SCHRÖDINGER'S CYBERSECURITY

48 UC DAVIS LAW REVIEW (forthcoming 2014)

Derek E. Bambauer[*]

Abstract

Both law and cybersecurity prize accuracy. Cyberattacks, such as Stuxnet, demonstrate the risks of inaccurate data. An attack can trick computer programs into making changes to information that are technically authorized but incorrect. While computer science treats accuracy as an inherent quality of data, law recognizes that accuracy is fundamentally a socially constructed attribute. This Article argues that law has much to teach cybersecurity about accuracy. In particular, law's procedural mechanisms and contextual analysis can define concepts such as authorization and correctness that are exogenous to code. The Article assesses why accuracy matters, and explores methods law and cybersecurity deploy to attain it. It argues both law and cybersecurity have but two paths to determining accuracy: hierarchy, and consensus. Then, it defends the controversial proposition that accuracy is constructed through social processes, rather than emerging from information itself. Finally, it offers a proposal styled on the common law to evaluate when accuracy matters, and suggests that regulation should bolster technological mechanisms through a combination of mandates and funding. Like the cat of Schrödinger's famous thought experiment, information is neither accurate nor inaccurate until observed in social context.

[*] Professor of Law, University of Arizona James E. Rogers College of Law. Thanks for helpful suggestions and discussion are owed to Jane Bambauer, Howard Beales, Tim Brennan, Mike Carroll, Dan Castro, James Cooper, Deven Desai, Jeff Eisenach, James Grimmelmann, Woody Hartzog, Dan Hunter, Bruce Kobayashi, Bruce Johnsen, Geoff Manne, Toni Massaro, Thinh Nguyen, Sasha Romanosky, Michael Scott, Mark Spottswood, Peter Swire, Berin Szoka, Alan Trammell, and Felix Wu, along with the participants in the George Mason University School of Law LEC Research Roundtable on Privacy & Data Security, the Fourth Annual Internet Law Scholars Works-in-Progress, and the Elon University School of Law faculty workshop. Thanks for expert research are owed to Maureen Garmon and Nick Whitley. Thanks for research support are owed to the Law & Economics Center at George Mason University School of Law. The author welcomes comments at <derekbambauer@email.arizona.edu>.

Table of Contents

> *What men make, men may unmake; but what nature makes no man may dispute.*
>
> - *Steven Shapin & Simon Schaffer,* Leviathan and the Air-Pump

I. INTRODUCTION

Tom Clancy got it right: accuracy is socially constructed.

In Clancy's 1994 novel *Debt of Honor*[1], a group of Japanese nationalists[2] launches a cyberattack on U.S. stock exchanges. The attack garbles records beginning at noon on a given Friday; after a short period of time, traders are unable to obtain reliable information about their positions, leading quickly to economic crisis and widespread panic. Clancy's hero, Vice President Jack Ryan, proposes a clever solution: each investor is returned to the financial position he or she occupied as of noon Friday – the last moment when reliable data were available – and ensuing activity is treated as never having taken place. Ryan's "do-over" saves the day, and America's economy.

Clancy's plot provides three important insights. First, information systems such as the stock exchange depend upon access to accurate data – the data must reflect the latest, authorized changes, and only those changes. Second, even small disruptions to data integrity can have large effects: suspicion about reliability can become widespread, and poisonous. The economic crisis depicted in the novel developed not because of fundamental weakness in the American economic system, but rather because uncertainty about transactions – their prices, their completion, and their documentation

[1] TOM CLANCY, DEBT OF HONOR (1994).

[2] Clearly Clancy had limited prescience.

– deterred people from engaging in them. Finally, and most critically, what counts as accurate data is a social and legal construct, not simply a technical one. In Clancy's story, trades on the exchange took place after noon on the critical Friday – offers were made, and accepted – but America collectively decided that they did not count, regardless of the extant data. These insights reveal that accuracy issues in cybersecurity are not merely a set of implementation questions for engineers, computer scientists, and other geeks. Rather, they raise profound normative questions about authority, trust, and power – questions that are often legal in character.

Accuracy is a central concern for both cybersecurity and law, yet law's view of the concept is both more nuanced and more useful. Cybersecurity tends to treat accuracy from a positivist perspective, where the quality is an uncontroversial, emergent property of the data.[3] It is technologically deterministic. Law, by contrast, has a flexible, contextual approach to what counts as accurate information. Cybersecurity tends to elide the hard questions about accuracy by embedding them in code: authorization is a question about the level of one's access to a system, rather than one's purpose or intent.[4] Yet that approach is fundamentally unstable.

Accuracy of information is vitally important to cybersecurity in the real world as well. Consider three examples. First: Stuxnet.[5] The United States and Israel jointly developed, and launched, a cyberattack on Iran's nuclear refinement complex at Natanz.[6] The cyberweapon, Stuxnet, cleverly performed two interrelated tasks. First, it sped up the centrifuges used to enrich uranium to weapons-grade levels, causing them to wear out rapidly and become unstable.[7] Second, Stuxnet fed false information to the technicians monitoring the centrifuges, lulling them into the belief that the machines were performing normally.[8] The Iranian engineers could not divine why their expensive, fragile devices were failing so often. The inaccurate information that the Stuxnet worm relayed kept them from diagnosing the problem until considerable damage had been done. The attack set back Iran's nuclear program by years.[9]

[3] *See, e.g.*, Fergal Glynn, *What is Data Integrity? Learn How to Ensure Database Data Integrity via Checks, Tests, & Best Practices*, VERACODE, http://blog.veracode.com/2012/05/what-is-data-integrity/.

[4] *Id.*

[5] Derek E. Bambauer, *Conundrum*, 96 MINN. L. REV. 584, 585-86 (2011); *see generally* Ralph Langner, *Stuxnet's Evil Twin*, FOREIGN POLICY (Nov. 19, 2013), http://www.foreignpolicy.com/articles/2013/11/19/stuxnets_secret_twin_iran_nukes_cyber_attack.

[6] William J. Broad et al., *Israel Tests Called Crucial in Iran Nuclear Setback*, N.Y. TIMES, Jan. 16, 2011, at A1.

[7] *Id.*

[8] Christopher Williams, *Western Power Created Virus to Sabotage Iran's Nuclear Plans*, DAILY TELEGRAPH (LONDON), Jan. 22, 2011, at 20.

[9] Broad, *supra* note 6.

Second, DigiNotar. Iran can be a cyberattacker as well as a victim. A hacker located in Iran compromised the systems at DigiNotar, a Dutch certificate authority, in July 2011.[10] (Certificate authorities issue the encryption keys that protect Internet communications, such as over Secure Sockets Layer (SSL).[11]) After infiltrating DigiNotar's computers, the attacker used them to issue fake SSL certificates for domains such as google.com and microsoft.com.[12] This gave the attacker the capability to appear to Internet users as Google or Microsoft; the users' browsers would recognize and trust the fake certificates.[13] Iranian Gmail users, including dissidents, immediately fell victim to a "man in the middle attack" – they believed they were interacting securely with Google's e-mail system, but in fact were under surveillance by Iranian security services.[14] The certificates were technically correct, having been issued by a provider authorized to do so, but were normatively inaccurate, since they did not in fact originate from an authorized process nor did they actually represent the purported domains.[15] The disjunction between technical and normative accuracy put Iranian citizens at considerable risk – their trust in using encryption to prove Google's identity was, in this case, misplaced.

Third, YouTube. Pakistan, objecting to YouTube's hosting of the anti-Islamic film "Fitna," ordered Pakistan Telecom to censor access to the video service.[16] Pakistan Telecom did so by altering its Border Gateway Protocol (BGP) entry for YouTube.[17] The company's goal was to re-route Pakistani Internet users who attempted to reach YouTube to a page indicating that the site was censored.[18] This effort worked, but too well: Pakistan Telecom's upstream provider, PCCW Global, accepted the BGP

[10] Dennis Fisher, *Final Report on DigiNotar Hack Shows Total Compromise of CA Servers*, THREATPOST (Oct. 31, 2012), http://threatpost.com/final-report-diginotar-hack-shows-total-compromise-ca-servers-103112.

[11] *See, e.g., What Are CA Certificates?*, MICROSOFT TECHNET (Mar. 28, 2003), http://technet.microsoft.com/en-us/library/cc778623%28v=ws.10%29.aspx.

[12] John Leyden, *Inside "Operation Black Tulip": DigiNotar hack analysed*, THE REGISTER (Sept. 6, 2011), http://www.theregister.co.uk/2011/09/06/diginotar_audit_damning_fail/.

[13] Steve Schultze, *DigiNotar Hack Highlights the Critical Features of our SSL Web Security Model*, FREEDOM TO TINKER (Sept. 6, 2011), https://freedom-to-tinker.com/blog/sjs/diginotar-hack-highlights-critical-failures-our-ssl-web-security-model/.

[14] *Id.*; *see* Dennis Fisher, *What is a Man-in-the-Middle Attack?*, KASPERSKY LAB DAILY (Apr. 10, 2013), http://blog.kaspersky.com/man-in-the-middle-attack/.

[15] Fisher, *supra* note 10.

[16] Pakistan Telecommunication Authority, *Blocking of Offensive Website*, *available at* http://renesys.com/wp-content/uploads/blog/pakistan_blocking_order.pdf (Feb. 2008).

[17] Brown, *supra* note 41.

[18] Ryan Singel, *Pakistan's Accidental YouTube Re-Routing Exposes Trust Flaw in Net*, THREAT LEVEL (Feb. 25, 2008), http://www.wired.com/threatlevel/2008/02/pakistans-accid/.

update and advertised it to the rest of the Internet.[19] For technical reasons internal to BGP[20], the censored route was widely accepted, and many Internet service providers began to route requests for YouTube to the censored site in Pakistan[21]. BGP, which is both obscure and critical to proper routing of Internet traffic, essentially works on trust: many service providers accept updates without careful validation of their origin.[22] So, Pakistan was able, for a few hours, to hijack YouTube. The BGP update it provided was specific, and the most recent for YouTube, but it did not reflect an authorized change.

Law and cybersecurity are both concerned with accuracy: with creating and maintaining it, with evaluating its costs, with determining where it is more and less necessary. Between the two, though, cybersecurity would seem to hold pride of place when it comes to determining accuracy. Computer science has a wealth of techniques that push towards greater accuracy: authentication through credentials and cryptography[23], logging changes via journaling file systems[24], robust backup and recovery procedures[25], and verification of data through checksums[26], to name only a few. Law seems much more tolerant of lower states of accuracy. The standard of proof in most civil lawsuits is a mere preponderance: we think one party's version is just slightly more probable than not.[27] Judges, rather than technical specialists, define key data such as contract terms or patent

[19] *YouTube Hijacking: A RIPE NCC RIS case study* (Mar. 17, 2008), http://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study.

[20] The Pakistan Telecom update advertised a /24 network, which was more specific (for a portion of YouTube's network) than YouTube's own BGP route, which was a /22. *See* Brown, *supra* note 17; on IP addressing generally, *see Understanding IP Addressing*, RIPE NCC, http://www.ripe.net/internet-coordination/press-centre/understanding-ip-addressing.

[21] *Id.*

[22] *See, e.g.*, Bezawada Bruhadeshwar et al., *Symmetric Key Approaches to Securing BGP – A Little Bit of Trust Is Enough*, 22 IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYS. 1536 (2011).

[23] *See, e.g.*, Richard Duncan, *An Overview of Different Authentication Methods and Protocols*, SANS INSTITUTE (Oct. 23, 2001), https://www.sans.org/reading-room/whitepapers/authentication/overview-authentication-methods-protocols-118.

[24] *See, e.g.*, Vijayan Prabhakaran, Andrea C. Arpaci-Dusseau, & Remzi H. Arpaci-Dusseau, *Analysis and Evolution of Journaling File Systems*, PROCEEDINGS OF THE USENIX 2005 ANNUAL TECHNICAL CONFERENCE, *available at* http://research.cs.wisc.edu/wind/Publications/sba-usenix05.pdf.

[25] *See, e.g.*, IBM, *Tivoli Storage Manager for System Backup and Recovery*, http://www-03.ibm.com/software/products/en/tivostormanaforsystbackandreco.

[26] *See supra* note 61.

[27] *See, e.g.*, Cal. Evidence Code § 115 ("Except as otherwise provided by law, the burden of proof requires proof by a preponderance of the evidence").

claims.[28] Analytical methods of questionable accuracy – bite mark comparisons[29], narcotics dog sniffs[30], even fingerprint evidence[31] – are permitted as bases for lay jurors to opine on guilt and innocence. The legal system seems like a cacophony of conflicts and fuzzy data when compared with computer science.

And yet law has much to teach cybersecurity and computer science. The latter tends towards a positivistic view of data: a given piece of information is accurate, or it is not. This approach implicitly emphasizes the state of the information as the key determinant.[32] Law, by contrast, focuses on processes of meaning-making within a given set of inputs, rules, and norms. Accuracy is contextual and decided after the application of legal processes. Since the Legal Realist movement, there is a general consensus that accuracy, and outcomes, are determined, not predetermined.[33] In this sense, Chief Justice John Roberts was more correct than he knew when he described a judge's role, using a baseball analogy, as calling balls and strikes.[34] Roberts meant this in the positivist sense: the outcome emerges naturally on examination of the data (here, the case, or pitch).[35] That, most legal scholars agree, is a falsehood, though an oft-appealing one.[36] Instead, the genius of Roberts's point is that balls and strikes vary with the umpire.[37]

[28] *Markman v. Westview Instruments*, 517 U.S. 370, 388-90 (1996) (holding that "The construction of written instruments is one of those things that judges often do and are likely to do better than jurors unburdened by training in exegesis").

[29] Erica Beecher-Monas, *Reality Bites: The Illusion of Science in Bite-Mark Evidence*, 30 CARDOZO L. REV. 1369 (2009).

[30] Jane R. Bambauer, *Defending the Dog*, 91 ORE. L. REV. 1203 (2013).

[31] *See, e.g.*, Jonathan J. Koehler, *Fingerprint Error Rates and Proficiency Tests: What They Are and Why They Matter*, 59 HASTINGS L.J. 1077 (2008).

[32] The trinity of security objectives in information systems is confidentiality, integrity, and availability (typically abbreviated "CIA"). *See* Nat'l Inst. of Standards & Tech., U.S. Dep't of Commerce, *Standards for Security Categorization of Federal Information and Information Systems* 2, FIPS PUB 199 (Feb. 2004), http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf (defining these three objectives for the Federal Information Security Management Act); PETER W. SINGER & ALLAN FRIEDMAN, CYBERSECURITY AND CYBERWAR: WHAT EVERYONE NEEDS TO KNOW (2014); 35 U.S.C. § 3542(b)(1)(A) (defining "integrity" as "guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity").

[33] *See, e.g.*, Michael Steven Green, *Legal Realism as Theory of Law*, 46 WM. & MARY L. REV. 1915 (2005).

[34] *Roberts: "My job is to call balls and strikes and not to pitch or bat,"* CNN (Sept. 12, 2005), http://www.cnn.com/2005/POLITICS/09/12/roberts.statement/.

[35] Neil S. Siegel, *Umpires At Bat: On Integration and Legitimation*, 24 CONST. COMMENT. 701, 703 (2007).

[36] *Id.*; Charles Fried, *Balls and Strikes*, 61 EMORY L.J. 641 (2012); Thomas Colby, *In Defense of Judicial Empathy*, 96 MINN. L. REV. 1944 (2012).

[37] *See, e.g.*, Josh Weinstock, *Which umpire has the largest strike zone?*, HARDBALL TIMES (Jan. 11, 2012), http://www.hardballtimes.com/which-umpire-has-the-largest-strikezone/;

Some have a wide strike zone; others, a narrow one. Some call strikes at the letters; some don't. The strike zone, like the law, depends upon the context. That insight can be fruitfully applied to cybersecurity.

Yet legal scholarship has largely neglected questions of accuracy for cybersecurity. This is strange for at least two reasons. First, inaccurate information has potentially severe consequences for cybersecurity: it can destroy tangible objects[38], enable surveillance of putatively private communications[39], injure hospital patients[40], and block Internet users from knowledge[41]. Second, legal doctrine is highly attentive to accuracy in other areas. From recording statutes for real property[42] to rules of evidence[43] to sanctions for perjury[44], law has developed a panoply of techniques to define accuracy and to pursue it. Critically, law has a realistic understanding of the difference between the normative and technical aspects of accuracy. A director and a special effects studio may have intended to transfer ownership of the copyright in movie footage; money may have changed hands, the transaction may have been recorded with the Copyright Office, and the parties may believe the deal is done, but if there is not an

Stuart Miller, *Technology's Place in the Strike Zone*, BATS (Aug. 9, 2010), http://bats.blogs.nytimes.com/2010/08/09/technologys-place-in-the-strike-zone/; ANDREW GOLDBLATT, MAJOR LEAGUE UMPIRES' PERFORMANCE, 2007-2010 (2011).

[38] William J. Broad et al., *Israel Tests Called Crucial in Iran Nuclear Setback*, N.Y. TIMES, Jan. 16, 2011, at A1; *Christopher Williams, Western Power Created Virus to Sabotage Iran's Nuclear Plans*, DAILY TELEGRAPH (London), Jan. 22, 2011, at 20.

[39] Kim Zetter, *Someone's Been Siphoning Data Through a Huge Security Hole in the Internet*, WIRED (Dec. 5, 2013), http://www.wired.com/threatlevel/2013/12/bgp-hijacking-belarus-iceland/; Jim Cowie, *The New Threat: Targeted Internet Traffic Misdirection*, RENESYS (Nov. 19, 2013), http://www.renesys.com/2013/11/mitm-internet-hijacking/; Dan Goodin, *Repeated attacks hijack huge chunks of Internet traffic, researchers warn*, ARS TECHNICA (Nov. 20, 2013), http://arstechnica.com/security/2013/11/repeated-attacks-hijack-huge-chunks-of-internet-traffic-researchers-warn/.

[40] Scott Allen, *Drug-error risk at hospitals tied to computers*, BOSTON GLOBE (March 9, 2005), http://www.boston.com/yourlife/health/other/articles/2005/03/09/drug_error_risk_at_hospitals_tied_to_computers/?page=full; Dan Munro, *New Cyberthreat Report By SANS Institute Delivers Chilling Warning To Healthcare Industry*, FORBES (Feb. 20, 2014), http://www.forbes.com/sites/danmunro/2014/02/20/new-cyberthreat-report-by-sans-institute-delivers-chilling-warning-to-healthcare-industry/ (noting insecurity in health care industry, and stating that the "larger consumer risk isn't financial – it's the life-threatening inaccuracies in the medical records themselves").

