as an atom or photon can exist as a combination of multiple states until directly observed.[57] In describing the thought experiment, Schrödinger wrote:

> One can even set up quite ridiculous cases. A cat is penned up in a steel chamber, along with the following device (which must be secured against direct interference by the cat): in a Geiger counter there is a tiny bit of radioactive substance, so small, that perhaps in the course of the hour one of the atoms decays, but also, with equal probability, perhaps none; if it happens, the counter tube discharges and through a relay releases a hammer which shatters a small flask of hydrocyanic acid. If one has left this entire system to itself for an hour, one would say

[56] Erwin Schrödinger, *Die gegenwärtige Situation in der Quantenmechanik*, 23 NATURWISSENSCHAFTEN 807–12, 823–28, 844–49 (1935), *translated in* John D. Trimmer, *The Present Situation in Quantum Mechanics*, 124 PROCEEDINGS OF THE AM. PHIL. SOC'Y 323, 328 (1980).

[57] *Id.*

> that the cat still lives if meanwhile no atom has decayed. The psi-function of the entire system would express this by having in it the living and dead cat (pardon the expression) mixed or smeared out in equal parts.
>
> It is typical of these cases that an indeterminacy originally restricted to the atomic domain becomes transformed into macroscopic indeterminacy, which can then be resolved by direct observation. That prevents us from so naively accepting as valid a "blurred model" for representing reality.[58]

Put simply, Schrödinger's thought experiment illustrates that small facts—for example, the state of an atom—can create unacceptable indeterminacy in larger systems—for example, allowing a cat to be simultaneously alive and dead at the same time.

Similarly, *how* a hacker obtains material nonpublic information seems as though it ought to be trivial in regard to punishing under federal securities regulation because in all instances, the hacker is stealing information, and the hacking poses a danger to the stability of capital markets in the United States. However, similar to the Schrödinger's cat thought experiment, the relatively trivial issue of how the hacker obtains the information creates unacceptable large-scale uncertainty as to whether such behavior can be pursued under federal securities regulation.

IV. The End of the Story

The behavior found in all of the hypotheticals is almost certainly punishable under United States law. However, federal securities regulation is designed to

[58] *Id.*

encourage investor confidence in the capital markets. As a result, hacking in all four of the hypotheticals ought to be rendered unlawful under federal securities regulation, especially because the SEC's actions in *Dorozhko* and similar cases suggest that the agency is interested in pursuing such behavior. Three potential pathways exist for this to occur, including common law created by the courts, congressional legislation, or rulemaking by the SEC. Although a congressional enactment is most desirable, SEC rulemaking is likely the most feasible means for resolving the issues created by trading on material nonpublic information related to data breaches by hackers.

A few words ought to be said about each of the pathways for resolving this issue. First, the courts could ultimately determine that all hacking is a deceptive act under section 10(b) and Rule 10b-5. This pathway is unpalatable because it would likely take a very long time for a case to reach the Supreme Court, and the Court is no longer willing to innovate in regard to federal securities law.[59]

Second, Congress can and should amend section 10(b) to entail all forms of hacking within the purview of that provision. Although such an undertaking would likely create redundancies within existing federal law, because the federal securities law exists at least in part to encourage market confidence, such an undertaking would help to raise investor confidence. In the wake of the Equifax data breach and other cyberattacks, Congress has at least 148 million stories of individuals who are concerned about hacking. Congress should make it unequivocally clear that hacking that interferes with the efficient operation of the capital markets will not be tolerated.

Notably, at the time writing of this essay, the

[59] *See supra* note 54 and accompanying text (discussing that the Roberts Court has worked to maintain the status quo regarding most substantive issues of securities regulation).

