Nebraska Law Review

Volume 96 | Issue 2 Article 6

2017

Cybersecurity Stovepiping

David Thaw
University of Pittsburgh, dbthaw@pitt.edu

David Thaw*

Cybersecurity Stovepiping

TABLE OF CONTENTS

* Assistant Professor of Law, Information Sciences, and Public and International Affairs, University of Pittsburgh; Affiliated Fellow, Information Society Project, Yale Law School.

This work benefitted from the thoughtful commentary of Alessandro Acquisti, Ashok Agrawala, Bryan Choi, Sue Glueck, Jim Graves, Woodrow Hartzog, Eric Hatleback, Justin (Gus) Hurwitz, Margot Kaminski, Kate Klonick, Christopher Lee, Paul Mazzucco, Christina Mulligan, Pierluigi Perri, Bryant Walker Smith, Richard Warner, and Christopher Yoo.

The author expresses thanks to: Justin (Gus) Hurwitz, the University of Pennsylvania Center for Technology, Innovation, and Competition and the participants in the Third Annual Works-in-Progress Roundtable on Law and Computer Science; Sue Glueck and the participants in the 2015 Privacy Law Scholars conference; Richard Warner, Grzegorz Gorksi, and the participants in the Kolegium Jagiellońskie/European Union Workshop on e-Administration; Christopher Lee and the scholars of the Korea Legislative Research Institute; and Bart van der Sloot and the participants in the 2015 Amsterdam Privacy Conference for their feedback on early drafts of this work.

This work benefitted substantially from the excellent research assistance of Matt Belenky.

All errors are the responsibility of the author.

I. INTRODUCTION

Most readers of this Article probably have encountered—and been frustrated by—password-complexity requirements. Such requirements have become a mainstream part of contemporary culture—the more complex your password is, the more secure you are, right? So the cybersecurity experts tell us. Moreover, policy makers have accepted this "expertise" and have even adopted such requirements into law and regulation.[1]

This Article asks two questions. First, it examines whether complex passwords actually achieve the goals many experts claim. Does using the password "Tr0ub4dor&3" or the passphrase "correcthorsebatterystaple" actually protect one's account? Concluding complex passwords are a red herring, as recently confirmed by the federal standards makers,[2] this Article then examines why such requirements became so widespread.

Through analysis of historical computer-science and related literature, this Article reveals a fundamental disconnect between the best available scientific knowledge and the application of that knowledge to password policy[3] development. Discussions with computer scientists who were leading experts in computer security during the period

[1] *See, e.g.*, FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 624 (D.N.J. 2014), *aff'd* 799 F.3d 236 (3d Cir. 2015); Twitter, Inc., 151 F.T.C. 162 (2011); NAT'L INST. STANDARDS & TECH., GUIDE TO ENTERPRISE PASSWORD MANAGEMENT (DRAFT) (2016), https://crsc.nist.gov/crsc/media/publications/sp/800-118/archive/2009-04-21/documents/draft-sp800-118.pdf [perma.unl.edu/9S3F-F574]; *see also Password Complexity Policy*, CORNELL U., https://www.ilr.cornell.edu/about-ilr/faculty-and-staff-resources/technology-services/technology-policies/password-complexity [https://perma.unl.edu/WYH6-DNSR] (providing Cornell University's ILR School password-complexity policy).

[2] During the publication stages of this Article, the National Institute of Standards and Technology (NIST) released revised guidelines regarding password complexity, effectively reversing its position and recommending against widespread use of highly complex passwords for authentication purposes. PAUL A. GRASSI ET AL., NAT'L INST. OF STANDARDS & TECH., SPECIAL PUBL'N 800-63B, DIGITAL IDENTITY GUIDELINES (2017), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf [https://perma.unl.edu/BJ9K-T3VX]. Shortly thereafter, in a media interview, the original lead author of those standards at NIST publicly spoke out against his original decision to recommend such policies, largely on the basis of the fact they caused more harm than was prevented. Robert McMillan, *The Man Who Wrote Those Password Rules Has a New Tip: N3v$r M1^d!*, WALL STREET J. (Aug. 7, 2017), https://www.wsj.com/articles/the-man-who-wrote-those-password-rules-has-a-new-tip-n3v-r-m1-d-1502124118.