[41] Martin Brown, *Pakistan hijacks YouTube*, RENESYS (Feb. 24, 2008), http://www.renesys.com/2008/02/pakistan-hijacks-youtube-1/.

[42] *See* Corwin W. Johnson, *Purpose and Scope of Recording Statutes*, 47 IOWA L. REV. 231 (1961).

[43] *See, e.g.*, Fed. R. Ev. 1002 (requiring original writing, recording, or photograph).

[44] *See* 18 U.S.C. § 1621 (penalizing perjury).

assignment in writing signed by the author, the transfer is inoperative.[45] Similarly, law may excuse technical defects when it seeks to validate transactions that it believes to be normatively desirable and correct, as when copyright law creates implied licenses based on oral understandings[46], or contract law establishes a term not written into the instrument to save a bargain[47].

Recent work in the second wave of cybersecurity scholarship in law has concentrated principally on regulatory mechanisms, without deep analysis of the substance of those rules. For example, Alan Butler assesses how the Third Amendment may affect American policy for cyberweapons and cyberwarfare.[48] David Thaw argues that regulatory capture can help regulators to utilize private expertise to meet public policy goals, drawing upon a case study in health care cybersecurity.[49] Nancy King and V.T. Raja press the case that both the U.S. and the European Union should undertake regulatory reform to address security and privacy in cloud computing.[50] Peter Swire, building on Neil Komesar's work, examines how negative externalities plague both public and private-sector security efforts, and evinces considerable skepticism about the potential for government to play a useful role.[51] Paul Rosenzweig, assessing whether cybersecurity poses unique problems for policymakers, identifies two points of cyberexceptionalism: the Internet's unprecedented speed and ubiquitous availability, and the asymmetric empowerment that code-based tools provide.[52] Peter Shane advocates for greater public participation in cybersecurity policymaking.[53] A team of researchers from universities in the Netherlands evaluates the technical and market characteristics of cryptographic certificates used to protect Web communication.[54] And Gerard Stegmaier and Wendell Bartnick contend that the Federal Trade

[45] 17 U.S.C. § 204(a); *see Effects Assocs. v. Cohen*, 908 F.2d 555 (9th Cir. 1990).
[46] *Cohen*, *id.*
[47] The classic case is *Wood v. Lucy, Lady Duff-Gordon*, 118 N.E. 214 (1917).
[48] Alan Butler, *When Cyberweapons End Up on Private Networks: Third Amendment Implications for Cybersecurity Policy*, 62 AM. U. L. REV. 1203 (2012).
[49] David Thaw, *Enlightened Regulatory Capture*, 89 WASH. L. REV. (forthcoming 2014), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2298205.
[50] Nancy J. King & V.T. Raja, *What Do They Really Know About Me in the Cloud? A Comparative Law Perspective on Protecting Privacy and Security of Sensitive Consumer Data*, 50 AM. BUS. L.J. 413 (2013).
[51] Peter P. Swire, *Finding the Best of the Imperfect Alternatives for Privacy, Health IT, and Cybersecurity*, 2013 WISCONSIN L. REV. 649, 665-68.
[52] Paul Rosenzweig, *Making Good Cybersecurity Law and Policy: How Can We Get Tasty Sausage?*, 8 I/S 393 (2012).
[53] Peter M. Shane, *Cybersecurity Policy as if "Ordinary Citizens" Mattered: The Case for Public Participation in Cyber Policy Making*, 8 I/S 439 (2012).
[54] Hadi Asghari et al., *Security Economics in the HTTPS Value Chain*, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2277806 (2013).

Commission's recent efforts to regulate data security practices provide insufficient notice to regulated entities, running afoul of the fair notice doctrine.[55] These are all valuable contributions. However, like earlier cybersecurity work in law[56], they fail to address the core concerns of information security: confidentiality, integrity, and availability. This Article fills that gap.

Law has a vital role to play in regulating – and defining – what accuracy means for cybersecurity. Counterintuitively, legal approaches may be superior to computer science ones in addressing accuracy. The information security literature typically employs the term "integrity" to determine whether information should count as correct.[57] However, integrity has varying contours.[58] It may reflect merely that information has not been altered since it was originally stored, or it may indicate that the information originated from a particular authorized user.[59] Most broadly, it signals that the authorized user entered valid and reliable data.[60] Technological systems are adept at determining whether data has been modified since entry.[61] However, deciding whether a change is authorized or correct is necessarily external to IT systems. An authorized user may make a change she is not supposed to input, as when a fired employee continued to post to an entertainment chain's Twitter feed after her termination.[62] Or, she may make a mistake in data entry, such as when

[55] Gerard M. Stegmaier & Wendell Bartnick, *Psychics, Russian Roulette, and Data Security: The FTC's Hidden Data Security Requirements*, 20 GEO. MASON L. REV. 673 (2013).

[56] *See* Derek E. Bambauer, *Ghost in the Network*, 162 U. PA. L. REV. 1011, 1016-17 (2014) (describing second wave of cybersecurity research in law).

[57] *See, e.g.*, MATT BISHOP, COMPUTER SECURITY: ART AND SCIENCE 5-6 (2003) (defining integrity).

[58] *See, e.g.*, Peng Li, Yun Mao, & Steve Zdancewic, *Information integrity policies*, PROCEEDINGS OF THE WORKSHOP ON FORMAL ASPECTS IN SECURITY & TRUST (FAST 2003) 1, 1 (stating "the concept of integrity is difficult to capture and context dependent"), *available at* http://www.cis.upenn.edu/~stevez/papers/LMZ03.pdf; Ed Gelbstein, *Data Integrity – Information Security's Poor Relation*, 6 ISACA JOURNAL 1, 1-2 (2011) (listing various definitions of integrity and concluding "the word means different things to different people").

[59] *See, e.g.*, University of Miami Miller School of Medicine, *Confidentiality, integrity, availability (CIA)*, PRIVACY / DATA PROTECTION PROJECT (Apr. 24, 2006), http://privacy.med.miami.edu/glossary/xd_confidentiality_integrity_availability.htm.

[60] *Id.*

[61] *See, e.g.*, *Checksum Definition*, LINUX INFORMATION PROJECT (Nov. 4, 2005), http://www.linfo.org/checksum.html.

[62] Susan Adams, *Don't Fire An Employee And Leave Them In Charge Of The Corporate Twitter Account*, FORBES (Feb. 1, 2013), http://www.forbes.com/sites/susanadams/2013/02/01/dont-fire-an-employee-and-leave-them-in-charge-of-the-corporate-twitter-account/ (describing terminated employee who posted, via the firm's official Twitter account, that "the company you dearly love is being ruined" and "mass execution, of loyal employees who love the brand").

errors in building a database of Pacific Gas and Electric natural gas pipelines led to an explosion that killed eight people.[63] Evaluating whether a user is complying with her obligations as an employee[64], or using a standard to determine whether information is mistaken[65] – these are the domain of law, not computer science. Such outcomes are socially constructed, not technologically determined. Law can help cybersecurity move from a focus on integrity, a technical characteristic about data, to accuracy, a measure of whether information is both unchanged and reflects only permissible modifications. Legal and technical measures thus reinforce one another.

More profoundly, cybersecurity's dependence upon external, societal measures for key criteria such as authorization means that accuracy is socially, not technologically, constituted.[66] This is plainly a controversial proposition. To be clear, accuracy is created through social processes. That does not make it arbitrary. The data captured in information systems are a key input into this determination. This Article contends that, while empirical data influence and constrain decisions regarding accuracy, they do not have sole sway over those judgments. Sociological accounts of scientific knowledge are also only partial explanations.[67] Both cultural processes and experimentation inform the debate among physicists over whether the universe's missing mass should be explained via dark matter or

[63] Eric Nalder, *PG&E's computer system faulted for pipeline errors*, SFGATE (Feb. 13, 2011), http://www.sfgate.com/news/article/PG-E-s-computer-system-faulted-for-pipeline-errors-2459766.php.

[64] *See U.S. v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (interpreting whether employee exceeded authorized access to employer's computer system and thereby incurred liability under Computer Fraud and Abuse Act, 18 U.S.C. § 1030).

[65] *See, e.g.*, Tim Hume, *Too good to be true: New York to Hong Kong for $43*, CNN (July 23, 2012), http://www.cnn.com/2012/07/23/travel/price-error-air-fare-united/ (describing varying airline responses in honoring tickets sold too cheaply by mistake); Krystina Gustafson, *Wal-Mart response to pricing glitch not unusual, say experts*, CNBC (Nov. 7, 2013), http://www.cnbc.com/id/101180011 (discussing Wal-Mart's refusal to honor low prices generated by software error).

[66] On the positivist approach to accuracy, *see generally* EMILE DURKHEIM, THE RULES OF THE SOCIOLOGICAL METHOD (1895); ERNST MACH, THE SCIENCE OF MECHANICS (1960 ed.); C.D. Hardie, *Logical Positivism and Scientific Theory*, 47 MIND 214 (1938); *see generally* WILLIAM BECHTEL, PHILOSOPHY OF SCIENCE 17-31 (1988) (explaining logical positivism); Anjan Chakravartty, *Scientific Realism*, in THE STANFORD ENCYCLOPEDIA OF PHILOSOPHY (Edward N. Zalta, ed., 2013 ed.), http://plato.stanford.edu/archives/sum2013/entries/scientific-realism/. For critiques of the positivist approach, *see, e.g.*, MICHAEL POLANYI, PERSONAL KNOWLEDGE: TOWARDS A POST-CRITICAL PHILOSOPHY (1958); Michael Polanyi, *Life's irreducible structure*, 160 SCIENCE 1308 (1968).

[67] *See, e.g.*, DAVID BLOOR, KNOWLEDGE AND SOCIAL IMAGERY 18 (1976) (noting that "The changing meaning of empirical results provides rich opportunities for misunderstanding and misdescription").

via adjustments to how gravity works.[68] No one would accept a theory arguing that the missing matter is made of cheese. Similarly, social forces may determine whether your bank account should be debited by $100 when a skimmer removes that amount of funds, or whether the balance should remain constant.[69] If you report the transaction promptly, your liability is limited by law or contract, but you never face a loss greater than $100.[70] No one would accept as legitimate an outcome where the fraud *increased* your balance by $100,000.

This Article is the third in a series that advances an information-based theory of cybersecurity. This larger project re-orients cybersecurity theory away from infrastructure and towards information – it concentrates on what flows through the pipes, rather than the pipes themselves.[71] This new approach rejects existing methodologies that are grounded in long-established, but poorly fitting, doctrines such as criminal law, international law, and the law of armed conflict.[72] The information-based framework articulates three core principles: access, alteration, and accuracy.[73] Access and alteration have both positive and negative ranges. The positive aims to ensure authorized users can reach and change data. The negative seeks to prevent unauthorized ones from doing so. This Article explores the third principle by addressing the difficult challenge of accuracy in cybersecurity.

The core claim of this Article is that accuracy is socially constructed, in cybersecurity as well as in law. What counts as correct inevitably depends upon context. This proposition is highly controversial for cybersecurity, but the Article contends it is unavoidable. It also argues that regulatory proposals for addressing accuracy should emerge from a process styled on the common law, where regulators begin with a set of principles that they apply on a case-by-case basis to develop a body of useful, tailored guidelines. Where greater accuracy is necessary for a given cybersecurity context, regulators should employ a mixture of funding and mandates to drive deployment of technological measures that will achieve that end.

[68] *See, e.g.*, J.P. Ostriker & P. Steinhardt, *New Light on Dark Matter*, 300 SCIENCE 1909 (2003) (dark matter); J.R. Brownstein & J.W. Moffat, *The Bullet Cluster 1E0657-558 evidence shows modified gravity in the absence of dark matter*, 382 MONTHLY NOTICES OF THE ROYAL ASTRONOMICAL SOCIETY 29 (2007) (modifications to gravitational theory).

[69] 15 U.S.C. § 1693g(a) (limiting consumer liability in debit card transactions).

[70] *Id. See infra* Section III.A.

[71] Bambauer, *supra* note 5, at 621-28.

[72] *Id.* at 591-98; *see generally* Bambauer, *supra* note 56.

[73] These are fundamental concepts for computer science and engineering. *See, e.g.*, U.S. DEP'T OF HOMELAND SECURITY, NATIONAL INFRASTRUCTURE PROTECTION PLAN 103 (2006), http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf, at 108 (defining cyber security as "[t]he prevention of damage to, unauthorized use of, exploitation of, and, if needed, the restoration of electronic information and communications systems and services (and the information contained therein) to ensure confidentiality, integrity, and availability").

This Article proceeds in four further parts. Part II explores why accuracy matters, and evaluates both technical and legal methods to increase accuracy. Part III defends the contention that accuracy is not an inherent quality of information, but rather a socially constructed conclusion. Part IV proposes a common law-style approach to regulating accuracy by first launching a regime of testing, simulation, and experimentation to determine where greater and lesser accuracy-enhancing measures are needed, and then encouraging adoption of technical measures using a mixture of mandates and inducements. Part V concludes with suggestions for the further implications of this approach for cybersecurity law and policy. Fundamentally, like the well-being of the cat in Erwin Schrödinger's famous thought experiment, information is neither accurate nor inaccurate until it is observed in context.[74]

II. THE TOOLS OF ACCURACY

A. Law's Tools

To understand the role of accuracy in law, consider the Imperial Walker.

Imperial Walkers are an iconic aspect of the second *Star Wars* movie, "The Empire Strikes Back."[75] Elephantine and terrifying, they bear down on the Rebel base where Luke Skywalker, Princess Leia Organa, and Han Solo are hiding.[76] Impervious to the rebel's weapons (except, in one case, a tow cable), the Walkers overrun the Rebel defenses, forcing a retreat.[77] The Walkers remain one of George Lucas's most memorable creations.

But were they actually his creation? Lee Seiler did not think so. He sued Lucas and his film company Lucasfilm for copyright infringement.[78] Seiler claimed to have created similar creatures called Garthian Striders in 1976, four years before *Empire Strikes Back* made its debut.[79] His case had one weakness: Seiler could not produce any evidence of the Garthian

[74] *See, e.g.*, Melody Kramer, *The Physics Behind Schrödinger's Cat Paradox*, NAT'L GEOGRAPHIC (Aug. 12, 2013), http://news.nationalgeographic.com/news/2013/08/130812-physics-schrodinger-erwin-google-doodle-cat-paradox-science/ .

[75] Technically, the walkers are All Terrain Armored Transports, or AT-ATs. *See All Terrain Armored Transport*, WOOKIEEPEDIA, http://starwars.wikia.com/wiki/All_Terrain_Armored_Transport.

[76] Spencer Ackerman, *Inside the Battle of Hoth*, WIRED (Feb. 2013), http://www.wired.com/dangerroom/2013/02/battle-of-hoth/.

[77] *Id.*

[78] *Seiler v. Lucasfilm Ltd.*, 808 F.2d 1316 (1986).

[79] *Id.* at 1317.

Striders that pre-dated the movie.[80] Instead, he sought to use reconstructions of the Striders at trial to highlight their similarities to Lucas's Walkers.[81]

The trial judge refused to permit Seiler to introduce the reconstructions into evidence.[82] Under Rule 1002 of the Federal Rules of Evidence, one must introduce the original of a writing to prove its content.[83] Since Seiler's drawings counted as writings, and since he could not produce the originals, his case evaporated.[84] Even if Seiler's reconstructions were perfect duplicates of the works he claimed to have produced in 1976, the legal system refused to treat them as accurate.[85]

Law has an obvious concern for accuracy and deploys a wide range of doctrinal and procedural mechanisms to enhance it. For example, as in Seiler's case, the rules of evidence police the admission of information into a trial, screening out the irrelevant and incorrect.[86] The Federal Rules of Evidence require that evidence be authenticated before it can be considered by the finder of fact.[87] Authentication applies to all forms of evidence save live testimony.[88] The party seeking to introduce the evidence must be able to prove adequately that the thing is what the party claims it to be.[89] That proof is adduced by a variety of means: testimony by a person with knowledge of the evidence, certification, self-authentication, and even sufficient age.[90]

Similarly, the best evidence rule mandates that when a party seeks to prove the content of a writing, such as a will or contract, that party must introduce the original (or a reliable duplicate) as proof.[91] The rule operates as a safeguard against document forgery and against the vagaries of memory, as compared with the relative stability of written information. The Ninth Circuit made this worry explicit in *Seiler v. Lucasfilm*: "Seiler's reconstructions were made four to seven years after the alleged originals; his memory as to specifications and dimensions may have dimmed

[80] *Id.* at 1319.

[81] *Id.* at 1318.

[82] *Id.*

[83] Fed. R. Ev. 1002; *see id.* at 1318-20.

[84] 808 F.2d at 1318-20.

[85] *Id.* at 1322.

[86] *See* Fed. R. Ev. 102 (stating that purpose of rules is "ascertaining the truth and securing a just determination").

[87] Fed. R. Ev. 901.

[88] Fed. R. Ev. 901(a); *see Cook v. Hoppin*, 783 F.2d 684, 688 (7th Cir. 1986).

[89] *See, e.g., Orr v. Bank of Am., NT & SA*, 285 F.3d 764, 773 (9th Cir. 2002).

[90] Fed. R. Ev. 901(b); *U.S. v. Landron-Class*, 696 F.3d 62, 69 (1st Cir. 2012) (testimony of person with knowledge); *U.S. v. Layne*, 973 F.2d 1417, 1422 (8th Cir. 1992) (certification); Fed. R. Ev. 902 (self-authenticating evidence); *Moore v. City of Desloge*, 647 F.3d 841, 848 (8th Cir. 2011) (arrest warrant with seal is self-authenticating); *George v. Celotex Corp.*, 914 F.2d 26, 30 (2d Cir. 1990) (ancient document).

[91] Fed. R. Ev. 1002.

significantly… [and] reconstructions made after the release of the Empire Strikes Back may be tainted, even if unintentionally, by exposure to the movie."[92]

Accuracy of evidence, though, is not absolute, and does not trump all other values in the trial system. Indeed, the rules of evidence are pragmatic. Authentication – proving that an item of evidence is what it is claimed – is a relative measure. The role of the court is to evaluate whether authentication meets evidentiary minima, not to make an absolute determination.[93] If authentication surpasses that minimum, the evidence is introduced, and the court leaves it to the finder of fact to assess its ultimate accuracy.[94]

Similarly, the best evidence rule at times excuses production of writings, and accepts less reliable forms of proof of their content. If the writing has been lost, through no fault of the party seeking to use its content, the rules of evidence permit other forms of proof rather than precluding introduction of the information.[95] Where the writing is either non-critical to the matter at issue, or simple and straightforward, courts will often excuse production by labeling it "collateral."[96]

Law also employs a set of techniques to force the recording and preservation of information, against the risk that it may be lost, degraded, or maliciously altered. Certain promises and bargains must be placed in writing to become legally enforceable. The Statute of Frauds requires, for example, that contracts treating valuable obligations (such as interests in real property[97], or goods valued at more than $500[98]) or involving the assumption of risky obligations (such as marriage, surety, duration of more than one year, or assumption of estate debt by an executor[99]) be embodied in written, signed form. Transfers of ownership in a copyright must also be in writing, and signed by the owner of the rights conveyed.[100] To assign a patent, or an exclusive right in one, the owner must create a written instrument setting down the transaction.[101] Recording statutes create incentives to memorialize transfers of land by placing copies of deeds with

[92] 808 F.2d at 1320.