United States House of Representatives had passed the Insider Trading Prohibition Act.[60] The bill provides a broader prohibition against insider trading than currently exists under federal law and would modify existing federal securities law to include the following provision:

> It shall be unlawful for any person, directly or indirectly, to purchase, sell, or enter into, or cause the purchase or sale of or entry into, any security, security-based swap, or security-based swap agreement, while aware of material, nonpublic information relating to such security, security-based swap, or security-based swap agreement, or any nonpublic information, from whatever source, that has, or would reasonably be expected to have, a material effect on the market price of any such security, security-based swap, or security-based swap agreement, if such person knows, or recklessly disregards, that such information has been obtained wrongfully, or that such purchase or sale would constitute a wrongful use of such information.[61]

In defining the type of "wrongful" conduct would be rendered unlawful, the drafters include use of "information [that] has been obtained by, or its communication or use would constitute, directly or indirectly . . . a violation of any Federal law protecting computer data or the intellectual property or privacy of computer users."[62] Importantly, even if this bill is passed by the Senate and alters federal securities law, hypothetical four in which a hacker exploits a weakness

[60] H.R. 2534, 116th Cong. (as passed by the House, Dec. 5, 2019).

[61] *Id.* at § 2(a).

[62] *Id.*

in a website to shut down a web-based company and then trades in the company's securities likely would still not be covered by federal law. With that said, this result is not entirely certain because of the breadth of the language contained under the Insider Trading Prohibition Act.[63] Regardless, the uncertain coverage potentially would still jeopardize the confidence in the capital markets that federal securities law is designed to protect. Even if the Insider Trading Prohibition Act becomes law, additional steps would be needed to remove uncertainty in regard to the intersection of hacking and the behavior rendered unlawful by section 10(b) and Rule 10b-5.

Third, the SEC could promulgate a rule interpreting the language of section 10(b) and Rule 10b-5 to include all hacking as "deceptive acts or contrivances." The concern with this approach is that the SEC's power is limited to the power that Congress has authorized, and as a result, promulgating such a rule may be beyond the SEC's authority if it increases the coverage of section 10(b). However, The SEC has clarified the coverage of section 10(b) and Rule 10b-5 in past by enacting provisions such as Rule 10b-5-2, which clarifies when duties of trust or confidence exist for cases involving the misappropriation theory of insider trading.[64]

In regard to hacking, the SEC could promulgate the following:

(a) For purposes of section 10(b) and Rule 10b-5, material misrepresentations or omissions include:

> (1) intentionally accessing a computer without authorization or exceeding authorized access, and thereby obtaining information from any protected computer;
>
> (2) intentionally, without authorization to access

[63] *Id.*

[64] 17 C.F.R. § 240.10b5-2 (2020).

any nonpublic computer of a department or agency of the United States, accessing such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

(3)

(A) knowingly causing the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causing damage without authorization, to a protected computer;

(B) intentionally accessing a protected computer without authorization, and as a result of such conduct, recklessly causing damage; or

(C) intentionally accessing a protected computer without authorization, and as a result of such conduct, causing damage and loss.

(b) As used in this section—

(1) the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;

(2) the term "protected computer" means a computer—

(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or

(B) which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States;

(3) the term "financial institution" means—

(A) an institution, with deposits insured by the Federal Deposit Insurance Corporation;

(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;

(C) a credit union with accounts insured by the National Credit Union Administration;

(D) a member of the Federal home loan bank system and any home loan bank;

(E) any institution of the Farm Credit System under the Farm Credit Act of 1971;

(F) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934;

(G) the Securities Investor Protection Corporation;

(H) a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978); and

(I) an organization operating under section 25 or section 25(a) 1 of the Federal Reserve Act;

(4) the term "exceeding authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter;

(5) the term "department of the United States" means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5;

(6) the term "damage" means any impairment to the integrity or availability of data, a program, a system, or information;

(7) the term "government entity" includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country; and

(8) the term "loss" means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.[65]

[65] This proposed rule is based upon 18 U.S.C. § 1030, which is known as the Computer Fraud and Abuse Act. Much of the

Such a rule would clarify that section 10(b) and Rule 10b-5 covers all four of the hypotheticals discussed above and would help to promote market confidence and stability by insulating investors from the evils of hacking. Beyond that, such a rule would address the due process and notice concerns that linger in the wake of *Dorozhko*,[66] especially because violations of the federal securities law can be prosecuted criminally.[67]