[3] I use "policy" broadly throughout this Article to refer to any legislative, regulatory, or organizational policy impacting complexity requirements for passwords.

when password-complexity policies developed suggests that the disconnect between scientific literature and policy outcomes cannot be fully explained by a simple failure of computer-security researchers to identify the shortcomings of complex passwords. Nor can it be fully explained by a failure of computer-science research to consider the user design implications of password complexity and associated research in psychology. This Article proposes the alternative hypothesis that the disconnect resulted from a "stovepiping" failure of a different type—the failure to convey relevant scientific knowledge in a framework which could drive a shift in policy direction.[4]

A common approach to arguing for policy reversal or change is the presentation of new evidence. However, this Article posits that in certain contexts mere contrary or "corrective" evidence may be insufficient. This is because of the effects of policy inertia, which result in a state where more evidence is required to reverse a policy than would have been required to implement it in the first place. Frequent vacillation of policy positions can have destabilizing effects on economic markets and social structures, and within certain highly technological or scientific contexts, this differential may be even more harmful. Using cybercecurity as an example, this Article proposes the hypothesis that in such cases, the same (high) level of evidence should be required for implementation of policy in the *first* instance as is required for subsequent reversal or revision of policy.

Under such a hypothesis, in the context of complex passwords, the result would be that this higher standard of evidence was not met after computer science gained understanding that password complexity did not address the problems it claimed to solve. Thus, what was required for policy reversal was not merely new computer-science evidence but the characterization of that evidence within a framework demonstrating that continuing the original course of action was actually resulting in a *worse* condition than originally existed. In fact, this type of net benefit/loss economic framing was largely missing from the discourse regarding authentication at the time and, indeed, remains deeply undertheorized in contemporary discourse regarding cybersecurity policy.[5]

The implications of these results are compelling. If the assertions in this Article are correct, the technical complexity of society has vastly outstripped our policy-making process's ability to keep pace. A dystopian view of this result suggests we are heading toward technocracy. (How did you feel the last time Facebook or Google implemented a major overhaul?) A perhaps more optimistic view, however, suggests that such technical complexity is not a new concept in relative terms

[4] For a discussion of the concept of stovepiping, see *infra* Part II.

[5] *See supra* note 2.

and that historical context can provide some guidance as to how to adapt.

This optimistic view proposes that regulatory history may provide suggestions for regulating rapidly changing fields like cybersecurity. Looking to other fields such as medicine, aviation, and other technologies whose development outpaced the policy makers of the time can provide such insight for the Information Age. Each of these fields had to develop a scientific knowledge base upon which to base policy frameworks and evaluate subsequent policy changes. Developing a science of cybersecurity and requiring evidence-based policy making can provide solutions applicable to the specific problems presented in this Article, and that process of developing a scientific base as a regulatory prerequisite may also benefit other highly technical subjects faced by an increasingly complex society.

Simply put, cybersecurity policy making must, as with other technical fields, move towards requiring evidence-based policy making in the first instance. To do otherwise in such a highly technical and rapidly evolving field undermines the very purposes of the regulatory process itself, particularly in the context of delegation to "expert" administrative agencies. This Article examines that concept through the lens of the specific problem of password complexity and offers a policy making prescription by way of example: the myth of "risk prevention" must be replaced with the empirically founded calculus of risk management. And the primary question to be addressed must not be "Is your system secure?" but rather "*Do your risk mitigation techniques match your risk tolerance?*"