[93] *See* Fed. R. Ev. 104(a); *see generally Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574 (1986).

[94] *See* David S. Schwartz, *A Foundation Theory of Evidence*, 100 GEO. L.J. 95, 107-110 (2011).

[95] Fed. R. Ev. 1004(1).

[96] Fed. R. Ev. 1004(4).

[97] *See, e.g.,* N.Y. Gen. Oblig. L. § 5-703 (2013).

[98] *See, e.g.,* U.C.C. § 2-201.

[99] *See, e.g.,* N.Y. Gen. Oblig. L. § 5-701 (2013).

[100] 17 U.S.C. § 204(a).

[101] 35 U.S.C. § 261.

local government officials (typically a Recorder of Deeds).[102] While recording a deed is not mandatory, landowners risk loss of title if they fail to do so and a later purchaser buys the property without knowledge of the earlier purchaser.[103] The recording statutes specify characteristics that a deed must possess to be recorded, such as being signed by the grantor, identifying the grantee, and describing the property.[104] Information-preserving incentives generated by the recording statute thus accrue not only to notice of the deed itself, but to details about the transaction and the affected property.

However, data is not determinative. The legal system does not always assign rights and duties based upon recorded information. Courts in particular will, at times, alter the outcome dictated by recorded evidence to achieve the outcome they regard as normatively desirable. For example, contract law may enforce promises via promissory estoppel that fail technical requirements if the alternative outcome appears unjust.[105] The parties may have agreed to most, but not all, of the key details of a transaction, leading one side to rely on the understanding and suffer as a result.[106] Similarly, when parties fail to follow copyright's rules for assigning an interest in writing, courts may imply an oral, non-exclusive license that gives both sides something of value. A colorful example involves "The Stuff," a horror movie operating on the premise that a new frozen dessert craze is, in fact, made from alien creatures that take over the minds of unfortunates who eat it.[107] Director Larry Cohen needed special effects footage for several scenes, and hired Effects Associates to produce them for just over $62,000.[108] Their agreement neglected to treat copyright ownership.[109] Effects Associates generated the footage, but Cohen disliked the quality of their work, and unilaterally cut their pay.[110] The special effects studio sued.

The dispute posed a quandary: if the studio had transferred copyright in the footage to Cohen, then their federal claim (and opportunity to collect significant damages under the Copyright Act) would vanish.[111]

[102] *See* Johnson, *supra* note 42.

[103] *See, e.g.*, *Chrysler Credit Corp. v. Burton*, 599 F. Supp. 1313, 1318 (M.D.N.C. 1984); Mass. Gen. L. § 183-5.

[104] *See, e.g.*, Mass. Gen. L. § 183-6.

[105] § 90, Restatement of Contracts (Second). The classic case is *Hoffman v. Red Owl Stores*, 133 N.W.2d 267 (1965); *see also Barnes v. Yahoo!*, 565 F.3d 560 (9th Cir. 2009).

[106] *Hoffman*, 133 N.W.2d.

[107] *See The Stuff*, IMDB, http://www.imdb.com/title/tt0090094/.

[108] *Effects Assocs. v. Cohen*, 908 F.2d 555, 555-56 (9th Cir. 1990).

[109] *Id.* at 556.

[110] *Id.*

[111] 17 U.S.C. § 501(b) limits standing to sue for infringement to the owner of an exclusive right under a copyright. Had there been a transfer, Effects Associates would no longer own any of the exclusive rights in the footage.

But if they did not transfer the right to use the footage, then Cohen would have paid roughly $56,000 for what amounted to a lawsuit.[112] The Ninth Circuit cut the knot, deciding that Effects Associates had granted Cohen a non-exclusive license, enabling him to use the footage, and allowing the studio both to sue for breach of contract and to permit others to use the shots.[113] Even though the recorded information was insufficiently accurate to constitute a binding contract for a transfer, the court worked around the requirements to construct what it saw as the socially desirable result.

Law is particularly attentive to implementing technical measures that augment accuracy, such as specifying transactional form or requiring recordation, in 3 sets of circumstances: sizable consequences, effects on third parties (externalities), and risks of strategic behavior. These zones, derived from long experience, can and should guide cybersecurity policy on when to employ greater technological measures for accuracy.

The legal system often seeks to heighten accuracy through technical means when the consequences of inaccuracy seem significant. For example, attorneys must obtain waivers in writing from clients if they seek to represent a party who raises a professional or ethical conflict.[114] Under the Federal Truth In Lending Act, a credit card agreement must record, and prominently disclose to consumers, the rates, fees, and grace period for the card.[115] The information is standardized across providers and must appear in the "Schumer box," which specifies details down to font size.[116] Similar provisions apply to payday loans, which often have high annual percentage rates of interest.[117] State Statutes of Frauds typically require that contracts above a certain value be captured in writing, along with agreements to assume the debt of another.[118] Agreements to waive certain consumer protections, such as the warranty of merchantability or the warranty of fitness for a particular purpose, must be disclosed explicitly in the contract and must generally be conspicuous.[119]

[112] 908 F.2d at 559 (noting that "To hold that Effects did not at the same time convey a license to use the footage in 'The Stuff' would mean that plaintiff's contribution to the film was 'of minimal value,' a conclusion that can't be squared with the fact that Cohen paid Effects almost $ 56,000 for this footage").

[113] *Id.*

[114] R.1.7(b)(4), Am. Bar Ass'n, *Model Rules of Prof'l Conduct* (requiring that "each affected client gives informed consent, in writing").

[115] 12 C.F.R. § 226.5a(a)(2).

[116] *See, e.g.,* 12 C.F.R. § 226.5a(b)(1); *but see* Tim Chen, *The "Schumer Box" is Flawed*, FORBES (Oct. 28, 2010), http://www.forbes.com/sites/moneybuilder/2010/10/28/the-schumer-box-is-flawed/.

[117] 65 FED. REG. 17129, 17131 (Mar. 31, 2000).

[118] *See, e.g.,* N.Y. Gen. Oblig. L. §§ 5-701, 5-703 (2013).

[119] U.C.C. § 2-316(2); *but see* U.C.C. § 2-316(3)(a) (describing generalized language sufficient to disclaim implied warranties).

Sometimes, these requirements are expressed through technological means. For example, program trading caused unexpected market volatility in 1987 and 1989, leading the New York Stock Exchange to voluntarily institute trading curbs (also known as circuit breakers), which temporarily halt trading of stocks under certain conditions of high volatility.[120] The Exchange, with permission from the Securities and Exchange Commission, recently reworked these Rule 80B curbs to better respond to high-speed trading and to more accurately calibrate criteria for market-wide trading halts.[121] The new "limit up, limit down" system will apply to all stock exchanges under SEC jurisdiction, and prevents stocks from trading outside a prescribed range when the curbs are triggered.[122] The curbs are designed to enhance accuracy by enabling traders to react more carefully to additional or new information.[123] However, the circuit breakers achieve this end at the cost of counting some information – trades that are recorded during the curbs, but that violate its rules – as inaccurate.[124] An investor may receive information that she has successfully sold a stock, only to learn later that the trade has been disallowed.

Law also shows heightened attention to the effects of inaccuracy on third parties. Real property doctrine or statutes often specify that transactions in land be publicly recorded to protect third-party interests.[125] For example, judgments against real estate that create liens must typically be recorded, at peril of having the judgment deemed unenforceable against unknowing purchasers.[126] Trademark law has a similar provision.[127] This prevents innocent buyers from purchasing a parcel that is worth less than they believe, since someone else has prior claim to its value. (It also prevents strategic behavior, discussed below, by both judgment holders and landowners. Landowners may attempt to transfer the property without disclosing the lien. Judgment holders may fail to disclose the debt in the hope that a more solvent party will purchase the parcel.) Similarly, copyright law has statutory mandates for recording that protect third parties – specifically, people who may inadvertently infringe. For example, a

[120] *See* NYSE Euronext, *Circuit Breakers*, https://usequities.nyx.com/markets/nyse-equities/circuit-breakers.

[121] Securities and Exchange Commission, Release No. 34-68784, https://www.sec.gov/rules/sro/nyse/2013/34-68784.pdf.

[122] Bob Pisani, *New Trading Curbs: Limit Up, Limit Down is Finally Here*, CNBC (Apr. 4, 2013), http://www.cnbc.com/id/100617758.

[123] NYSE Euronext, *supra* note 120.

[124] Pisani, *supra* note 122 (criticizing the "old single-stock circuit breakers" that resulted in "many erroneous trades that needed to be canceled").

[125] Johnson, *supra* note 42; *see, e.g.,* Mass. Gen. L. § 183-5.

[126] *See, e.g.,* Mass. Gen. L. § 254-7(a); *J&W Wall Sys. v. Shawmut First Bank & Trust Co.*, 413 Mass. 42 (Mass. 1992).

[127] 15 U.S.C. § 1060(a)(4).

copyright owner must promptly register her work with the U.S. Copyright Office to obtain statutory damages (which can be sizable) or attorney's fees.[128] Someone who wants to make use of a work of authorship can therefore check the Copyright Office's files to ascertain whether that work is definitively copyrighted. If there is no record, she faces actual damages, which the copyright owner must prove, rather than statutory ones.[129] And unless the copyright owner has also affixed notice of copyright to copies or phonorecords of the work, the potential infringer can mitigate damages based on an innocent infringement defense.[130] Lastly, trademark law requires that quality control provisions be captured in licenses to use a mark, as a means of safeguarding against unrestricted use that could result in injury to consumers who expect products or services of a certain quality, but are duped.[131] Failure to include such safeguards, which seek to protect the accuracy of informational signals from marks, can result in a naked license that destroys trademark rights.[132]

Finally, law requires formalities and safeguards to guard against strategic behavior. For example, many states require that a will be executed in front of two disinterested witnesses.[133] Alternatively, a handwritten or holographic will generally does not require any witnesses; it is self-attesting.[134] Similarly, the signature of the testator usually must come at the end of the text, as a signal that this is the point where accurate information stops.[135] All three of these techniques aim to prevent the alteration or wholesale creation of inaccurate provisions in the will. Normally, the best source of information about the testator's intent for devising her property – the testator herself – is dead at the time when questions of accuracy arise. This is likely also the point where beneficiaries – or people excluded from

[128] 17 U.S.C. § 412(1).

[129] 17 U.S.C. § 412; 17 U.S.C. § 504(b).

[130] 17 U.S.C. §§ 401(d), 402(d) (describing evidentiary role of notice); 17 U.S.C. § 504(c)(2) (describing reduction of statutory damages); but see Pamela Samuelson & Tara Wheatland, *Statutory Damages in Copyright Law: A Remedy in Need of Reform*, 51 WM. & MARY L. REV. 439, 474-75 (2009) (describing dearth of cases where damages reduced for innocent infringers).

[131] *See* 15 U.S.C. §§ 1055 (providing that trademark use by related companies accrues to benefit of mark owner, unless "such mark is not used in such manner as to deceive the public"), 1127 (defining "related company" to mean "any person whose use of a mark is controlled by the owner of the mark with respect to the nature and quality of the goods or services on or in connection with which the mark is used").

[132] *See, e.g., Freecyclesunnyvale v. Freecycle Network*, 626 F.3d 509 (9th Cir. 2010).

[133] *See, e.g.,* Tex. Probate Code § 59(a) (requiring that "Every last will and testament… [must] be attested by two or more credible witnesses").

[134] *See, e.g.,* Ca. Probate Code § 6111(a) (holding that a will "is valid as a holographic will, whether or not witnessed, if the signature and the material provisions are in the handwriting of the testator").

[135] *See, e.g.,* Fl. Stat. § 732.502(1)(a)(1) (requiring that "The testator must sign the will at the end").

that status – learn what they will or won't receive. This is the point where they may be tempted to cheat.[136] By specifying how information about bequests must be recorded, probate law makes it costly and difficult to game the system. Absent these precautions, accuracy would likely decrease, as disappointed parties sought to alter or replace the testator's document with their own provisions.

Similarly, contract law has adopted protections against gaming. Perhaps the most well-known is the parol evidence rule.[137] In its strong form, the parol evidence rule forces parties to record in writing all of the terms of their bargains, on pain of having external or extrinsic terms rendered unenforceable.[138] Even in its weaker variant, the common law rule requires that a party show that the contract is either only partially integrated or ambiguous to introduce extrinsic evidence.[139] The rule's object is to increase accuracy by capturing the bargain's terms in more stable form, and by preventing self-serving testimony (or outright fraud) at a later time.[140] The interpretive maxim *contra proferentem* plays a similar role: when an adjudicating court confronts two interpretations of an ambiguous term, the maxim leads the judge to select the one less favorable to the drafting party.[141] The rule attempts to reduce strategic ambiguity – that is, to increase accuracy – by forcing the party capturing the bargain's terms to explain them sufficiently.[142] Otherwise, that party might leave the provision vague, hoping to convince the other side to agree to a deal it did not fully understand, or to persuade a court that the term meant something favorable

[136] *See, e.g., Fowler v. Stagner*, 55 Tex. 393, 398 (Tex. 1881) (stating that the "policy of the statute is to prevent frauds, imposition or deceit, by providing that these dispositions of property, usually made in ill-health or at the near approach of death, and under circumstances peculiarly liable to imposition, shall be fairly made in the presence of at least two wholly disinterested persons").

[137] *See generally* Peter Linzer, *Plain Meaning and the Parol Evidence Rule*, 71 FORDHAM L. REV. 799 (2002).

[138] *See, e.g., Neal v. Marrone*, 239 N.C. 73, 77 (N.C. 1953) (holding that "where the parties have deliberately put their engagements in writing in such terms as import a legal obligation free of uncertainty, it is presumed the writing was intended by the parties to represent all their engagements as to the elements dealt with in the writing").

[139] *See* Arthur Corbin, *The Parol Evidence Rule*, 53 YALE L.J. 603, 618-22 (1944)

[140] *See, e.g., W.W.W. Assocs. v. Giancontieri*, 77 N.Y.2d 157, 162 (N.Y. 1990) (stating that rule's goal is "safeguarding against fraudulent claims [and] perjury").

[141] *See* § 206, Restatement (Second) of Contracts; *Mastrobuono v. Shearson Lehman Hutton*, 514 U.S. 52, 62-63 (1995).

[142] § 206, Restatement (Second) of Contracts, cmt a (stating rationale for rule as that "Where one party chooses the terms of a contract, he is likely to provide more carefully for the protection of his own interests than for those of the other party. He is also more likely than the other party to have reason to know of uncertainties of meaning. Indeed, he may leave meaning deliberately obscure, intending to decide at a later date what meaning to assert").

rather than unfavorable.[143] Thus, where law anticipates potential strategic behavior by participants, it often adopts technical measures aiming to reduce gaming.

Accuracy is a core concern for the legal system. Law utilizes a set of technical and procedural rules to enhance this quality – techniques that have counterparts in cybersecurity and computer science.

B. Cybersecurity's Tools

Imagine you and a friend are deep into a hotly-contested game of chess. Suddenly, the cat leaps onto the table, knocking over and scattering the pieces. You want to finish the game, but how to reconstruct the board? Both you and your friend likely remember at least some of the positions, but are you fully confident in the perfection of your memory, or of that of your friend? Might one of you, even acting in good faith, tend to remember a board slightly more favorable to your position? Or should you simply start anew?

Serious chess players tend to keep a history of each game using a notation system that abbreviates movements by pieces on both sides.[144] With a list of moves, you can resolve the cat-based crash quite simply: reset the pieces to a clean board, and replay the listed moves in order. In this simplified example, there is no contention about the validity of the notations themselves, but if cheating were a concern, you could accept a notation as valid only if, for example, it were countersigned by the opposing player. Logging the game's moves has benefits beyond recovery. Perhaps you were unsure about surrendering a rook. With the list, you can recover to the positions just before that move, and then try a different tactic, exploring its effects.[145]

Computer science has long been concerned with accuracy of information, typically under the rubric of "integrity."[146] In part, this is because computer systems themselves are not always reliable custodians of data: disks fail physically, systems crash before committing changes to those disks, software errors inadvertently modify information, and so on.[147]

[143] *Id.*

[144] *See Understanding Chess Notation*, CHESS FOR DUMMIES, http://www.dummies.com/how-to/content/understanding-chess-notation.html.

[145] *See, e.g.*, Steve Lopez, *5 Easy Ways to Improve Your Chess Game*, CHESS CENTRAL, https://www.chesscentral.com/Easy_Improve_Chess_a/152.htm (suggesting players "Replay [their] own games and try to figure out what you did right and wrong").

[146] *See, e.g.*, Gelbstein, *supra* note 58.

[147] *See* Gopalan Sivathanu, Charles P. Wright, & Erez Zadok, *Ensuring Data Integrity in Storage: Techniques and Applications*, PROCEEDINGS OF FIRST ACM WORKSHOP ON STORAGE SECURITY AND SURVIVABILITY (2005), *available at* http://www.fsl.cs.sunysb.edu/docs/integrity-storagess05/integrity.html.

In part, the advent of new techniques, such as distributed data stores connected via the Internet, has required engineers to plan for instances where different versions of the same datum have divergent values.[148] And, in part, computer science has had to plan for malicious activity. Hackers have an interest not only in reading information, but in altering it.[149] Cybersecurity has a range of accuracy-enhancing techniques to mitigate these risks. Most prominently, these include verification methods, auditing techniques, and backup and recovery technologies.