Two major complaints might be lodged against the proposed rule. First, one might argue that the proposed rule is duplicative of existing federal law. In actuality, that alleged weakness is actually a strength. The proposed rule is modeled upon 18 U.S.C. § 1030, which is also known as the Computer Fraud and Abuse Act. Most of the provisions of the proposed rule are taken from section 1030, although the proposed rule is narrowed to the most likely circumstances in which securities fraud concerns might occur. Because it was enacted in 1986, section 1030 has a substantial body of case law and commentary associated with it. By using verbatim text, the proposed rule has the benefit of being better developed because the case law and commentary relating to section 1030 can be used to interpret the meaning of the provisions of the proposed rule. Of course, this creates the issue of whether it is beneficial to have an SEC Rule that is duplicative of existing federal law. In this instance, having both section 1030 and the proposed rule would be beneficial. Section 1030 is a general provision of

language contained in the proposed rule is adopted verbatim from that statute.

[66] The Fifth and Fourteenth Amendments to the United States Constitution each contain a due process clause that prevents the government from depriving individuals of "life, liberty, or property, without due process of law," and this requirement applies to civil and criminal matters. *See* U.S. CONST. amends. V, XIV.

[67] *See* 15 U.S.C. § 77x (2020) (providing criminal penalties for violating the Securities Act); *id.* § 78ff (providing criminal penalties for violating the Exchange Act).

the federal criminal law found in Title 18 of the United States. The proposed rule would be used for a very different purpose, i.e. maintaining the stability in the capital markets in the United States. Federal securities law in the United States exists for purposes of market protection.[68] Hacking has become a major concern in the United States. The proposed rule, which addresses hacking in relation to the purchase and sale of securities, should be included within federal securities law to the communicate that federal securities law is a coherent and comprehensive system of regulation that can be relied upon and trusted.

Second, one might argue that the proposed rule exceeds the SEC's authority to define the scope of Rule 10b-5. Rule 10b-5 is promulgated based upon the authority granted to the SEC under section 10(b) of the Securities Exchange Act, which mandates that

> It shall be 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, or any securities-based swap agreement 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

[68] *See* Susan B. Heyman, *Rethinking Regulation Fair Disclosure and Corporate Free Speech*, 36 CARDOZO L. REV. 1099, 1111 (2015) ("The Exchange Act was enacted after the 1929 stock market crash to restore confidence in the nation's securities market by governing securities transactions on secondary markets."); Arthur R. Pinto, *The Nature of the Capital Markets Allows a Greater Role for the Government*, 55 BROOK. L. REV. 77, 77 (1989) ("[T]he securities laws were enacted during the New Deal to insure that our capital markets remain free from the abuses and fraud that Congress believed plagued both the sale and trading of securities.").

> protection of investors.[69]

Rule 10b-5 is a product of that mandate. Any rule created by the SEC must remain within the power granted to them by Congress in section 10(b). One could argue that the proposed rule would exceed that authority. With that said, hacking is deceptive in the sense that it is often wed with attempts to conceal and redirect knowledge of the hacker's identity.

If the SEC is unwilling to promulgate a rule that makes certain acts of hacking per se material misrepresentations or omissions, the agency could promulgate a rule that creates a rebuttable presumption that in certain instances involving hacking that a misrepresentation or omission occurred. This solution has an elegance because it would force hackers to explain how they committed their bad acts to escape liability under section 10(b) and Rule 10b-5 by rebutting the presumption. If they did that, then section 1030 could easily be used to punish their bad behavior.

Hacking has become a ubiquitous concern in our society. Oleksandr Dorozhko's story illustrates that federal securities regulation is currently inadequate to deal with the securities issues associated with hacking, which poses a threat to the stability of securities markets in the United States. This Essay offers a proposed rule to remedy this problem, and it gives the SEC the opportunity to write the next chapter in this story.

[69] 15 U.S.C. § 78j (2020).