II. THE CONCEPT OF STOVEPIPING

Academic research departments often debate the concept of "stovepiping"—the idea that intense focus within their own discipline, while beneficial to depth-oriented research, decreases the likelihood that broader questions may be investigated. In recent years, many major U.S. research institutions have increased the number of interdisciplinary or cross-disciplinary initiatives.[6] While a promising trend, examples like those presented in this Article suggest the trend may not be adequate to address the complex technical problems facing an increasingly interconnected society. This paper explores, through the example of information-security regulations, the disconnect between how legal and policy communities versus technical and scientific communities formulate questions. That disconnect, combined with the increasing interconnectivity and resulting complexity in

[6] *See* Creso M. Sá, *"Interdisciplinary Strategies" in U.S. Research Universities*, 55 SPRINGER SCI. & BUS. MEDIA 537 (2008).

global society, suggests that traditional policy-making processes may be inadequate to address certain contemporary challenges.

This project began with the hypothesis that a lack of interdisciplinary integration within computer-science research failed to identify the shortcomings of complex passwords discussed in section III.A. of this Article. While only a small percentage of the literature on password complexity has addressed this concern,[7] based on discussions with computer scientists[8] involved in early password policy making and feedback received during the development of this Article, that hypothesis appears incomplete. It is important to note that there exists little, if any, formal literature documenting this history. Substantial credit is owed to Professors Steven Bellovin, David Clark, and Matthew Blaze for their direct recitation of relevant history during the development of early password-authentication practices during the 1980s and early 1990s.

The initial inquiry of this Article began from the hypothesis that computer-science research failed to account for certain human factors, thus leading to the production of incomplete evidence that formed the basis of policy recommendations. This hypothesis seemed unsatisfying, however, because substantial research into human–computer interaction and human factors (in technology) has been ongoing for several decades.[9] Furthermore, discussion with leading computer scientists during the period when password-complexity policies first were developed indicated that, even if unpublished, at least some key components of the computer-security community recognized that raw password complexity was not a simple tradeoff. Based on this knowledge, this Article posits a revised hypothesis suggesting that, notwithstanding an understanding of various factors, the policy-making processes—at the legislative, regulatory, and organizational levels—were mismatched with the processes for developing and refining technical knowledge to adapt to changing situations, particularly in the context of matters of "safety and security."

Thus, the "stovepiping story" is not one of a failure of computer-science research to recognize human factors and incorporate expertise from psychology, sociology, and related fields. Rather, this Article proposes that the disconnect resulted from a stovepiping failure of a different type—the failure of *any* scientific or policy discipline to connect

[7] *See, e.g.*, DINEI FLORENCIO ET AL., DO STRONG WEB PASSWORDS ACCOMPLISH ANYTHING? 5–6 (2007), https://www.usenix.org/legacy/event/hotsec07/tech/full_papers/florencio/florencio.pdf [https://perma.unl.edu/6MRZ-7DLK].

[8] In large part, there is a lack of authoritative literature surrounding many of the topics I discuss in Part II. The foregoing paragraphs detail information and opinions gained from my own conversations with computer scientists, including Professors Steven Bellovin, David Clark, Matthew Blaze, and others.

[9] *See, e.g.*, BEN SHNEIDERMAN, DESIGNING THE USER INTERFACE: STRATEGIES FOR EFFECTIVE HUMAN–COMPUTER INTERACTION (1986).

the results of scientific knowledge to a characterization which could drive a shift in policy direction. Factors such as policy entrenchment[10] and heightened standards for justification of policy rescission[11] make the process for changing policy direction more stringent than that for establishing initial policy. Furthermore, the fear of moving away from a known quantity (an apparent "protective measure") to an unknown quantity—particularly when that unknown quantity involves removal of the original protective measure—is a well-known condition which organizations and policy makers resist. After all, "nobody ever got fired for buying IBM," as the old saying goes.[12]

Several computer-science articles identify the shortcomings of complex passwords, with some even going so far as to assert that the complex-password proposition is fundamentally flawed in the modern context.[13] What this body of literature fails to accomplish, however, is developing a model for overcoming the policy inertia already in place with respect to password complexity. Overcoming this inertia, as discussed above, requires not simply demonstrating the inapplicability of the original proposition but taking a step further to demonstrate the *harm* caused by maintaining policies based on the original proposition. Put simply, what is missing from the existing debate is a demonstration that complex passwords cause more harm than good.