Verification methods are used to detect problems with information. One common technique for file systems (the software component that manages storage of information on disks) is to employ checksums.[150] When saving a piece of information, the file system uses an algorithm to compute a unique mathematical value for that information, called a checksum.[151] It stores both the checksum and the information. Later, if the file system needs to access that information, it can repeat the calculation, and then compare the new checksum to the old one.[152] If they differ, the data has changed.[153] More advanced techniques use cryptographic algorithms to compute checksums, to prevent tampering[154], or store the checksum independent from the information itself, to achieve end-to-end integrity (ensuring that the data is not altered after the check, but before use)[155]. Most modern file systems employ checksums or similar techniques, but some operate more reliably than others, delivering greater accuracy.[156]

Auditing techniques allow a system (or, more accurately, its operators) to examine a record of changes made to information and, in most cases, to undo or redo those alterations. Large database systems, such as

[148] *See, e.g.*, *An Unorthodox Approach To Database Design: The Coming of the Shard*, HIGH SCALABILITY (Aug. 6, 2009), http://highscalability.com/unorthodox-approach-database-design-coming-shard; *What Is Sharding?*, SCALEBASE, http://www.scalebase.com/resources/database-sharding/.

[149] *See, e.g.*, Dan Rowinski, *SQL Injection Hacker Attacks Are On The Rise. Here's How To Defend Your Servers*, READWRITE (Oct. 10, 2012), http://readwrite.com/2012/10/10/sql-injection-hacker-attacks-are-on-the-rise-heres-how-to-defend-your-servers.

[150] *See* Gopalan Sivathanu, Charles P. Wright, & Erez Zadok, *Enhancing File System Integrity Through Checksums* (May 8, 2004), http://www.filesystems.org/docs/nc-checksum-tr/nc-checksum.html.

[151] *Id.*

[152] *See, e.g.*, Tom White, *Data Integrity*, in HADOOP: THE DEFINITIVE GUIDE (2012).

[153] It is also possible that the checksum may have been corrupted. Some operating systems store checksums redundantly to manage this problem. *See* Jeff Bonwick, *ZFS End-to-End Data Integrity*, ORACLE (Dec. 8, 2005), https://blogs.oracle.com/bonwick/entry/zfs_end_to_end_data.

[154] Sivathanu, Wright, & Zadok, *supra* note 150.

[155] Bonwick, *supra* note 153.

[156] Robin Harris, *ZFS data integrity tested*, ZDNET (Feb. 25, 2010), http://www.zdnet.com/blog/storage/zfs-data-integrity-tested/811.

IBM's Lotus Domino[157] or Microsoft's SQL server[158], typically implement this type of auditing via transaction, or write-ahead, logging[159]. When a program or user attempts to change the database, the software first creates a record of the change in a separate file (generally on a separate physical disk).[160] Once that change record is safely stored, the software implements the change to the database itself. This ensures that if the system crashes while making the change to the database, or somehow the database is later damaged or destroyed, a separate, durable record of the change exists.[161] To return to the chess analogy: you don't move a piece until you have made a notation of that move. And if the database were lost entirely, the organization running the system could restore an older version of the database, and then replay the transactions from the log to roll it forward, returning its information to the latest state.[162] Similarly, if some of the transactions were deemed inaccurate or unwanted, the restoration could move forward partially, to the point of the last known accurate change.[163] Overall, a transaction log system lets the operator replay history – and, if necessary, revise it.

Finally, backup and recovery technology helps organizations keep redundant versions of their information – typically stored separately from the active version.[164] Backups protect against loss or corruption of data, enabling restoration of information known to be accurate. And, backups can serve as archives, to meet data retention requirements or simply to provide historical records.[165] Both natural and human-generated disasters have recently reinforced the need for organizations to ensure their backup systems are effective. Indeed, the Department of Homeland Security and the Federal Emergency Management Agency advise, as part of their Ready

[157] *Transaction Logging*, IBM LOTUS DOMINO ADMINISTRATOR (Aug. 14, 2008), http://ibm.co/1nVrrXE.

[158] *The Transaction Log (SQL Server)*, MICROSOFT SQL SERVER, http://technet.microsoft.com/en-us/library/ms190925.aspx.

[159] C. Mohan & Frank Levine, *ARIES/IM: An Efficient and High Concurrency Index Management Method Using Write-Ahead Logging*, 1992 ACM SIGMOD, *available at* http://www.ics.uci.edu/~cs223/papers/p371-mohan.pdf.

[160] *Planning for Transaction Logging*, IBM LOTUS DOMINO ADMINISTRATOR (Aug. 14, 2008), http://ibm.co/1kWyYmy.

[161] *Id.*

[162] C. Mohan et al., *ARIES: A Transaction Recovery Method Supporting Fine-Granularity Locking and Partial Rollbacks Using Write-Ahead Logging*, 17 ACM TRANSACTIONS ON DATABASE SYSTEMS 94 (1992).

[163] *Id.*

[164] *See generally* Lincoln Spector, *7 Backup Strategies for Your Data, Multimedia, and System Files*, PCWORLD (Aug. 25, 2009), http://www.pcworld.com/article/170688/7_backup_strategies.html.

[165] *Id.*

Business campaign, that all IT services have a functional data backup plan.[166]

These three accuracy-enhancing technologies reinforce one another. Applications and file systems often employ mechanisms such as transaction logging to simplify backup and recovery.[167] And, as with the chess example, logging has additional benefits for accuracy. If someone accidentally (or deliberately) deletes part of the data set, those changes can effectively be reversed. This can be helpful in situations such as those where document preservation is required in response to regulatory mandates or litigation.[168]

There are limits to these technological methods – ones that highlight the need for external normative input. Determining which transactions count as inaccurate is a decision beyond the analytical scope of the system itself. So, too, are the tradeoffs – an invalid change may be followed by a set of valid ones, to the same piece of information. Discarding the invalid transaction may necessitate forfeiting the valid ones. Both law and cybersecurity share common models for making such determinations: hierarchy, and consensus

C. Hierarchy and/or Consensus

Approaches to determining which information counts as accurate share striking similarities, whether in law or in computer science. Law approaches accuracy – its construction of legal truth – via a set of processes imposed by the force of the state.[169] Cybersecurity similarly approaches accuracy via a set of processes, but imposed by the force of software code or hardware.[170] The two fields share one striking similarity, and are characterized by one important difference. The similarity is that both disciplines' methods can be reduced to one of two mechanisms: hierarchy, or consensus. This suggests that there may be ways for the two fields to synchronize – to share advances related to accuracy. Methods that rely upon hierarchy have a canonical information source whose decisions override any conflicts. Ultimately, the contents of Verisign's database determine which IP address corresponds to a particular .com domain name – and Verisign

[166] *IT Disaster Recovery Plan*, READY.GOV (Oct. 25, 2012), http://www.ready.gov/business/implementation/IT.

[167] Mohan et al., *supra* note 162.

[168] *See* Bambauer, *supra* note 71, at 641-42 (listing data retention requirements imposed by statutes).

[169] Robert M. Cover, *Violence and the Word*, 95 YALE L.J. 1601 (1986).

[170] *See* Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 509-10 (1999).

decides who is authorized to change those records.[171] Similarly, the U.S. Supreme Court decides whether restrictions upon the distribution of information about the drugs pharmacists dispense offend the First Amendment, regardless of whether the circuit courts of appeal agree or not.[172] The difference between the two disciplines is that legal methods are far more flexible. That, this Article argues, suggests that law has much to teach cybersecurity.

Hierarchy, in both law and cybersecurity, involves making decisions by ultimate recourse to an authoritative resource or entity. For example, in cybersecurity, the Domain Name System is a distributed resource; some DNS servers will cache outdated information.[173] A domain name used to map to one IP address, and now maps to a new one. Thus, a server caching the old mapping will deliver inaccurate data to any computer asking about the domain name. But the DNS has a solution. Through its delegated structure, it designates a particular server as authoritative for top-level domains.[174] If there is confusion about the IP address corresponding to arizona.edu, a querying computer can get an authoritative answer from the .edu name servers, which are maintained by Educause.[175] The system obeys: if there is a conflict between an extant DNS record for a .edu name and the one maintained by Educause, the latter triumphs.

Methods that rely upon consensus are non-hierarchical: when different sources of a piece of information disagree about its content, the contender with the most support wins. The obvious exemplar is the jury system: a small group of peers must decide between two conflicting versions of a transaction, or a car accident. Cybersecurity has similar techniques. For computer systems that use RAID mirroring (assuming there are more than two copies of the data), the information state with the greatest number of matching copies is authoritative. If a particular datum is mirrored onto four drives, three of which say its value is 0, and the other claims it is 1, the system will treat 0 as the accurate value.[176] Consensus approaches have become popular due to certain informational advantages.[177] For

[171] *See, e.g.*, Mark Jeftovic, *Verisign seizes .com domain registered via foreign Registrar on behalf of US Authorities*, EASYDNS (Feb. 29, 2012), http://blog.easydns.org/2012/02/29/verisign-seizes-com-domain-registered-via-foreign-registrar-on-behalf-of-us-authorities/.

[172] *Sorrell v. IMS Health*, 564 U.S. __ (2011); *compare IMS Health v. Sorrell*, 630 F.3d 263 (2d Cir. 2010) *with IMS Health v. Ayotte*, 550 F.3d 42 (1st Cir. 2008).

[173] *See* Ron Aitchison, PRO DNS AND BIND 10 17 (2011) (describing use of time-to-live value to manage stale data).

[174] *Technical requirements for authoritative name servers*, IANA, https://www.iana.org/help/nameserver-requirements.

[175] *See Educause*, https://net.educause.edu/edudomain/.

[176] *See* Jon L. Jacobi, *RAID Made Easy*, PCWORLD (Apr. 19, 2012), http://www.pcworld.com/article/194360/raid_made_easy.html.

[177] *See, e.g.*, JAMES SUROWIECKI, THE WISDOM OF CROWDS (2005).

example, prediction markets tend to forecast elections more accurately than polling, and averages of major polls tend to predict elections more accurately than any individual poll.[178] At times, consensus will outperform hierarchy, as in the famous case where Francis Galton averaged the guesses by fairgoers of a bull's weight and compared them to estimates by seasoned cattle dealers. The crowd's average was closer to the true mark.[179]

Cybersecurity employs both hierarchy and consensus models. Consider cash, or at least electronic commerce. Sensitive Web-based exchanges of information, such as those that take place during an e-commerce transaction, are typically protected by Secure Sockets Layer encryption.[180] Users have been trained to look for the lock icon in their browser's location bar that indicates communication with the Web site is encrypted. To keep Internet users from having to manage cryptographic keys, browser developers include root certificates for major certificate authorities when the browser is installed on a computer or mobile device.[181] When the user connects to a site that uses SSL, that site's server transmits the server's cryptographic certificate to the user's browser.[182] The certificate is signed using a certificate authority's key. The browser verifies the signature against the appropriate root certificate information in its files.[183] Secure on-line commerce thus depends upon a hierarchy: you trust Amazon.com's server because the certificate authority Verisign vouches for Amazon's SSL certificate.[184] The certificate authority's word is law for on-line encryption, which can lead to mischief if an attacker manages to subvert the authority and issue bogus certificates.[185] The public key infrastructure that undergirds on-line commerce is thus a potent example of hierarchy.

In contrast, the latest digital currency to gain popularity, Bitcoin, depends upon consensus. The Bitcoin software operates a peer-to-peer

[178] *See* Nate Silver, *Oct. 23: The Virtues and Vices of Election Prediction Markets*, FIVETHIRTYEIGHT (Oct. 24, 2012), http://fivethirtyeight.blogs.nytimes.com/2012/10/24/oct-23-the-virtues-and-vices-of-election-prediction-markets/?_r=0.

[179] *Id.* at XII.

[180] *See* Johnny Papa, *Secure Sockets Layer: Protect Your E-Commerce Web Site with SSL and Digital Certificates*, MSDN MAGAZINE (Apr. 2001), http://msdn.microsoft.com/en-us/magazine/cc301946.aspx.

[181] *What is an SSL certificate?*, GLOBALSIGN, https://www.globalsign.com/ssl-information-center/what-is-an-ssl-certificate.html.

[182] *Id.*

[183] *Id.*

[184] *Symantec Trust Network (STN) Certification Practice Statement, Version 3.8.14*, https://www.symantec.com/content/en/us/about/media/repository/stn-cps.pdf (Dec. 12, 2013). Technically, Amazon uses TLS 1.0, SSL's successor.

[185] *See supra* notes 10-13.

network.[186] Bitcoins are created ("mined") when a computer in that network is the first to solve a challenging mathematical problem.[187] When a Bitcoin is mined originally, or transferred thereafter, it updates an ownership record (the block chain) using cryptographic techniques similar to SSL.[188] However, the block chain has one critical difference: it is distributed to every computer, or node, in the Bitcoin network.[189] Verification of the creation or transfer of Bitcoins occurs via voting: if a majority of network nodes authenticate the transaction, it counts as accurate.[190] Bitcoin's design is avowedly libertarian – it is intended to remove control over the currency from any government or central bank, and places its faith in mathematics, not politics.[191] However, consensus has an ironic drawback: if a single entity can obtain control over a majority of Bitcoin nodes, it can falsify transactions, such as by spending a given Bitcoin more than once.[192] Early in 2014, the Bitcoin mining pool GHash.IO approached majority control of the nodes, generating anxiety among the currency's aficionados.[193] While GHash.IO reassured users that it did not intend to gain a majority share, the possibility highlights the potential weakness of the consensus model – especially for an anonymous currency.[194]

These two poles blur into one another: generally, there must be some consensus about the initial designation of a particular source of authority, and recourse must be had to authority to determine whose vote counts for the purpose of consensus. Thus, hierarchy and consensus are ends of a continuum, and do not exist in a vacuum – they have reciprocal, interacting effects in most cases. Nonetheless, the division, though rough, provides a useful model.

Critically, the choice between using hierarchy or consensus is driven not by technical concerns, but by normative criteria. This is easy to grasp for legal decisions. Juries vote to decide whether the state has proved a person's guilt with sufficient accuracy because they represent, in

[186] Maria Bustillos, *The Bitcoin Boom*, THE NEW YORKER (Apr. 2, 2013), http://www.newyorker.com/online/blogs/elements/2013/04/the-future-of-bitcoin.html.

[187] *Id.*

[188] Benjamin Wallace, *The Rise and Fall of Bitcoin*, WIRED (Nov. 23, 2011), http://www.wired.com/magazine/2011/11/mf_bitcoin/all/.

[189] *Id.*

[190] *Id.*

[191] Bustillos, *supra* note 186.

[192] *See* Christopher Mims, *The existential threat to bitcoin its boosters said was impossible is now at hand*, QUARTZ (Jan. 9, 2014), http://qz.com/165273/the-existential-threat-to-bitcoin-its-boosters-said-was-impossible-is-now-at-hand/.

[193] Alec Liu, *Bitcoin's Fatal Flaw Was Nearly Exposed*, MOTHERBOARD (Jan. 10, 2014), http://motherboard.vice.com/blog/bitcoins-fatal-flaw-was-nearly-exposed.

[194] GHash.IO, *Bitcoin mining pool GHash.IO is preventing accumulation of 51% of all hashing power*, https://ghash.io/ghashio_press_release.pdf.

microcosm, the collective judgment and moral weight of society.[195] In addition, the selection here between hierarchy (the judge) and consensus (the jury) reflects a deeply held commitment to constraining the power of the state to use force against its citizens.[196] The hierarchy represented by the Constitution's Supremacy Clause represents a different normative election: to place the collective interests of the United States above the interest of any one state so united.[197] The Supremacy Clause demonstrates that the larger polity holds pride of place over any of America's constituent elements, recapitulating the historical evolution from the Articles of Confederacy and its weak centralization to the Constitution and its stronger federal government.[198]

More challenging, yet revealing, is the insight that cybersecurity too picks between these models based on values that become embedded in the technological architecture. The Domain Name System, the distributed database that maps Internet protocol addresses to user-friendly domain names, is typically lauded for its technical efficiency: the decentralized model makes updating DNS records less burdensome for any individual entity.[199] More importantly, though, the DNS model encodes the cyberlibertarian ethos of the Internet's early days, and architects, into its design.[200] Responsibility is divided, and isolated: it is no concern of the administrators of google.com what those responsible for bbk.co.uk do with their subdomains.[201] As Voltaire's Candide said, everyone must cultivate

[195] *See, e.g.,* Charles R. Nesson, *Reasonable Doubt and Permissive Inferences: The Value of Complexity*, 92 HARV. L. REV. 1187, 1195 (1979).

[196] *See* Cover, *supra* note 169.

[197] *See* Henry P. Monaghan, *Supremacy Clause Textualism*, 110 COLUM. L. REV. 731, 788-96 (2010) (advancing textualist basis for broad reading of Supremacy Clause).

[198] *See, e.g.,* Max Ferrand, *The Federal Constitution and the Defects of the Confederation*, 2 AM. POL. SCI. REV. 532, 532 (1908) (stating that "the Constitution was framed because of defects in the Articles of Confederation is universally accepted"); *Gonzales v. Raich,* 545 U.S. 1, 16 (2005) (stating that "The Commerce Clause emerged as the Framers' response to the central problem giving rise to the Constitution itself: the absence of any federal commerce power under the Articles of Confederation.").

[199] *See* Verisign, *Domain Name System*, http://www.verisigninc.com/en_US/domain-names/online/domain-name-system/index.xhtml; *see generally* CRICKET LIU & PAUL ABITZ, DNS AND BIND (5th ed. 2006); WhatIsMyIPAddress, *What is the Domain Name System (DNS)*?, http://whatismyipaddress.com/dns (lauding the "highly organized and efficient nature of the DNS").

[200] *See* John Perry Barlow, *A Declaration of the Independence of Cyberspace* (Feb. 8, 1996), https://projects.eff.org/~barlow/Declaration-Final.html; David R. Johnson & David G. Post, *Law and Borders: The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996).

[201] *See* Jim Boyce, *Understanding how DNS works, part 2*, TECHREPUBLIC (Sept. 14, 2000), http://www.techrepublic.com/article/understanding-how-dns-works-part-2/# (noting that a "benefit to delegation is that it makes possible the decentralization of the DNS name space… [a] subdomain can manage its own portion of the name space and the records that go along with it.").

their own garden.[202] The decision to decentralize power has technical benefits, but it was initially and ultimately a political act.