This Article articulates that calculation and further identifies that within the context of cybersecurity, such tradeoffs must be the approach through which researchers frame policy-oriented results and through which policy makers translate research into rules. The existing "technological arms race" of cybersecurity is hopelessly doomed as system complexity will always introduce new opportunities for compromise. Rather, as discussed in Part IV, a risk-analysis/risk-mitigation approach is required to develop long-term solutions to cybersecurity problems that endure technological change. Similarly, such an approach may be applicable to other areas of policy making where technological change is likely to disrupt social, political, or economic assumptions inherent in carefully crafted policy solutions.

[10] *See generally* Antonios Kouroutakis & Sofia Ranchordás, *Snoozing Democracy: Sunset Clauses, De-Juridification, and Emergencies*, 25 MINN. J. INT'L L. 29 (2017); Sofia Ranchordás, *Time, Timing, and Experimental Legislation*, 3 THEORY & PRAC. LEGIS. 135 (2015).

[11] *See generally* Motor Vehicle Mfrs. Ass'n v. State Farm Mut. Auto. Ins. Co., 463 U.S. 29, 41–42 (1983).

[12] *See generally* H.O. Maycotte, *Your Startup Dilemma: Nobody Ever Got Fired for Buying IBM*, FORBES (Dec. 9, 2014), http://www.forbes.com/sites/homaycotte/2014/12/09/your-startup-delimma-nobody-ever-got-fired-for-buying-ibm [https://perma.unl.edu/N2VX-WZCW].

[13] *See* FLORENCIO ET AL., *supra* note 7.

III. STOVEPIPING IN CYBERSECURITY

Information security, or "cybersecurity,"[14] presents an interesting quandary for researchers. Many of its elements, such as encryption algorithms, require the development of deep subject-matter knowledge to solve new problems. Yet at the same time, defending a complex system requires a wide breadth of knowledge including how administrative, technical, and physical elements interact with one another. This interaction requires understanding not just the appropriate subfields of computer science but operations science, psychology, economics, and many other fields as well.

A. Policy Making, Complexity, and Change

The failure to consider properly the interaction among many fields of expertise may have negative impacts beyond mere less-than-optimal outcomes. If the advice given by depth-oriented expertise is not properly contextualized within the problem of the overall technological and operational system, the result may in fact be policies that are worse than had no action been taken. Depth-oriented expertise may recognize this concern but fails to contextualize it within a comprehensive risk-analytic framework workable for policy makers.

However, this disconnect does not stop at the development of scientific and technical knowledge; it is key to issues of policy making, particularly in safety and security contexts. Those contexts are instructive of one part of the problem: the emotional need not to decrease security or to implement measures that give the appearance of comfort, a concept often colloquially described as "security theater."[15]

The context of cybersecurity is instructive of the second half of the problem—rapidly changing technology and societal structures outpace

[14] As noted by Professor Andrea Matwyshyn, "Referring to all of information security, particularly in private sector contexts, as 'cybersecurity' is technically incorrect." Andrea M. Matwyshyn, *Hacking Speech: Informational Speech and the First Amendment*, 107 Nw. U. L. Rev. 795, 817 n.99 (2013). Matwyshyn describes this misnomer as ignoring the aspects of physical security inherent in "holistic" protection of data maintained by an enterprise. *Id.* I concur with this assessment and further suggest, as consistent with the administrative–technical–physical breakdown adopted by the example of information security in healthcare, 42 U.S.C. § 1320d-2(d)(2) (2012), that such a characterization also overlooks the administrative aspects involved in protecting and securing information. *See* David Thaw, *Criminalizing Hacking, Not Dating: Reconstructing the CFAA Intent Requirement*, 103 J. Crim. L. & Criminology 907 (2013) (discussing the distinction between purely technical restrictions on computer usage and comprehensive administrative, technical, and physical restrictions thereon). Cybersecurity remains the common term with which most readers will be familiar, and thus I utilize that term when describing the matter generally.

[15] *See generally* Adam Slagell, Fear, Uncertainty, and Doubt: The Pillars of Justification for Cyber Security 2–4 (2009), https://www.slagell.info/Adam_J._Slagell/Publications_files/TAM7.pdf [https://perma.unl.edu/A6VU-5P67].

the capacities of traditional policy-making processes. Some scholars have gestured at general concerns regarding rapid technological change,[16] although as of this writing these concerns remain largely undertheorized. While full development of such a theory exceeds the scope of this Article,[17] it makes an important step forward by describing a tractable example of a policy-making failure that can be traced from start to (near) finish.[18]

Modern computer and information systems require various degrees of and methods for security, one of which includes a concept known as "authentication"—the ability of the system to confirm that the human interacting with it is who they claim and that they possess the proper authority for those interactions. As discussed in section III.B., authentication credentials, including usernames and passwords, form the primary method of this process. Yet, as most users of modern computing systems are aware, passwords are largely considered cumbersome and unusable—too complex to remember, too frequently changing, and largely regarded as insecure.

B. Complex Passwords: A Case Study

This section challenges the assumptions of security theatre regarding passwords and authentication, arguing that password-complexity requirements are an illusory solution resulting in large part from the problems of policy entrenchment and a breakdown between the expectations of the policy-making process and the manner in which rapidly changing technical fields develop and articulate their knowledge bases.

Organizations often require users to have certain complexity elements in their passwords, such as multiple classes[19] of characters. This security measure was developed in consultation with experts in cryptography and cryptanalysis, who (correctly) informed policy makers that (in the abstract case) the more complex passwords are harder

[16] *See, e.g.*, YOCHAI BENKLER, THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM (2006); LAWRENCE LESSIG, CODE: VERSION 2.0 (2006).

[17] The author anticipates completing future work further exploring these concepts.

[18] Shortly before publication of this Article, the U.S. National Institute for Standards and Technology released guidance expressly repudiating the efficacy of password complexity within the authentication context. GRASSI ET AL., *supra* note 2. As of the time of writing, however, the author anticipates that substantial time will be required before those recommendations are incorporated into legislative, regulatory, and—lastly—organizational policy, in large part for the reasons articulated in Part IV of this Article.

[19] A character class is a (somewhat arbitrary) delineation of categories of text characters. Traditionally, these are keyboard characters that are grouped into four classic sets: uppercase (English) alphabet characters, lowercase (English) alphabet characters, (decimal) numerals, and special characters, which usually comprise punctuation.

to compromise than less complex passwords. As a result, most organizations have implemented password-complexity requirements,[20] and some policy makers considered imposing strict requirements.

Most readers of this Article likely have encountered (and perhaps even been frustrated by) a password-complexity requirement for a computer system or Internet service they have used. Some readers may even have questioned the efficacy or necessity or such practices. As the following example illustrates, such questions hold merit—the efficacy and necessity of password-complexity requirements are, as yet, unsubstantiated by empirical evidence for most contexts.[21] Yet such requirements have become industry standard practice[22] and have even become part of generally applicable policy making at the federal level in the United States.[23]

The concept of password complexity is the proposition that by requiring users to select passwords meeting certain restrictions, the overall security of an information system is improved by decreasing the likelihood that an attacker will be able to guess a given user's password. This concept is a proverbial sacred cow in computer-security literature, vigorously defended both in academic and professional publications.[24] Yet the scientific origins and bases of this proposition

[20] *See* Rajat Bhargava, *Why Should I Enforce Password Complexity Requirements*, JumpCloud (Nov. 18, 2015), https://jumpcloud.com/blog/reasons-to-implement-password-complexity-requirements [https://perma.unl.edu/4PRL-5LFH].