Similarly, the Federal Bureau of Investigation's National DNA Index System (NDIS) is a centralized database that holds DNA profiles submitted by crime laboratories at the national, state, and local levels.[203] Here, too, centralization is often lauded on efficiency grounds; it is easier to have a single database to query rather than working with a welter of repositories with different requirements and interfaces.[204] This account, however, overlooks a value choice that drives the system: empowering law enforcement, almost exclusively. This orientation can be discerned by the differential access entities have to the database. Law enforcement officials have ready access to query the data, which is helpful – dozens of cold cases have been solved by matching crime scene DNA against NDIS profiles.[205] Defendants, however, have a much more difficult path, especially post-conviction, if they wish to use the data to demonstrate their innocence (and even someone else's likely guilt).[206] Only a handful of states have authorized post-conviction searches, and even when a search is authorized, it may be blocked by FBI database administrators.[207] Moreover, the legislation authorizing the database defers to the FBI for certain decisions, such as which law enforcement agencies may access the data, or add to it.[208] The FBI chose to mandate that agencies limit access to the DNA profiles they control as a condition of access – and required that they undergo annual audits to ensure compliance with the Bureau's rules.[209] Use of the database is tilted heavily towards law enforcement, and away from defendants – even those with highly plausible claims of innocence. That is a normative choice embedded in a centralized database under FBI control. A decentralized system that permits queries across all data stores (such as the Food and Drug Administration's Mini-Sentinel system) would likely

[202] VOLTAIRE, CANDIDE (1759) ("I also know, said Candide, that we must cultivate our own garden") (translation by author).

[203] Federal Bureau of Investigation, *Frequently Asked Questions (FAQs) on the CODIS Program and the National DNA Index System*, http://www.fbi.gov/about-us/lab/biometric-analysis/codis/codis-and-ndis-fact-sheet.

[204] *See, e.g.,* Natalie A. Bennett, *Note: A Privacy Review of DNA Databases*, 4 I/S 816, 821 (2008). In addition to NDIS, the FBI also maintains the Combined DNA Index System (CODIS), which provides a single interface to a hierarchy of state and local DNA databases. *Id.*

[205] Jason Kreag, *Letting Innocence Suffer* 8-14 (manuscript on file with author).

[206] *Id.* at 18-22.

[207] *Id.* at 22-27.

[208] 42 U.S.C. § 14131.

[209] 42 U.S.C. § 14132(b)(3); FBI LABORATORY, NATIONAL DNA INDEX SYSTEM (NDIS) OPERATIONAL PROCEDURES MANUAL 7-10 (Jan. 31, 2013), http://static.fbi.gov/docs/NDIS-Procedures-Manual-Final-1-31-2013-1.pdf.

provide more variegated access to defendants, and hence inherently embody a more balanced ethos regarding prosecution versus defense.[210]

Furthermore, the FBI imposes strict criteria on uploading profiles to the database – criteria that prioritize law enforcement needs. As Jason Kreag documents, the Bureau only allows certain DNA profiles to be added to NDIS.[211] DNA found at a crime scene may be added only if it is attributable to a perpetrator and not a victim. Partial profiles may be uploaded only if the probability of a random match is extraordinarily remote.[212] Profiles from small samples of DNA are prohibited.[213] The FBI prizes a high degree of reliability in the DNA data over a larger sample size. Either might be construed as accurate: a greater degree of certainty in a match, or a greater probability of making a match. The FBI chose the one that points towards meeting the prosecution's burden in a criminal trial.

While there are technical aspects to centralized versus distributed models, such as resilience and efficiency, at base the choice between hierarchy and consensus comes down to normative preferences for a single source of authority that can be stoutly protected or a multitude of voices where it is costly to co-opt a sufficient share.[214] The shared orientation towards either hierarchy or consensus provides a path for dialogue between law and cybersecurity. Where one doctrine faces a similar values-based choice, decisions from the other may be a useful guide.

III. CONSTRUCTING ACCURACY

A. The Casino and the Skimmer

Accuracy, in both law and cybersecurity, is a socially constructed characteristic. For law, this claim is not particularly controversial after the Legal Realist movement.[215] Decisions in cases result from complex, political processes, rather than being divined by judges from pre-existing Platonic natural law.[216] Agency rulemaking emerges from a welter of

[210] On Mini-Sentinel, *see* Bambauer, *supra* note 56, at 40-41.
[211] *Id.* at 10.
[212] *Id.* (noting that submitting law enforcement agency must show that odds of a random match probability of the profile are 1 / (number of profiles in the database)).
[213] *Id.*
[214] *Cf.* Bambauer, *supra* note 274, at 1 (quoting Isaiah Berlin, "the fox knows many things, but the hedgehog knows one big thing").
[215] *See* Oliver Wendell Holmes, *The Path of the Law*, 10 HARV. L. REV. 457 (1897); Felix Cohen, *Transcendental Nonsense and the Functional Approach*, 35 COLUM. L. REV. 809 (1935); DAVID ROSENBERG, THE HIDDEN HOLMES: HIS THEORY OF TORTS IN HISTORY (1995).
[216] *See* THE THEORY OF PUBLIC CHOICE – II (James M. Buchanan & Robert D. Tollison, eds., 1984); Green, *supra* note 33.

warring interest groups, administrative aggregation of power, and political goals, rather than from carefully rational policy analysis.[217] For cybersecurity, though, this contention is controversial, perhaps even scandalous. This Article spent some time describing techniques available to computer science to safeguard accuracy. It seems contradictory to suggest that accuracy is a social creation rather than a technological one. This Section defends the notion of accuracy as the output of social processes, rather than a pre-existing state of being. It draws upon work in the philosophy and sociology of science that attempted a similar shift – concentrating attention on the ways in which science and technology are path-dependent, culturally encoded, and socially determined. The Section identifies decisions about accuracy as, fundamentally, questions of power.

Consider the balance in your bank account. Your bank keeps careful track of transactions in the account: withdrawals, deposits, fees, and so forth. If you take $100 out of your account via ATM, and lose it at the casino, the bank may sympathize with your conviction to draw on 17, but it will not replenish your account for your losses.[218] The ATM keeps a record – your debit card and PIN were presented, and $100 was withdrawn.[219] As a result, the account is $100 poorer. The bank is confident in this information: the account was yours, and not your neighbor's; the amount taken out in cash was $100, not $1000. Even you, though perhaps regretting the ready availability of cash withdrawals, probably concede the accuracy of the bank's data.

Imagine instead that a thief has managed to skim your card and password.[220] The thief, too, withdraws $100, goes to the casino, and fares poorly at blackjack. As before, your funds have gone from your account to the casino's cash drawer. At the recordkeeping level, the two situations look the same to the bank: correct credentials, followed by money withdrawn. The bank thinks you are now in the hole by $100. Yet federal law requires the bank to cut your losses (unlike the casino). If you report unauthorized transactions within two days of learning about the hack, your maximum liability is $50.[221] Certainly, you would not view the bank's records as

[217] *See, e.g.*, Susan Webb Yackee, *Sweet-Talking the Fourth Branch: The Influence of Interest Group Comments on Federal Agency Rulemaking*, 16 J. PUBLIC ADMIN. RESEARCH & THEORY 103 (2006); Sidney A. Shapiro & Rena Steinzor, *Use and Abuse of Information: Capture, Accountability, and Regulatory Metrics*, 86 TEX. L. REV. 1741 (2008);

[218] *See* Kenneth R. Smith, *Casino Blackjack: Rules of the Game*, BLACKJACKINFO, http://www.blackjackinfo.com/blackjack-rules.php.

[219] *See generally* MasterCard, *Transaction Processing Rules* 7-5 – 7-6 (Dec. 13, 2013), https://www.mastercard.com/us/merchant/pdf/ORME-Entire_Manual.pdf.

[220] Federal Bureau of Investigation, *Taking a Trip to the ATM? Beware of Skimmers*, http://www.fbi.gov/news/stories/2011/july/atm_071411 (July 14, 2011).

[221] 15 U.S.C. § 1693g(a). If you tarry, and wait longer (but less than 60 days), your maximum exposure is only $500. *Id.*

correct at the moment of withdrawal – there is nothing wrong with its record-keeping, but the transaction ought not to count against you. Federal banking law agrees.[222] The bank's data is now inaccurate.

In both situations, the *integrity* of the bank's data is unquestioned: someone withdrew $100 from your account by using your PIN and debit card. When that someone is you, the data is accurate, as well as having integrity. If that someone is a third party, operating without your authorization, the data may be accurate or inaccurate. That quality of the information changes depending on how you behave after the skim.[223] Wait too long, and the bank's records go from uncertain to accurate, as you bear the loss.[224] Report quickly, and the data is inaccurate; your account is topped up.

It may be optimal to have banks bear the risk of fraud or hacking rather than consumers. Perhaps this liability scheme is simply the result of interest group lobbying, and precautions would be superior if customers absorbed this risk.[225] But regardless of the best allocation of risk, note the divergence between how the transactional record views your account in the two scenarios versus how the law, and hence society at large, does. We have made a collective decision to override the trail of withdrawals made with your card and credentials in some cases, even where the integrity of that trail is not in doubt. Accuracy derives from a fluid process that mixes banking law, recorded data, and your actions to arrive at a result that cannot be correctly predicted ahead of time. Accepting volition rather than possession as the key criterion may make sense, but it is a social choice – it prioritizes one set of information (that reflecting the account holder's subjective intent) over another (that reflecting the objective manifestations of authorization via card and PIN).

Law and cybersecurity are mutually engaged in a process of meaning-making that results in accuracy. Changes in either can alter the outcome. Law could adopt a different position on transactions that occur without the account holder's authorization – it could force the holder to bear

[222] *See generally* Fed. Trade Comm'n, *Lost or Stolen Credit, ATM, and Debit Cards* (Aug. 2012), http://www.consumer.ftc.gov/articles/0213-lost-or-stolen-credit-atm-and-debit-cards.

[223] 15 U.S.C. § 1693g(a); *see* Danielle Douglas, *Why you should keep that debit card at home*, WASH. POST. (Feb. 6, 2014), http://www.washingtonpost.com/blogs/wonkblog/wp/2014/02/06/heres-why-you-should-keep-your-debit-card-at-home/.

[224] *Id.*

[225] *Cf.* Alan Schwartz, *The Case Against Strict Liability*, 60 FORDHAM L. REV. 819 (1992) (describing liability regime where consumers purchase first-party insurance against residual risk); Adam J. Levitin, *Priceless? The Economic Costs of Credit Card Merchant Restraints*, 55 UCLA L. REV. 1321, 1381 (2008) (noting that "Most state no-surcharge rules are apparently the result of the credit card industry lobbying in the 1980s, when it was uncertain whether the federal surcharge ban would be renewed after it lapsed").

some, all, or none of the charges, or could condition that result upon certain behavior. Cybersecurity could capture additional information during the transaction to contribute to the analysis, such as by requiring biometric identification (a thumbprint, a retinal scan) that further limits the capacity for transactions by someone other than the account holder.[226] For accuracy, though, neither law nor technology is determinative. Without records of your account and associated transactions, banking law has nothing upon which to operate. And cybersecurity requires rules – generated by law and embedded in the logic of software code – to sort which transactions count. The process is not unbounded on either side; as with all social mechanisms, there are constraints. For example, when Congress crafts rules regarding unauthorized use of debit cards, it could plausibly place the liability on either party, in part or in whole. Less plausibly, it could impose the loss on both (perhaps by forcing the account holder to pay a fine equal to the loss). But it would be quite implausible for financial regulation to impose a penalty of ten times the loss on either party, or to assign liability randomly. As both law and cybersecurity shape accuracy, they each constrain the range of outcomes perceived as reasonable and justified.

B. Skepticism

Cybersecurity is likely to resist the argument that accuracy is a socially constructed quality. Treating integrity as an inherent quality of the stored data has a long history, and engineers are reluctant to re-examine the concept.[227] When moving from simple definitions of integrity to more advanced ones that consider authorization and correctness, cybersecurity operates in technical terms, not social ones. Authorization is mediated by code, which dictates what actions a user or program can take with data.[228] Even researchers who recognize the limits of an access control model typically fall back to technical fixes that attempt to define accuracy via code-based techniques such as integrity labeling.[229]

[226] Walt Disney World, for example, uses fingerprint scans to ensure that patrons do not share tickets, or re-sell them in secondary markets. Cory Doctorow, *Fingertip biometrics at Disney turnstiles: the Mouse does its bit for the police state*, BOINGBOING (Mar. 15, 2008), http://boingboing.net/2008/03/15/fingertip-biometrics.html.

[227] *See, e.g.*, Vicente Aceituno, *Give up confidentiality, integrity and availability*, SC MAGAZINE UK (May 28, 2013), http://www.scmagazineuk.com/give-up-confidentiality-integrity-and-availability/article/294730/ (describing resistance to change).

[228] *See, e.g.*, *Protecting Data Within the Database*, ORACLE SECURITY OVERVIEW 10G RELEASE 1 (10.1), http://docs.oracle.com/cd/B14117_01/network.101/b10777/protdata.htm (stating "Authorization is permission given to a user, program, or process to access an object or set of objects").

[229] *See* § 7.2, Peng Li, Yun Mao, & Steve Zdancewic, *Information integrity policies*, PROCEEDINGS OF THE WORKSHOP ON FORMAL ASPECTS IN SECURITY & TRUST (FAST 2003) 1, 1 (stating "the concept of integrity is difficult to capture and context dependent"

But code alone won't suffice. Concepts such as authorization, even if cleanly binary as a technological matter, blur into shades of gray once people enter the system. Congress revised the Computer Fraud and Abuse Act to reflect this reality.[230] Hacking by outsiders, who lacked authorization to access a computer system, was not the only threat. Insider attacks, such as by employees who exceeded authorization, were at least as dangerous. When authorization was simply a matter of code, decisions were easier. Once the CFAA covered activity by users with permission to interact with the system and data, though, the case law grew muddied. For example, courts disagreed over whether it was a CFAA violation to continue to use a computer system in violation of contractual terms of use[231], and over whether employees transgressed the statute if they acted for their own ends rather than their employer's benefit[232]. Some scholars, such as Orin Kerr, have argued that this approach is untenable, and that legal definitions of authorization ought to mirror technological ones.[233] On this view, a violation of the statute ought to require crossing a cybersecurity barrier, not merely a contractual or agency one. At present, though, most courts disagree[234], and even ones that take a more jaundiced view of CFAA liability have left room for more contextual definitions of authorization, such as via terms of access agreements[235]. Law may be imposing an undesirable scope of authorization for the CFAA. However, law plainly has a vital role to play in charting authorization's uncertain path.

As legal scholarship has long recognized, social processes define what arguments and methodologies count as relevant. That means, then, that accuracy is ultimately about power: who decides legitimacy, and how? Power may be based in government. Congress may pass laws requiring a

and noting that "Depending upon the context of the application, the integrity of the data may have very different meanings. Nevertheless, they all require some property of the data… such properties must be computable, so that given a specific value, we can decide whether it is good or bad"), *available at* http://www.cis.upenn.edu/~stevez/papers/LMZ03.pdf.

[230] *See* Orin Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1615-16 (2003).

[231] *Compare U.S. v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009) (acquitting defendants accused of CFAA violations) *with U.S. v. John*, 597 F.3d 263, 271 (5th Cir. 2010) (holding that "an employer may 'authorize' employees to utilize computers for any lawful purpose but not for unlawful purposes and only in furtherance of the employer's business").

[232] *Compare Nosal*, 676 F.3d 854, *with Int'l Airport Ctrs. v. Citrin*, 440 F.3d 418 (7th Cir. 2006).

[233] Kerr, *supra* note 230, at 1643.

[234] *U.S. v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010); *EF Cultural Travel BV v. Explorica*, 274 F.3d 577 (1st Cir. 2001); *U.S. v. Morris*, 928 F.2d 504 (2d Cir. 1991); *John*, 597 F.3d 263; *P.C. Yonkers v. Celebrations the Party & Seasonal Superstore*, 428 F.3d 504 (3rd Cir. 2005)

[235] *Nosal*, 676 F.3d 854.

bank to verify the identity of customers as a means of reducing money laundering. Or, it may be private. Credit card companies may decide that their rules include denying all transactions from a country such as Macedonia, if they find the incidence of fraud from that state to be unacceptable. Or, power may derive from code. If your smartphone's operating system refuses to run Voice over Internet Protocol applications, you will have to make calls over the usual telephone network, benefitting your wireless provider's profits.

This is less foreign to computer science than it appears: one of the most famous data problems in history demonstrates that the discipline has already had to grapple with the contextual nature of accuracy. Consider dates. In particular, think of 2/8/04.[236] What date does it signify?

Most readers will answer February 8, 2004. That is an entirely reasonable interpretation of the quoted date. Yet, the intent was for the date to correspond to the start of the Russo-Japanese War on February 8, 1904. This problem – of multiple possible meanings – increasingly worried policymakers in the late 1990s. The Year 2000, or Y2K, problem confronted computer scientists with how norms and context were embedded in code and in data.[237] Older programs in particular stored years as a two-digit number, because their creators operated under two key assumptions: that the dates would be understood as corresponding to the twentieth century (with an implicit "19" prepended to their value), and that the programs would be out of service long before twenty-first century dates were at issue.[238] The failure of the second assumption exposed the first. Thus, it was not that the values, from a data storage perspective, were inaccurate. Rather, it was that the context for accuracy had changed. The code that handled them operated within a set of societal assumptions that became stale. The numbers stored on disk never changed. But, they went from highly inaccurate to questionably accurate – to a state of uncertainty – despite their stability. Programmers worldwide worked to make dates, and date-handling code, more accurate by making explicit the embedded assumptions in them. They were almost uniformly successful (though at considerable expense): December 31, 1999 ended with fireworks, but with no IT meltdowns.[239]

On its own terms, cybersecurity is not methodologically sufficient to answer questions about accuracy of information. The technical mechanisms

[236] For those outside the U.S., read as 08/02/04.

[237] Farhad Manjoo, *Apocalypse Then*, SLATE (Nov. 11, 2009), http://www.slate.com/articles/technology/technology/features/2009/apocalypse_then/was_y2k_a_waste.html.

[238] John Quiggin, *The Y2K scare: Causes, Costs and Cures*, 64 AUSTL. J. PUB. ADMIN. 46, 48-49 (2005).

[239] Manjoo, *supra* note 237.

for ensuring accuracy can tell us what changes count under the *system*'s rules. Cybersecurity also needs an account of which of those changes should count under *society*'s rules. Whatever the means, social power drives our conceptions of accuracy.

IV. PROPOSAL

A. Failure as Focusing Event

Accuracy needs to become a core part of the dialogue and debate over cybersecurity. There is a tendency to sideline accuracy as a technological question: either the data is correct, or it is not. Realizing that accuracy is a social construct makes the issue more difficult, and more important. There are at least two issues that can serve as focusing events for accuracy in cybersecurity: health care, and the stock market.