[21] Certain "high reliability" environments—such as strategic-arms-control systems, commercial aviation, and nuclear-energy generation—are more likely to benefit from any marginal security afforded by such measures and concurrently be able to implement the strict operational controls required to prevent users from circumventing password complexity requirements. *See infra* subsection III.B.3.

[22] Richard Shay et al., *Designing Password Policies for Strength and Usability*, 5 ACM Transactions on Info. & Sys. Security 1, 4–5 (2016).

[23] *See* Internal Revenue Serv., Tax Information Security Guidelines for Federal, State and Local Agencies (2016); Paul N. Otto et al., *The ChoicePoint Dilemma: How Data Brokers Should Handle the Privacy of Personal Information*, 5 IEEE Security & Privacy 15 (2006); Benjamin R. Dryden, *The FTC's Use of Section 5 to Regulate Internet Password Security*, Icarus (Commc'ns & Dig. Tech. Indus. Comm., Am. Bar Ass'n Section of Antitrust Law, Chicago, Ill.), Winter 2011, at 4.

[24] *See, e.g.*, Shirley Gaw & Edward W. Felten, Password Management Strategies for Online Accounts (2016), https://cups.cs.cmu.edu/soups/2006/proceedings/p44_gaw.pdf [https://perma.unl.edu/4E57-7PV5]; Shon Harris & Fernando Maymí, CISSP All-in-One Exam Guide 751–52 (2016); Daniel McCarney, Password Managers: Comparative Evaluation, Design, Implementation and Empirical Analysis (2013), https://binaryparadox.net/assets/pubs/McCarney.MCS.Archive.pdf [https://perma.unl.edu/73MB-MRQT]; Richard Shay, Creating Usable Policies for Stronger Passwords with MTurk (2015), https://pdfs.semanticscholar.org/1f97/d867d4934778031a9b17ee2b998b82cbff57.pdf [https://perma.unl.edu/P73N-LUJD]; Lorrie Cranor, *Time to Rethink Mandatory Password Changes*, Fed. Trade Commission (Mar. 2, 2016), https://www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes [https://perma.unl.edu/ETA8-22TX].

remain somewhat murky, obfuscated by conclusory assumptions in the relevant literature. Discussions with relevant experts in the field suggest that this proposition originated with a 1979 paper by Robert Morris and Ken Thompson of Bell Laboratories titled *Password Security: A Case History*.[25] While apparently quite applicable at the time, the context of information systems has changed vastly from the time at which Morris and Thompson wrote. While the author currently is undertaking a comprehensive literature review to investigate the chain of causality from this work to present literature, based on discussions of earlier drafts of this Article, it appears that until 2007,[26] little work was conducted directly to reexamine the continued applicability of Morris and Thompson's original proposition.[27]

It is these conclusory assumptions that stovepipe the concept of password-complexity analysis in cybersecurity. A review of the leading literature on password complexity reveals a deep analysis of the usability, guessability, and other probabilistic metrics of password-complexity requirements.[28] However, very little literature addresses either of the following two critical questions: (1) Are complex passwords the most efficient means to achieve the defensive goals they facilitate; and (2) if not, does the marginal benefit (if any) of complex passwords—in addition to more efficient techniques for protecting data—justify any other costs or vulnerabilities introduced into the system as a result of increased complexity requirements?[29] The lack of satisfactory answers to these questions within the existing literature results in the disconnect between scientists and policy makers at the heart of this Article. Because existing work fails to demonstrate empirically (or even test) whether complex passwords have a net positive impact on overall system security, it becomes extremely difficult for policy makers to overcome policy entrenchment.[30] Put vastly more simply, no one has scientifically answered the question: Are complex passwords "worth it"? This Article asks why such a question has gone

[25] Robert Morris & Ken Thompson, *Password Security: A Case History*, 22 COMM. ACM 594 (1979).