With the passage of the Patient Protection and Affordable Care Act in 2010[240], and the debut of the Healthcare.gov Web site on October 1, 2013[241], national health care became a cybersecurity issue. The site, and its associated set of databases and middleware, rapidly generated concern over problems with accuracy. It often provided estimates of health care costs that were significantly below what consumers would actually face.[242] The data transmitted from the federal health care portal to insurers (who provide coverage to those who sign up at Healthcare.gov) was riddled with errors – 25% of forms passed along in October and November 2013 had mistakes, and even after remediation, 10% had errors in December.[243] Overall, the process of enrolling people in plans has been plagued by errors.[244] One-third of enrollees were affected by bad data.[245] The consequences were significant: "tens of thousands of consumers are at risk of not having coverage when the insurance goes into effect Jan. 1, because the health

[240] Pub. L. 111-148, 124 STAT. 119 (2010).

[241] *Technical Woes on Web Site*, N.Y. TIMES, Oct. 2, 2013, at A15.

[242] *HealthCare.gov pricing feature can be off the mark*, CBSNEWS.COM (Oct. 23, 2013), http://www.cbsnews.com/news/healthcaregov-pricing-feature-can-be-off-the-mark/ (noting that some consumers could pay twice the estimated monthly cost).

[243] Adrianne Jeffries, *One in ten forms sent to insurers still have errors, says Healthcare.gov spokesperson*, THE VERGE (Dec. 6, 2013), http://www.theverge.com/2013/12/6/5183026/one-in-ten-forms-sent-to-insurers-still-have-errors-says-healthcare/in/4623357.

[244] Christopher Weaver, *Errors Continue to Plague Government Health Site*, WALL ST. J. (Dec. 13, 2013), http://online.wsj.com/news/articles/SB10001424052702304202204579256680760860664.

[245] Amy Goldstein & Juliet Eilperin, *Health-care enrollment on Web plagued by bugs*, WASH. POST (Dec. 2, 2013), http://www.washingtonpost.com/national/health-science/health-care-enrollment-on-web-plagued-by-bugs/2013/12/02/e3021b86-5b79-11e3-a49b-90a0e156254b_story.html.

plans they picked do not yet have accurate information needed to send them a bill."[246] The system often could not correctly identify whether a user was eligible for a tax credit that subsidizes the cost of insurance.[247] Similarly, people identified as eligible for Medicaid, the federal program that provides health coverage to low-income Americans, have been unable to enroll in the program due to data and software errors.[248] These accuracy problems emerged in an environment without attacks – they result solely from the health care software's bug-riddled design. Inadvertent data breaches have already occurred in at least one state's similar health care exchange.[249] The difficulties in accuracy with health care data could be far worse; white hat hackers have already warned of serious security flaws with the site and its associated databases.[250] A successful hack could make the problems to date appear mild by comparison.

While the accuracy problems with Healthcare.gov have been widely covered, there has been less attention to solving them in context. Thus far, solutions have been technologically-driven, whether high-tech (fixing bugs in the site's code[251]) or low-tech (reaching out to Medicaid-eligible people via letters and phone calls[252]). These are helpful steps, but there are others that emerge once the context of data accuracy is considered. For example,

[246] *Id.*

[247] Jennifer Preston, *Even With Website Fixes, Troubles Persist in Applying for Insurance*, N.Y. TIMES (Dec. 3, 2013), http://www.nytimes.com/news/affordable-care-act/2013/12/03/even-with-website-fixes-troubles-persist-in-applying-for-insurance/.

[248] Amy Goldstein & Juliet Eilperin, *HealthCare.gov defect leaves many Americans eligible for Medicaid, CHIP without coverage*, WASH. POST (Jan. 4, 2014), http://www.washingtonpost.com/national/health-science/healthcaregov-defects-leave-many-americans-eligible-for-medicaid-chip-without-coverage/2014/01/04/f8ed10d2-7400-11e3-8b3f-b1666705ca3b_story.html.

[249] Dave Gram, *State confirms health website security breach*, BURLINGTON FREE PRESS (Nov. 22, 2013), http://www.burlingtonfreepress.com/viewart/20131122/NEWS03/311220030/State-confirms-health-website-security-breach.

[250] Reports are legion. *See, e.g.*, Jim Finkle & Alina Selyukh, *Some cyber security experts recommend shutting Obamacare site*, REUTERS (Nov. 19, 2013), http://news.yahoo.com/exclusive-expert-warn-congress-healthcare-gov-security-bugs-144729835--sector.html; Lance Whitney, *Healthcare.gov security – "a breach waiting to happen,"* CNET (Jan. 16, 2014), http://news.cnet.com/8301-1009_3-57617335-83/healthcare.gov-security-a-breach-waiting-to-happen/ (quoting Counter Hack founder Ed Skoudis that "given the numerous vulnerabilities, perhaps a breach has already happened"); Adrianne Jeffries, *White hat hacker says he found 70,000 records on Healthcare.gov through a Google search*, THE VERGE (Jan. 21, 2014), http://www.theverge.com/2014/1/21/5331756/white-hat-hacker-says-he-found-70000-records-on-healthcare-gov/in/4623357.

[251] *See, e.g.*, *Ongoing Software Fixes to Improve User Experience*, HHS.GOV DIGITAL STRATEGY (Nov. 21, 2013), http://www.hhs.gov/digitalstrategy/blog/2013/11/software-fixes-improve-user-experience.html.

[252] Goldstein & Eilperin, *supra* note 248.

some users have had difficulty signing up for tax credits or for low-income programs (such as Medicaid) because of uncertain eligibility.[253] An alternative, though, is to worry less about accuracy: when in doubt, extend the credit, or enroll the person. This alternative comes at increased cost to the public fisc, but it is both simpler and faithful to the social objective of providing health care to all citizens. Changing what accuracy means in the system to reflect social goals can ameliorate some of the data problems. More importantly, though, the problems of accuracy with the health care rollout ought to concentrate attention on this issue.

Similarly, recurring problems with accuracy on stock markets should draw regulatory attention. They have already received notice in popular culture – a key plot point in the 2013 movie "Dark Knight Rises" involves the villain Bane bankrupting Bruce Wayne (Batman's alter ego) by falsifying transactions in Wayne's name.[254] The transactions turn out to be disastrous; Wayne loses his fortune, and control over Wayne Enterprises. But accuracy problems are fact as well as fiction. For example, in 2012, a bug in trading software operated by Knight Capital Group disrupted trading in roughly 150 stocks on the New York Stock Exchange, leaving Knight with losses of $440 million dollars after it compensated clients for the mistake.[255] Major corporations such as Berkshire Hathaway and General Electric experienced abnormal trading volumes and price swings.[256] In August 2013, a similar error at Goldman Sachs led to a number of mistaken trades in equity options.[257]

Technological errors have, at times, led to a dearth of accurate information altogether. On May 6, 2010, a combination of a large trade executed by a single investor's software trading system and a pullback by other automated systems caused the famous "flash crash" that stripped

[253] *Id.*

[254] Bane's plan has some holes. *See* Matthew O'Brien, *Bane's Plan to Bankrupt Batman Doesn't Make Any Sense*, THE ATLANTIC (July 23, 2012), http://www.theatlantic.com/business/archive/2012/07/banes-plan-to-bankrupt-batman-doesnt-make-any-sense/260191/; Ryan Davidson, *The Dark Knight Rises I: Corporate Shenanigans*, LAW AND THE MULTIVERSE (July 23, 2012), http://lawandthemultiverse.com/2012/07/23/the-dark-knight-rises-i-corporate-shenanigans/.

[255] Jenny Strasburg, Tom Lauricella, & Scott Patterson, *Electronic Trading Glitches Hit Market*, WALL ST. J. (Aug. 1, 2012), http://online.wsj.com/news/articles/SB10000872396390443687504577563001717194274; Maureen Farrell, *Trading glitches a sad new market reality*, CNNMONEY (Aug. 22, 2013), http://money.cnn.com/2013/08/22/investing/nasdaq-trading-glitch/.

[256] Strasburg, Lauricella, & Patterson, *id.*

[257] Chuck Mikolajczak & Rodrigo Campos, *Nasdaq market paralyzed by three-hour shutdown*, REUTERS (Aug. 22, 2013), http://www.reuters.com/article/2013/08/22/us-nasdaq-halt-tapec-idUSBRE97L0V420130822.

nearly 1000 points from the Dow Jones Industrial Average.[258] Last summer, the NASDAQ exchange halted trading for three hours due to problems with its information systems.[259] A week later, the same problem occurred with the pricing system for U.S. options markets.[260] Markets have always been vulnerable to rumors and other incorrect, external information, such as when hackers compromised the Associated Press's Twitter account and announced that an explosion in the White House had injured President Barack Obama.[261] (The Dow Jones lost 150 points of value almost immediately, but rapidly recovered.[262]) The more worrisome set of problems described here, though, are internal to the financial markets themselves. In an era where high-speed automated trading is the norm, financial firms and regulators are overdue for a serious discussion of how to handle accuracy concerns.[263]

The federal health care portal and the stock exchanges provide potent examples of why accuracy matters to cybersecurity. The first step in addressing the problem is to admit that there is, in fact, an accuracy problem.

B. The Common Law of Cybersecurity

Law can best approach accuracy issues with a scenario-driven, experimental, common law approach. Accuracy's normative questions are the most difficult ones. They involve considerations such as what changes should count as authorized; what level of risk of inaccuracy to accept given competing considerations and cost; and what harm inaccuracy for a given set of information is likely to impose on society. These questions are contextual and path-dependent. They change greatly over time. The best

[258] Ben Rooney, *Trading program sparked May "flash crash,"* CNNMONEY (Oct. 1, 2010), http://money.cnn.com/2010/10/01/markets/SEC_CFTC_flash_crash/; *One big, bad trade*, THE ECONOMIST (Oct. 1, 2010), http://www.economist.com/blogs/newsbook/2010/10/what_caused_flash_crash.

[259] Patrick Rizzo, *"Flash freeze" halts Nasdaq stock trading for 3 hours*, NBCNEWS (Aug. 22, 2013), http://www.nbcnews.com/business/markets/flash-freeze-halts-nasdaq-stock-trading-3-hours-f6C10974922.

[260] Kaitlyn Kiernan & Jacob Bunge, *Nasdaq Glitch Prompts Trading Halt in Some Markets*, WALL ST. J. (Oct, 29, 2013), http://online.wsj.com/news/articles/SB10001424052702304200804579165703242921222.

[261] Max Fisher, *Syrian hackers claim AP hack that tipped stock market by $136 billion. Is it terrorism?*, WASH. POST (Apr. 23, 2013), http://www.washingtonpost.com/blogs/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/.

[262] *Id.*

[263] *See* Brian Korn & Bryan Y.M. Than, *Why We Could Easily Have Another Flash Crash*, FORBES (Aug. 9, 2013), http://www.forbes.com/sites/deborahljacobs/2013/08/09/why-we-could-easily-have-another-flash-crash/.

course, then, is one similar to the common law: slow, careful, case-by-case development of a set of insights, and ultimately guidelines, on how to resolve accuracy questions. Cybersecurity regulation has begun to experiment with simulation-based learning – an approach that can usefully be expanded.

Cybersecurity policy, and the regulators who oversee industry-specific security regimes, should adopt a common law-style approach to questions about determining accuracy. At base, the common law operates on a model of emergent principles: over time, courts and judges consider a range of circumstances, track outcomes, engage in discourse about the advantages and drawbacks of various doctrinal levers, and adapt existing schemes to fit new circumstances.[264] This approach is flexible, familiar to lawyers, and responsive to new information. And, there are extant models to guide inquiries into accuracy – in particular, the Federal Trade Commission's recent use of its Section 5 powers to police privacy and security, the Internet Protocol transition trials supervised by the Federal Communications Commission, and the stress tests performed on major financial institutions under the Dodd-Frank Act.

Dan Solove and Woody Hartzog argue the Federal Trade Commission (FTC) has taken a common law-like approach when evaluating whether firms have engaged in unfair or deceptive practices regarding either privacy or data security.[265] Over time, the FTC has developed a body of principles that guide the agency's use of its regulatory powers under Section 5 of the Federal Trade Commission Act.[266] The FTC articulates these principles through a set of consent decrees and settlements with offenders, and regulated firms quickly internalize the resulting guidance.[267] The Commission began with a core mission – consumer protection – that led the agency to evaluate firms' treatment of customer privacy and cybersecurity.[268] Rather than prescribe particular technological measures or security practices, the FTC proceeded on a case-by-case basis, gradually defining the contours of reasonable and unreasonable practices. For security, the FTC began with a subjective standard, penalizing companies that failed to live up to their representations to consumers.[269] Gradually, the Commission moved to enforce even relatively vague assurances about cybersecurity, and then evolved towards adoption of industry standards and

[264] *See, e.g.*, KARL N. LLEWELLYN, THE COMMON LAW TRADITION: DECIDING APPEALS (1960); John Dewey, *Logical Method and Law*, 10 CORNELL L. QUARTERLY 17, 21 (1925).

[265] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. (forthcoming 2014), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2312913.

[266] *See* 15 U.S.C. § 45.

[267] Solove & Hartzog, *supra* note 265, at 23-28.

[268] *Id.* at 9-15.

[269] *Id.* at 34.

best practices as a baseline for its jurisprudence.[270] This process enabled the FTC to build expertise and to craft thoughtful rules.

The Federal Communications Commission has, in partnership with telecommunications firms, launched a series of experiments designed to evaluate and plan for the transition from time-division multiplexed telephone communications to Internet Protocol.[271] The FCC's goal is not to understand the technological issues in the transition.[272] Rather, the agency seeks to learn how the change will affect the core societal values that it has identified at stake: public safety, interconnection, competition, consumer protection, and universal access.[273] Telecommunications providers will test the effects of shifting protocols on affected stakeholders such as rural residents, and will report data back to the FCC to guide future policymaking during the IP Transition.[274]

Finally, in the wake of the financial crisis of 2008, the Dodd-Frank Wall Street Reform and Consumer Protection Act requires large financial institutions to participate in "stress tests" designed to assess the effects of a major economic crisis on the firms' ability to continue to participate in capital markets.[275] The Federal Reserve gives major banking firms a set of scenarios and conditions, such as the loss of a significant trading partner (counterparty risk) or a fall in the value of risky loans.[276] Firms must evaluate how they would perform when facing such stresses, including

[270] *Id.*

[271] Fed. Communications Comm'n, *In the Matter of Technology Transitions*, FCC 14-5 (Jan. 30, 2014), http://www.fcc.gov/document/fcc-oks-voluntary-experiments-testing-impact-technology-transitions-0.

[272] Statement of Chairman Thomas E. Wheeler, *Technology Transition Task Force Presentation*, http://transition.fcc.gov/Daily_Releases/Daily_Business/2013/db1212/DOC-324663A2.pdf (Dec. 12, 2013) (stating "Building IP-based networks has been refined over the years, so we don't really need 'technology' experiments. What we do need are technology impact experiments").

[273] Tom Wheeler, *Adapting Regulatory Frameworks to 21st Century Networks and Markets*, OFFICIAL FCC BLOG (Jan. 9, 2014), http://www.fcc.gov/blog/adapting-regulatory-frameworks-21st-century-networks-and-markets.

[274] Brian Fung, *The FCC is "beta testing" a next-gen telephone network*, THE SWITCH (Jan. 30, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/01/30/the-fcc-is-beta-testing-a-next-gen-telephone-network/; *see generally* Derek E. Bambauer, *Foxes and Hedgehogs in Transition*, J. ON TELECOMM. & HIGH TECH L. (forthcoming 2014) (manuscript on file with author).

[275] § 165(i), *Dodd-Frank Wall Street Reform and Consumer Protection Act*, 124 STAT. 1376, 1430-31 (July 21, 2010).

[276] *See* BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM, 2014 SUPERVISORY SCENARIOS FOR ANNUAL STRESS TESTS REQUIRED UNDER THE DODD-FRANK ACT STRESS TESTING RULES AND THE CAPITAL PLAN RULE (Nov. 1, 2013), http://www.federalreserve.gov/bankinforeg/bcreg20131101a1.pdf.

whether they would continue to meet capitalization requirements.[277] This data is used to shape the companies' capital plans, which must be approved by the central bank. The Federal Reserve releases a combination of aggregate and bank-specific data to guide future policymaking and to inform investors.[278] The stress tests allow the Fed to tailor its regulatory efforts based on more realistic information, and enable financial institutions to simulate how they might fare under highly adverse economic conditions.[279] Financial regulators in other countries use similar tools. In the United Kingdom, for example, regulators have expanded stress testing to include simulations of cyberattacks against banks.[280] The Bank of England published a summary report of results from the exercise, including a set of recommendations regarding information-sharing and coordination with law enforcement agencies.[281] This type of scenario-based exercise is precisely what this Article advocates should be used to understand accuracy risks.

The goal of common law-style development of accuracy principles for cybersecurity should be to understand how different institutions function under conditions of uncertainty about accuracy or outright inaccuracy, rather than to engage in comparative ranking of firms or other entities. For example, simulations and testing ought to evaluate how banks function when account information becomes uncertain, rather than measuring how Bank of America operated relative to Wells Fargo.[282] This will aid policymakers in tailoring measures, such as technological requirements, by industry. And it is likely to enhance firms' willingness to participate in the testing.

Federal and state governments have begun slowly to engage in simulations and tests of cybersecurity. For example, federal agencies simulated a cyberattack on New York's electricity grid during a summer heat wave to test how first responders, utilities, law enforcement, and others

[277] *See* BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM, THE SUPERVISORY CAPITAL ASSESSMENT PROGRAM: DESIGN AND IMPLEMENTATION 10-16 (Apr. 24, 2009), http://www.federalreserve.gov/newsevents/press/bcreg/bcreg20090424a1.pdf.

[278] *See* BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM, DODD-FRANK ACT STRESS TEST 2013: SUPERVISORY STRESS TEST METHODOLOGY AND RESULTS (March 2013), http://www.federalreserve.gov/newsevents/press/bcreg/dfast_2013_results_20130314.pdf

[279] *See, e.g.,* Daniel K. Tarullo, *Lessons from the Crisis Stress Tests*, FEDERAL RESERVE BOARD INTERNATIONAL RESEARCH FORUM ON MONETARY POLICY (Mar. 26, 2010), http://www.federalreserve.gov/newsevents/speech/tarullo20100326a.htm.

[280] John E. Dunn, *UK banks to stress test readiness for major cyberattack*, TECHWORLD (Oct. 7, 2013), http://news.techworld.com/security/3472366/uk-banks-to-stress-test-readiness-for-major-cyberattack/.

[281] Chris Keeling, *Waking Shark 2: Desktop Cyber Exercise – Report to Participants* 7-8, BANK OF ENGLAND (Nov. 12, 2013), http://www.bankofengland.co.uk/financialstability/fsc/Documents/wakingshark2report.pdf.

[282] *See* BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM, *supra* note 278.

would respond to such a crisis.[283] New York State's Department of Financial Services required the banks that it supervises to undergo cybersecurity testing in December 2013, including by evaluating their safeguards and procedures.[284] The Department of Defense tests the military's cybersecurity. The 2013 report from its Operational Test and Evaluation office showed both that cybersecurity remains a weak point and that testing tends to be less rigorous than a real-world cyberattack would be.[285] Four federal agencies along with the Securities Industry and Financial Markets Association (SIFMA) ran a cybersecurity exercise called Quantum Dawn 2 in July 2013 to test the financial industry.[286] The exercise involved external and internal attacks on financial firms, including a denial of service attack, fraudulent press releases about stocks, and disruption of order processing by a virus.[287] In March 2014, a public-private partnership will test the cybersecurity defenses of a dozen health care entities, including hospitals, insurers, pharmacies, and the Department of Health and Human Services.[288]

Regulators should build upon and expand these tests and simulations, and should move to include assessments of how firms and industries deal with information accuracy issues. Quantum Dawn 2 began to move in that direction by including a scenario where false news about a stock caused its value to drop, but the exercise concentrated on disruption of communications and operational capabilities.[289] SIFMA officials acknowledged the risk of hackers planting hidden code, such as advanced persistent threats, in financial organizations' systems, and then waiting for a

[283] Elizabeth Montalbano, *Feds Simulate Crippling Cybersecurity Attack On NYC Electricity*, INFORMATIONWEEK (Mar. 8, 2012), http://www.informationweek.com/security/risk-management/feds-simulate-crippling-cybersecurity-attack-on-nyc-electricity/d/d-id/1103273?.

[284] Bryan Yurcan, *Putting Cybersecurity Measures to the Test*, BANKTECH (Dec. 12, 2013), http://www.banktech.com/risk-management/putting-cybersecurity-measures-to-the-te/240164695.

[285] DIRECTOR, OPERATIONAL TEST AND EVALUATION, FY 2013 ANNUAL REPORT 330-33 (January 2014).

[286] SIFMA, *Cybersecurity Exercise: Quantum Dawn 2*, http://www.sifma.org/ /services/bcp/cybersecurity-exercise--quantum-dawn-2/.

[287] SIFMA, *Quantum Dawn 2* 4, http://www.sifma.org/uploadedfiles/services/bcp/after-actionreport2013.pdf?n=16428 (Oct. 21, 2013).

[288] Alex Ruoff, *HITRUST to Test Cybersecurity Readiness Of Health Care Orgs With Simulated Attacks*, BLOOMBERG BNA (Jan. 22, 2014), http://www.bna.com/hitrust-test-cybersecurity-n17179881490/; Aliya Sternstein, *Health Care Sector to Test Reflexes for Cyber Attack*, NEXTGOV (Jan. 13, 2014), http://www.nextgov.com/cybersecurity/2014/01/health-care-sector-test-reflexes-cyber-attack/76676/?oref=ng-HPriver.

[289] Lauren Tara LaCapra, *Wall Street banks learn how to survive in staged cyber attack*, REUTERS (Oct. 21, 2013), http://www.reuters.com/article/2013/10/21/net-us-usa-banks-cyberattack-drill-idUSBRE99K06O20131021.

crisis moment to trigger these attacks for maximum effect.[290] What the scenario also should include is the information equivalent of these threats: modeling how financial organizations react to internal data, such as records of trades, that are either false or, more challenging, of unknown veracity. The goal is to examine the processes that an organization uses to resolve accuracy questions, both at the technical and business operations levels, and to evaluate how it operates under conditions of uncertainty. For example, to return to Clancy's scenario, it would be valuable to learn not only how the stock exchange responds to a denial of service attack, but how quickly it can revert to a known, accurate information state; how it functions under conditions where information accuracy is uncertain or unknown; and how it would respond on learning that inaccurate information had entered the system in the past without detection.[291] The more stable and resilient the system under conditions of uncertain accuracy, the less the need for comprehensive accuracy. Thus, expanding and diversifying these simulations is vitally useful for cybersecurity.

Regulators have multiple tools at their disposal to engage in testing. The war games approach of Quantum Dawn 2 or the electricity grid test is one effective model. Distributed evaluation is also possible. For example, Section 404 of the Sarbanes-Oxley Act requires that publicly-traded firms detail their internal controls for the accuracy of financial reporting, including technological ones.[292] Companies must have their auditors document the controls, and compliance with them, and executives must certify that the audits are correct.[293] Most important, firms are required to test and evaluate their internal controls.[294] Cybersecurity assessments of accuracy could be added as part of Section 404 testing. Indeed, doing so comports with the goals of 404, as evaluating how a firm deals with uncertain or inaccurate information is excellent validation of its internal

[290] Lauren Tara LaCapra, *Wall Street goes to war with hackers in Quantum Dawn 2 simulation*, REUTERS (Oct. 21, 2013), http://blogs.reuters.com/unstructuredfinance/2013/06/13/wall-street-goes-to-war-with-hackers-in-cyber-dawn-2-simulation/.

[291] *See id.* (discussing denial of service attacks).

[292] 15 U.S.C. § 7262.

[293] 15 U.S.C. §§ 7262, 7241(a); *see* U.S. Securities & Exch. Comm'n, *Commission Proposes Amendments Regarding CEO, CFO Certification Under Sarbanes-Oxley* (Mar. 21, 2003), http://www.sec.gov/news/press/2003-39.htm.

[294] *See* Public Company Accounting Oversight Board, *An Audit of Internal Control over Financial Reporting That is Integrated with an Audit of Financial Statements*, PCAOB RELEASE NO. 2007-005A (June 12, 2007), http://pcaobus.org/Rules/Rulemaking/Docket%20021/2007-06-12_Release_No_2007-005A.pdf; Securities and Exchange Comm'n, *Commission Guidance Regarding Management's Report on Internal Control Over Financial Reporting Under Section 13(a) or 15(d) of the Securities Exchange Act of 1934*, http://www.sec.gov/rules/interp/2007/33-8810.pdf.

controls for financial reporting. Distributed testing may not be as robust as wargames – companies are not likely to be as ingenious as a dedicated mock adversary in thinking up stratagems – but it scales much more readily.

This common law-themed approach seeks to develop a sophisticated understanding of accuracy in action. A simple but useful methodology for this effort is to evaluate the consequences if data from a recent period of time – say, the last hour, or last business day – were suddenly to become unreliable (potentially inaccurate). In some contexts, such as prescription orders for a pharmacy, or air traffic control systems, the risks would be immediate and potentially sizable.[295] Those are situations, and systems, in need of strong accuracy-enhancing measures. In other situations, such as updates to the Domain Name System, the consequences would be far less. DNS is built with inherent tolerance for error; records are usually slightly out of date, and the distributed architecture of the system makes recovery fast.[296] In these contexts, forgoing additional measures to save cost makes sense.

Finally, a word of caution about this calculus is in order. As the Department of Defense's report on its internal testing notes, real cyberattacks are far more challenging than test conditions.[297] The SIFMA simulation above tests the financial industry's systems, but it will be difficult for it to model the reactions of fearful individual investors, foreign governments, or arbitrageurs.[298] It cannot meaningfully test conditions with other stressors, such as a concomitant physical attack on the United States, or a natural disaster. Cybersecurity should, therefore, err on the side of conservatism: on greater accuracy-preserving measures rather than fewer. Backups are useless until one needs them, and then they are priceless.

With that caveat, common law-style development of guidelines about accuracy through simulations and experimentation can usefully advance cybersecurity regulation. Accuracy is neither a binary concept nor an inherent property of information. An iterative, common law style approach can help elucidate processes for determining accuracy, and can assess how much accuracy matters in a given context. The goal of this project is to determine how various industrial and economic sectors respond to information of questionable or uncertain accuracy – how resilient they are, and how quickly they can recover to a state of greater accuracy. Those insights can guide regulation: the more resilient a sector is, the less need for intervention.

[295] *See supra* note 40; *see* Bambauer, *supra* note 56, at 16 (describing application of high reliability theory to air traffic control systems).

[296] *See* LIU & ABITZ, *supra* note 199, at 35 (noting that setting Time To Live value "is essentially deciding on a trade-off between performance and consistency").

[297] DIRECTOR, OPERATIONAL TEST AND EVALUATION, *supra* note 285.

[298] SIFMA, *supra* note 286.

C. Pushing the Boulder

Once the experimentation described above identifies the right levels of accuracy for a given industry or sector, regulators must determine how to press lagging firms to improve. Some organizations will need to improve both processes and technology to increase accuracy. They can do so through preventive measures and by increasing recovery capability. Prevention is geared to ensuring that only authorized updates occur, and that only the latest information state is presented to users. Recovery is oriented to undoing the effects of unauthorized or stale information, and to returning to normal operation of the system. As discussed in previous work, recovery is largely neglected in cybersecurity policy, despite the fact that errors are legion and inevitable.[299] Entities in critical economic and industrial sectors who fail to meet accuracy guidelines developed through testing should be required to bolster their capabilities. Non-critical sectors should be encouraged to develop similar capabilities through a combination of mechanisms, such as requirements for government funding or contracting, disclosure, and binding self-certification.

Prevention matters for accuracy. Accuracy necessitates that changes to information occur only when an authorized user or program requests them.[300] Systems thereby need measures – user accounts, roles, encryption – to enforce differential levels of access. Wikipedia allows anyone to enter information into its system; a credit card provider should not.[301] Existing regulatory regimes for cybersecurity treat prevention explicitly. For example, the Security Rule promulgated by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act incorporates preventive measures to protect health information.[302] Covered entities must put in place physical safeguards that limit access to data, such as workstation security mechanisms and procedures for disposal of electronic media that contained health data.[303] And, the Security Rule requires technical measures, such as access controls for both users and software programs.[304] The goal is straightforward: to maintain accuracy by preventing unauthorized access to or alteration of patient data.

[299] Bambauer, *supra* note 71, at 673.

[300] This implicitly focuses on alteration of data rather than access to it. One way of eliding this difference is to assume auditing: the system creates, and updates, a record of who has gained access to data. Access thus causes alteration, albeit of different information.

[301] *See Help:Editing*, WIKIPEDIA (Feb. 15, 2014), http://en.wikipedia.org/wiki/Help:Editing; MasterCard, *supra* note 219, at 3-1 – 3-10.

[302] 45 C.F.R. § 164.302 et seq.

[303] 45 C.F.R. § 164.310.

[304] 45 C.F.R. § 164.312.

Prevention, though, is ever imperfect: authorized users will make mistakes, and unauthorized ones will gain rights to the system.[305] For example, the department store chain Target is subject to the rigorous cybersecurity requirements imposed by payment networks via the PCI Security Standards.[306] However, Target's security precautions were breached because the company failed to segment its network properly.[307] Attackers went after a vendor who provided heating and air conditioning services to Target.[308] The vendor's systems connected to Target's network, and the attack took advantage of that connection.[309] The hack gave the attacker access to financial and personal data on 110 million Target customers.[310] Simply put, mistakes happen. Accuracy also needs recovery capabilities.

Recovery allows an information system to mitigate, and hopefully reverse, changes that occurred without authorization. Attacks from hackers or insiders are obvious examples, but so is simple error, or even natural disaster. Public and private entities alike must consider how they would respond if their data center were suddenly wiped out by a flood, by a terrorist attack, or by a bug in application code.[311] Backup capabilities are a basic recovery technology – if an organization suffers a hard drive failure, or a software error overwrites data, that entity needs to be able to restore the lost data. More sophisticated techniques involve audit trails, which track changes based on who made them, and transaction logging, which enables an organization to roll back unauthorized alterations to data.

Studies suggest that a significant number of businesses have questionable recovery capabilities. For example, research by backup vendor Acronis found that 23% of businesses do not have an offsite backup strategy: any backups they perform are kept in the same location as the

[305] *See* Derek E. Bambauer, *The Myth of Perfection*, 2 WAKE FOREST L. REV. ONLINE 22 (2012).

[306] PCI Security Standards Council, *PCI SSC Data Security Standards Overview*, https://www.pcisecuritystandards.org/security_standards/index.php; Ericka Chickowski, *Target Breach Should Spur POS Security, PCI 3.0 Awareness*, DARK READING (Dec. 24, 2013), http://www.darkreading.com/risk/target-breach-should-spur-pos-security-p/240164960.

[307] Brian Krebs, *Email Attack on Vendor Set Up Breach at Target*, KREBS ON SECURITY (Feb. 14, 2014), http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/.

[308] *Id.*; Rachel King, *Isolating Card Data May Have Prevented Target Breach*, CIO JOURNAL (Feb. 10, 2014), http://blogs.wsj.com/cio/2014/02/10/isolating-cardholder-data-may-have-prevented-target-breach/.

[309] *Id.*

[310] *Id.*

[311] *See* Bambauer, *supra* note 71, at 642-49.

original data.[312] Physical compromise of the original information is likely to harm the backup as well. Research by Symantec found that one-third of firms surveyed had backup success rates of under 70%.[313] Small enterprises face particular challenges. In a study by Aberdeen, 90% backed up their data once per day at most, and nearly half reported only having to restore data on rare occasions.[314] Thus, small firms have less resilience – their backups are more coarse-grained, and they have less experience restoring information. Unfortunately, they may need more resilience than expected: according to research by the National Federation of Independent Business, 30% of small businesses undergo damage from a natural disaster, and 10% have a major data loss due to simple human mistakes.[315] Acronis reports that 32% of businesses surveyed fear that their recovery systems would fail under the stress of a serious incident, and 34% believe their organizations would suffer significant downtime.[316] This may result from relatively crude backup techniques: 44% of enterprises surveyed by Acronis backed up only data files, excluding system and configuration files.[317] This lengthens downtime since administrators must configure operating system and application components before restoring data.[318] Organizations have minimalist recovery capabilities more often than one might suppose.

Cybersecurity efforts to improve accuracy should concentrate on recovery rather than prevention. Complete prevention of inaccuracy is impossible, and even meaningful prevention is hard to achieve.[319] Software code displays extraordinary complexity, leading inevitably to bugs.[320] Hackers are adept at finding and exploiting vulnerabilities, such as by using

[312] ACRONIS & PONEMON INSTITUTE, THE ACRONIS GLOBAL DISASTER RECOVERY INDEX: 2012 14 (2012). 42% of the businesses that do have an offsite backup strategy rely on manual transport of backup media rather than automating the task. *Id.*

[313] SYMANTEC & ALCHEMY SOLUTIONS GROUP, BACKUP AND RECOVERY 6 (2009).

[314] Aberdeen, *Small vs. Large Enterprise Data Backup; Same Concept, Very Different Process* (June 3, 2011), http://www.aberdeen.com/aberdeen-library/7230/RA-data-disaster-recovery-backup.aspx#sthash.GoG7wHQX.dpuf.

[315] Dawn Brister, *Small Business Network Disaster Recovery Planning*, CISCO BLOG (July 20, 2010), http://blogs.cisco.com/smallbusiness/small_business_network_disaster_recovery_planning/.

[316] Acronis, *supra* note 312, at 5.

[317] *Id.* at 15.

[318] *Id.*

[319] Bambauer, *supra* note 56, at 22-24; Nathan A. Sales, *Regulating Cyber-security*, 107 NW. U. L. REV. 1503 (2013).

[320] Deirdre K. Mulligan & Fred B. Schneider, *Doctrine for Cybersecurity*, 140 DAEDALUS 70, 72-73 (Fall 2011) (describing theoretical difficulty of proving software can be completely secured); *see* Caryn A. Conley & Lee Sproull, *Easier Said than Done: An Empirical Investigation of Software Design and Quality in Open Source Software Development*, PROCEEDINGS OF 42ND HAWAII INT'L CONF. ON SYS. SCI. 2 (2009).

zero-day exploits that have no known countermeasures.[321] National security services weaken protective techniques such as encryption standards to make surveillance easier.[322] Externalities cause organizations not to bear the full cost of insecurity, leading to underinvestment.[323] And information asymmetry means that defenders are always behind.[324] It is one thing to see the goal of prevention, and another to try to follow the path leading to it.[325]

Even targeted measures for accuracy are going to be difficult to achieve – cybersecurity resists regulation. The issue has been a national security priority since 1997, yet there has been no significant legislation on the topic, and the executive-driven efforts to date have been minimalist.[326] This seeming paradox results from a combination of technical and political challenges. On the technical side, legislators have been reluctant to adopt technology-specific measures, for fear that they will rapidly become obsolete, or that they will impose excessive costs.[327] Measuring those costs, and comparing them to potential benefits, is difficult, because cybersecurity demonstrates both positive and negative externalities.[328] Secure organizations do not receive the full benefit of their good computing health, and insecure ones fail to internalize the harms they cause to others.[329] Moreover, information asymmetries impede efforts to identify, and reward with purchases, vendors of more secure products and services.[330] Market failures justify regulation, but they also make it difficult to achieve.

The political calculus points the same way. Society as a whole benefits from greater cybersecurity in a diffuse fashion, but the costs are borne in a concentrated way by a set of private firms. Public choice theory predicts, correctly, that there will be considerable and effective resistance to

[321] JOHN VIEGA, THE MYTHS OF SECURITY 139-44 (2009); Bambauer, *supra* note 56, at 61-67.

[322] *See* Matt Blaze, *How Worried Should We Be About the Alleged RSA-NSA Scheming?*, WIRED (Dec. 27, 2013), http://www.wired.com/opinion/2013/12/what-we-really-lost-with-the-rsa-nsa-revelations/; Joseph Menn, *Exclusive: Secret contract tied NSA and security industry pioneer*, REUTERS (Dec. 20, 2013), http://www.reuters.com/article/2013/12/20/us-usa-security-rsa-idUSBRE9BJ1C220131220 (describing revelation that National Security Agency paid security firm RSA to use weakened encryption algorithm).

[323] Sales, *supra* note 319, at 13.

[324] Bambauer, *supra* note 45, at 23.

[325] *Cf.* ST. AUGUSTINE, THE CONFESSIONS OF ST. AUGUSTINE (E.B. Pusey trans. 2002) (writing "For it is one thing, from the mountain's shaggy top to see the land of peace… and another to keep on the way that leads thither").

[326] *See* Bambauer, *supra* note 56, at 18.

[327] *Id.* at 25.

[328] Ross Anderson & Tyler Moore, *The Economics of Information Security*, 314 SCI. 610, 610 (2006).