[26] *See* FLORENCIO ET AL., *supra* note 7.

[27] The author specifically invites comments on this point and is eager to learn of work conducted between 1979 and 2007 in this regard.

[28] *See Usable and Secure Passwords*, CARNEGIE MELLON U., http://sc.cs.cmu.edu/research-detail/51-usable-and-secure-passwords [https://perma.unl.edu/JJP9-BS99] (providing a list of helpful resources under the heading "Project Publications").

[29] *See, e.g.*, FLORENCIO ET AL., *supra* note 7; *see* Casey Johnson, *Password Complexity Rules More Annoying, Less Effective than Lengthy Ones*, ARS TECHNICA (June 28, 2013), http://arstechnica.com/security/2013/06/password-complexity-rules-more-annoying-less-effective-than-length-ones [https://perma.unl.edu/D2D3-7CRQ]; *Passwords and Authentication Research*, CARNEGIE MELLON CYLAB, http://cups.cs.cmu.edu/passwords.html [https://perma.unl.edu/N9C6-LHEG].

[30] *See* Ranchordás, *supra* note 10.

largely unaddressed for so long—nearly forty years from Morris and Thompson's 1979 work until the 2017 reversal of NIST guidance to recommend against overly complex passwords.

1. Fundamentals of Password Complexity

Password complexity primarily stems from concerns regarding the "guessability" of knowledge-based authentication tokens (e.g., passwords) used in computing systems. Unlike immutable characteristic-based authentication tokens (e.g., biometrics) that measure what a user *is* or possession-based authentication tokens (e.g., digital smart cards) that measure what a user *has*, knowledge-based authentication tokens measure what a user *knows* and then *shares* with the system provider—or as it is commonly called, the shared secret.[31] This is a critically important method of authentication because, at least as long as neurological science remains unable to observe precise thoughts of individuals, knowledge-based authentication tokens are both unobservable[32] and inalienable.[33]

The unobservability and inalienability of passwords thus makes guessing a user's secret (i.e., password) seem the most likely vector of attack. Therefore, the probability of success in guessing, whether by characteristic-based attacks,[34] probabilistic-based attacks,[35] or pure

[31] Saikat Chakrabarti & Mukesh Singhal, *Password-Based Authentication: Preventing Dictionary Attacks*, COMPUTER, June 2007, at 68, http://www.cs.nccu.edu.tw/~raylin/MasterCourse/AuthenticationSystem/2010Fall/PasswordAuthentication.pdf [https://perma.unl.edu/BW6L-KFB4].

[32] Unlike immutable characteristic-based tokens, such as biometrics, a person's thoughts cannot (yet) be captured by human or technological observation. By contrast, both fingerprints and optical patterns can be observed discreetly using over-the-counter technology such as a smartphone camera with sufficient accuracy to replicate the biometric data such security measures use to authenticate a user. It is perhaps worth mentioning that to be used, a knowledge-based authentication token must be shared (and therefore become observable by at least one other person or object). However, this distinction is orthogonal to the present claim.

[33] Unlike possession-based authentication tokens, such as digital smart cards, a person's thoughts cannot be physically "stolen" from them—only in the extremely improbable case of advanced psychological "reprogramming" or deliberate, targeted traumatic brain injury is the relevant knowledge replicated or destroyed. While it remains true that the input process of a password could be subject to observation, *see generally* ANDREW KELLY, CRACKING PASSWORDS USING KEYBOARD ACOUSTICS AND LANGUAGE MODELING (2010), https://www.inf.ed.ac.uk/publications/thesis/online/IM100855.pdf [https://perma.unl.edu/8J8Q-FCM5], this type of attack is equally applicable to both immutable characteristic-based authentication tokens and possession-based authentication tokens and is thus an issue orthogonal to the differential importance of passwords.