[329] *Id.*

[330] *See* Bambauer, *supra* note 22, at 23-24.

regulation under these conditions.[331] The flip side of this impasse is a collective action problem: we are all benefited by greater security, and those benefits likely outweigh the burdens of regulation overall, but transaction costs impede us from organizing to compensate regulated entities.[332] Given these challenges, it is small wonder that cybersecurity initiatives to date concentrate on modest steps such as designating a lead federal agency for the issue and voluntary information-sharing efforts.[333] To be candid, then, this Article's proposal faces challenging terrain to win passage in Congress.

To drive deployment of accuracy-enhancing methods in firms that lag, some entities should be nudged to adopt techniques to improve information accuracy, and some should be forced. Firms in a few key sectors should be required to implement technological measures that increase accuracy, and in particular to deploy backup and recovery capabilities. In prior work, I establish a set of six key sectors in which firms should be required to adopt related cybersecurity measures: finance and banking, defense contractors, transportation, utilities, government (federal, state, and local), and hospitals / medical centers.[334] The financial, transportation, and utility sectors are economically vital.[335] Finance and utilities both have significant dependence upon the Internet – in fact, many utilities are exposing key systems without adequate security in place.[336] Defense contractors are already frequent hacking targets.[337] And both government and health care organizations deliver vital services.[338]

In some of these sectors, firms already have robust backup and recovery technologies to meet the demands of customers and other regulators. This should reduce both the cost of regulation and, hopefully,

[331] Daniel A. Farber & Philip P. Frickey, *The Jurisprudence of Public Choice*, 65 TEX. L. REV. 873, 883-92 (1987).

[332] Bambauer, supra note 22, at 24.

[333] *See, e.g.,* Homeland Security Cyber and Physical Infrastructure Protection Act of 2011, H.R. 174, 112th Cong. § 222(a)(1) (2011), *available at* http://www.gpo.gov/fdsys/pkg/BILLS-112hr174ih/pdf/BILLS-112hr174ih.pdf (establishing "an Office of Cybersecurity and Communications" in the Department of Homeland Security); National Cyber Infrastructure Protection Act of 2010, S.3538, 111th Cong. § 102(a) (2010), *available at* http://www.gpo.gov/fdsys/pkg/BILLS-111s3538is/pdf/BILLS-111s3538is.pdf (establishing a "National Cyber Center" in the Department of Defense).

[334] Bambauer, *supra* note 45, at 50-51.

[335] *Id.*

[336] Paul Roberts, *Homeland Security Warns SCADA Operators Of Internet-Facing Systems*, THREATPOST (Dec. 12, 2011), http://threatpost.com/en_us/blogs/homeland-security-warns-scada-operators-internet-facing-systems-121211; James R. Koelsch, *Web-based SCADA Gathers More Fans*, AUTOMATION WORLD (Dec. 5, 2012), http://www.automationworld.com/control/web-based-scada-gathers-more-fans.

[337] Siobhan Gorman et al., *Computer Spies Breach Fighter-Jet Project,* WALL ST. J., Apr. 21, 2009, at A1.

[338] *See* Munro, *supra* note 40.

resistance to it. The Securities and Exchange Commission (SEC), for example, has interpreted the Computer Security Act of 1987 and a related executive order to require the agency to maintain robust backup capabilities for its systems.[339] HIPAA mandates that covered entities implement backup and disaster recovery plans, including creating and maintaining accessible duplicate copies of electronic health information, planning to recover that data, and establishing procedures for emergency operations and continuation of cybersecurity processes.[340] Similarly, the requirements for information security programs under the Gramm-Leach-Bliley Act's regulations typically encompass backup capabilities, including testing them.[341] And publicly-traded firms must comply with the auditing and reporting mandates for internal controls established by Section 404 of the Sarbanes-Oxley Act.[342] Effective reporting controls generally involve backup systems.[343] The larger the entity, the more likely it is to have recovery capabilities. A survey by the research firm Aberdeen found that 69% of large enterprises must recover data frequently (on a weekly or daily basis), and that 42% back up data every few hours; those firms are already likely to have sophisticated technologies and business practices in this area.[344] In all of these instances, the regulatory requirement to adopt accuracy-enhancing recovery measures should impose less of a burden on affected firms, if it imposes one at all. Thus, for firms in industries that already face a regulatory requirement regarding data backup and recovery, cybersecurity rules treating accuracy should begin by adopting that requirement.[345]

The common law-style regime of simulation and experimentation described above should also be used to modify regulations for existing firms, and to develop regulations for ones not yet subject to requirements for backup and recovery. Input from regulated organizations is key to developing effective accuracy guidelines.[346] Existing cybersecurity regulators, such as the SEC and Department of Health and Human Services,

[339] *See* Securities and Exchange Comm'n, *Data Back-up Procedures*, Audit Report No. 299 (Mar. 9, 2000), http://www.sec.gov/about/oig/audit/299fin.pdf.

[340] 45 C.F.R. § 164.308(a)(7).

[341] 16 C.F.R. §314.4; *see* Bd. of Governors of the Federal Reserve System, *Interagency Guidelines Establishing Information Security Standards* (Aug. 2, 2013) (stating that an institution "should take into consideration its ability to reconstruct the records from duplicate records or backup information systems"), http://www.federalreserve.gov/bankinforeg/interagencyguidelines.htm.

[342] 15 U.S.C. § 7262.

[343] Protiviti, *Guide to the Sarbanes-Oxley Act: Internal Control Reporting Requirements* 88 (July 2003) (noting that "Pervasive process controls… [include] redundant/backup capabilities"), http://www.complianceweek.com/s/documents/protiviti-033004.pdf.

[344] Aberdeen, *supra* note 314.

[345] Bambauer, *supra* note 56, at 50-53.

[346] *See* Thaw, *supra* note 49.

should undertake notice-and-comment rulemaking to tune their mandates.[347] Testing how organizations function under conditions of varying accuracy may also enable more finely-tuned, and thus less expensive, requirements. For example, the SEC instructs accounting firms to maintain records related to their auditing work for seven years after the date of the audit.[348] That requirement may be necessary for audits, but it may not comport with the firms' needs for daily business operations. Tuning regulation to context is precisely the goal of the common law-style cybersecurity regime described in this Article.

To the extent that these new accuracy requirements impose an untenable burden, the legislation implementing them should mitigate it via subsidies or tax credits – particularly given the public good characteristics of cybersecurity.[349] Tailored offsets could be provided through grant applications; firms would apply with specific, documented expenses, and then receive reimbursement at some rate. The federal government has experience with similar funding strategies through measures like the Broadband Technology Opportunity Program, where the Department of Commerce administered a competitive grant program to cover costs of greater broadband deployment.[350] Or, to save on administrative costs, fiscal support could come via a set amount of tax credit based on measures such as the firm's operating revenues.[351] Alleviating some of the fiscal burden of new recovery measures should also partially mute political resistance to this cybersecurity regulatory scheme.

Firms not in critical sectors should be nudged rather than compelled. The federal government has at least two effective tools to apply pressure: spending, and disclosure. For spending, the government certifies IT vendors on decade-long cycles, and awards contracts for a dizzying array of products and services.[352] Making assessment of recovery capabilities an

[347] *See, e.g.*, 45 C.F.R. § 164.308(a)(7); Securities and Exchange Comm'n, *supra* note 339; Dep't of Health & Human Servs., *Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act*, 75 FED. REG. 40868 (July 14, 2010) (initiating notice and comment rulemaking on, inter alia, changes to Security Rule made by HITECH Act).

[348] 17 C.F.R. § 210.2-6.

[349] Michel van Eeten & Johannes M. Bauer, *Emerging Threats to Internet Security: Incentives, Externalities and Policy Implications*, 17 J. CONTINGENCIES & CRISIS MGMT. 221, 230 (2009).

[350] U.S. Dep't of Commerce, *Broadband Technology Opportunities Program*, 75 FED. REG. 3792, 3792-93 (Jan. 22, 2010) (describing competitive grant applications for BTOP funding).

[351] *Cf.* 26 U.S.C. § 41 (establishing tax credit for research and development expenses, as percentage of such expenses incurred).

[352] *See* Michael D. Shear & Annie Lowrey, *In Tech Buying, U.S. Still Stuck in Last Century*, N.Y. TIMES (Dec. 22, 2013), http://www.nytimes.com/2013/12/23/us/politics/in-tech-buying-us-still-stuck-in-last-century.html?hp&_r=1&.

integral part of bidding for contracts would usefully press firms to adopt better measures and to disclose the ones they already take. And, once a contract is awarded, the federal government should have express authority to audit the firm's cybersecurity capabilities, including how it has deployed its backup and recovery methods.[353] The Obama administration has moved, via executive order and agency rules, to begin to implement similar cybersecurity protections.[354] For example, a new contract requirement promulgated by the U.S. General Service Administration requires, for unclassified information technology, that contractors submit IT security plans compliant with the Federal Information Security Management Act, and that firms permit GSA access to their facilities to audit that compliance.[355] And a joint GSA-Department of Defense report recommends that contractors be mandated to incorporate cybersecurity measures not only in products and services supplied to the federal government, but also in their basic corporate operations.[356] Each year, the federal government spends over half a trillion dollars on goods and services – a significant incentive for private sector firms to bolster their cybersecurity accuracy capabilities.[357]

The government could also press companies to disclose the cybersecurity measures they put in place, backed either by market sanctions, civil enforcement by the Federal Trade Commission, or both. One path would be to require firms to reveal the capabilities of their backup, recovery, and prevention systems, in the same way that Section 404 of Sarbanes-Oxley requires documentation and certification of internal controls for publicly traded companies[358], or that the SEC mandates

[353] U.S. Gen. Servs. Admin., *General Services Administration Acquisition Regulation, Implementation of Information Technology Security Provision*, 77 FED. REG. 749, 750-51 (Jan. 6, 2012); *see* Bambauer, *supra* note 56, at 47.

[354] *See generally* Aliya Sternstein, *What Obama's New Cyber Standards Mean for Federal Contractors*, NEXTGOV (Feb. 12, 2014), http://www.nextgov.com/cybersecurity/2014/02/what-obamas-new-cyber-standards-mean-federal-contractors/78713/; Fernand A. Lavallee, *Cybersecurity and US federal public procurements: what contractors need to know*, DLA PIPER (Mar. 11, 2013), http://www.dlapiper.com/cybersecurity-and-us-federal-public-procurements-what-contractors-need-to-know/.

[355] U.S. Gen. Servs. Admin., 77 FED. REG. at 750-51.

[356] Dep't of Defense and Gen. Servs. Admin., *Improving Cybersecurity and Resilience Through Acquisition* 13 (Nov. 2013), https://acc.dau.mil/adl/en-US/694372/file/75816/IMPROVING_CYBERSECURITY_AND_RESILIENCE_THROUGH_ACQUISITION.pdf.

[357] Jeanne Sahadi, *Cutting Washington could hit Main Street*, CNNMONEY (July 23, 2012), http://money.cnn.com/2012/07/23/news/economy/federal-spending/index.htm; Robert Brodsky, *Contracting spending dips for the first time in 13 years*, GOVT. EXECUTIVE (Feb. 3, 2011), http://www.govexec.com/oversight/2011/02/contracting-spending-dips-for-the-first-time-in-13-years/33238/.

[358] 15 U.S.C. § 7262.

disclosure of cyber-incidents and risks[359]. Market discipline could help push companies towards greater precautions; customers may evince a preference for firms with stronger security, particularly in the wake of coverage of Target's data breach[360] and the National Security Agency's surveillance of on-line activities[361]. The drawback to market-based sanctions is that they likely require third parties, such as rating entities or certifiers, to have any effect, since customers simply don't read privacy policies.[362] Certifiers themselves are vulnerable to capture, reinforcing the information asymmetry that consumers face with cybersecurity.[363] Disclosure alone may not suffice.

Alternatively, Congress could require companies to issue a security policy (similar to now-ubiquitous privacy policies) that could be enforced, in the breach, by the FTC under its Section 5 powers.[364] Some firms already make representations about cybersecurity in their privacy policies.[365] Moreover, the FTC increasingly takes the position that there are substantive minima for security precautions regardless of an organization's contractual obligations. Thus, companies already have de facto security policies – some are explicit, and some are imposed implicitly by regulators. While disclosure has its critics[366], the tactic does leverage private information about achieving accuracy[367], while also harnessing market forces to motivate compliance. FTC enforcement increases the likelihood that firms will comply with their policies. Though the agency brings only a handful of cases each year, and nearly all of them settle for relatively small financial

[359] U.S. Securities and Exchange Comm'n, *CF Disclosure Guidance: Topic No. 2 – Cybersecurity* (Oct. 13, 2011), http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[360] Bruce Horovitz, *Data breach takes toll on Target profit*, USA TODAY (Feb. 26, 2014),http://www.usatoday.com/story/money/business/2014/02/26/target-earnings/5829469/.

[361] *See, e.g.*, Barton Gellman, Todd Lindeman, & Ashkan Soltani, *How the NSA is infiltrating private networks*, WASH. POST (Oct. 30, 2013), http://apps.washingtonpost.com/g/page/national/the-nsa-is-hacking-private-networks/542/.

[362] *See* Bambauer, *supra* note 56, at 23-24; Jay P. Kesan, Carol M. Hayes, & Masooda Bashir, *Information Privacy and Data Control in Cloud Computing: Consumers, Privacy Preferences, and Market Efficiency*, 70 WASH. & LEE L. REV. 341 (2013).

[363] Bambauer, *id.*; *see* Benjamin Edelman, *Adverse Selection in Online "Trust" Certifications*, ICEC '09 205, 205-12, *available at* http://www.benedelman.org/publications/advsel-trust.pdf.

[364] *Cf.* Solove & Hartzog, *supra* note 265.

[365] *See, e.g.*, *U.S. v. ValueClick*, No. CV-08-01711 (C.D. Cal. 2008), at 10-12 (noting ValueClick's promise it "employs industry standard security measures to ensure the security of all data"), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2008/03/080317complaint.pdf.

[366] Omri Ben-Shahar & Carl E. Schneider, *The Failure of Mandated Disclosure*, 159 U. PA. L. REV. 101 (2011).

[367] *See* Thaw, *supra* note 49.

penalties, the administrative costs involved with litigating and with the FTC's ongoing monitoring (which it imposes in most settlements) encourage companies to follow the rules.[368] The FTC's security enforcement efforts also suggest an attractive hybrid model for accuracy precautions, mixing customized promises by organizations with cybersecurity minima imposed by the Commission itself.[369]

Finally, and perhaps most complex, cybersecurity regulation must push organizations to test these capabilities. This effort could fold neatly into the common law-style experimentation process described above as the starting point for regulation. While it is valuable to validate that backup and recovery technologies work, it is far more important that regulated entities evaluate how they operate under conditions of uncertain information accuracy, and that they build what they learn into their business processes.[370] Information is only accurate within a given context. Firms may learn that they operate quite well under conditions of uncertainty – for them, relatively inaccurate information is accurate enough. Others may determine that they need more refined capabilities to bolster accuracy, or additional means of buffering difficulties, such as contractual provisions or insurance coverage.[371] For example, after the terrorist attacks on September 11, 2001, MasterCard decided to build a new disaster recovery center to provide redundancy with its principal data center.[372] The company decided to build the center within 300 miles of its primary operations – far enough away to diminish the risk of a single disaster affecting both, but close enough that staff could drive to it if air travel were halted.[373] Put simply, organizations need not only to plan for the crash, but to test it.

Cybersecurity regulation is particularly difficult to achieve. However, most companies – and especially those in regulated sectors – have already put in place backup and recovery capabilities that bolster accuracy. Those in key industrial sectors that have not already done so, should be compelled to do so by regulation. Companies in other industries should be pushed to implement these mechanisms through an admixture of spending, disclosure requirements, and enforceable self-certification.

[368] Solove & Hartzog, supra note 318, at 15-23.

[369] *Cf. id.* at 59-62.

[370] *Cf.* Beth Bacheldor, *9/11: Are Lessons Learned Still Being Applied?*, ITWORLD (Sept. 9, 2011), http://www.itworld.com/disaster-recovery/202019/911-are-lessons-learned-still-being-applied.

[371] *See* Edward R. McNicholas, *Cybersecurity Insurance to Mitigate Cyber-Risks and SEC Disclosure Obligations*, BLOOMBERG LAW, http://about.bloomberglaw.com/practitioner-contributions/cybersecurity-insurance-to-mitigate-cyber-risks-and-sec-disclosure-obligations/.

[372] Ellen Messmer, *MasterCard factors 9/11 into disaster-recovery plan*, NETWORK WORLD (Dec. 2, 2002), http://www.networkworld.com/news/2002/1202mastercard.html.

[373] *Id.*

V. CONCLUSION

Recognizing that accuracy is socially constructed should unsettle us. We have become accustomed to viewing data as an unbiased representation of the physical world. The data may be wrong at times – Pi is not equal to three – but it can also be correct, and that correctness is invariant.[374] Destabilizing that belief is necessary but painful. Yet, on reflection, this new perspective on accuracy is also empowering. Empiricism continues to play a role in accuracy, but we recognize it is not capable of being definitive for that attribute. Pi is not equal to three because it does not square with our observations of the world, and because we rightly agree that such a definition is ridiculous. Seeing accuracy as the product of social processes usefully forces us to live in a more complex world.

This insight about accuracy has a second important advantage: it embeds trade-offs among competing values, or needs, within the concept. For both law and cybersecurity, accuracy is but one design goal for a system. Even where accuracy could be increased, it is not self-evident that it should be increased – that, too, is a social value judgment. The common law, experimental approach to regulating accuracy in cybersecurity is the best method to weigh these trade-offs, and to construct meaningful definitions of the attribute within context.

Informational accuracy is at the heart of cybersecurity. It is vital, yet difficult, to achieve. Without it, all other protections are greatly vitiated, because we cannot trust the information that our seemingly secure systems protect. This Article seeks to focus attention on accuracy's role in cybersecurity. It argues that backup and recovery capabilities for information systems are critical components to ensuring accuracy, and that prevention, here, deserves a more prominent role. The federal government should use simulations and experiments to build a more granular understanding of how normatively to understand accuracy in data, and how finely to require it, and should deploy a variety of tactics to press firms to implement these mechanisms. Most important, the Article encourages us to recognize that accuracy is an outcome of societal processes, into which data are an important but not singular input. It matters to us whether Schrödinger's cat is alive or dead.[375]

* * *

[374] *See* Alasdair Wilkins, *The Eccentric Crank Who Tried To Legislate The Value of Pi*, IO9 (Jan. 31, 2012), http://io9.com/5880792/the-eccentric-crank-who-tried-to-legislate-the-value-of-pi.

[375] "[T]he observer determines the truth." John H. Lienhard, *No. 347: Schrödinger's Cat*, ENGINES OF OUR INGENUITY, http://www.uh.edu/engines/epi347.htm.