[34] Characteristic-based attacks are those which rely on context-sensitive knowledge about the user to attempt password combinations that an individual user is likely to employ, such as permutations of their own and their family members' birthdates.

brute-force methods,[36] would seem a critical measure in evaluating system security. If an attacker were easily able to guess a user's password, then system security would be impaired. And the more complex that users' passwords are required to be, the less likely it is that an attacker would be able to guess those passwords—or so the (empirically unsubstantiated) story goes.

This widely accepted[37] (but unproven) proposition in security requires one rather substantial assumption—that an attacker has an available vector by which to repeatedly guess passwords.[38] Essentially, in order for the complexity of passwords to have any defensive efficacy, the attacker must first achieve one of the following steps: (1) acquire a copy of the password-storage files from the system; (2) compromise the authentication interface into which the username and password are entered; (3) otherwise compromise the system in a fashion enabling the attacker to surveil users' login attempts and observe their credentials; or (4) achieve some privilege which allows the attacker to physically observe the entry of the credentials. Additionally, password complexity will play a role if the authentication interface does not employ techniques to limit the number of password-guessing attempts. More generally, in the case of brute-force attacks, the attacker must either be able to run an offline analysis against a file containing users' credentials[39] or make very large numbers of guesses which are confirmed or rejected by the system in real time. Essentially, an attacker must already have compromised the system in some way before password guessing would become an effective technique. Yet, as discussed previously, much modern computer-science literature skipped this step and jumped straight to the assumption—car-

[35] Probabilistic attacks, commonly referred to as "dictionary attacks," are those which rely on generalized context for classes of users, such as permutations of common (U.S.) English words for the passwords of users in a U.S.-based organization. In addition to language dictionaries, attackers now have extensive "dictionaries" of commonly used passwords which are traded like commodities throughout electronic black markets (colloquially, the Dark Web). *See* Chakrabarti & Singhal, *supra* note 31, at 69.

[36] Pure brute-force methods make no assumptions about the probable composition of passwords beyond the enforced complexity requirements and iterate through every possible combination consistent with those requirements. An example brute-force attack on a decimal-numeric-only password would begin with the password "0," iterate through to the password "9," begin the next cycle with "10" continuing through to "99," then "100" through "999,, and so on.

[37] As noted by revisions to NIST guidance published during the publication process of this Article, commentators have recently begun questioning this proposition. *See* Grassi et al., *supra* note 2.

[38] Such vectors can include both online attacks (repeated attempts against an active authentication interface) and offline attacks (cryptanalytic analysis of authentication credential storage). *See* Chakrabarti & Singhal, *supra* note 31.

[39] In other words, the attackers must be able to analyze users' username–password combinations or their cryptographically stored equivalents.

ried over from 1979—that systems did not protect against "brute-force guessing" through other means.

2. *"Guessability"—the False Assumption*

It is this false assumption—that processes for attackers to guess passwords necessarily exist—which underpins the continuing of the false (and possibly scientifically disproven[40]) belief that complex passwords are an essential element of information security for all cases. Recent scientific cybersecurity literature generally is silent on the question of necessity,[41] and professional-practice literature in cybersecurity anecdotally documents and proceeds to assume the extant presence of such processes but also fails to address the necessity of such processes.[42] This Article argues that necessity is a provable falsehood—that for all cases there exist superior methods to sufficiently mitigate the possibility of password-guessing processes. This argument rests on the net cost–benefit economic framing of the problem proposed in this Article. If correct, this argument has substantial implications for the process of engaging technological expertise in policy making because that framing would satisfy the condition of demonstrating not only lack of efficacy but also actual net harm. This demonstration would be the type hypothesized to satisfy the thresholds required to overcome policy entrenchment.

As discussed above, neither scientific nor professional-practice literature adequately describes the reasoning behind why passwords necessarily are guessable. This section summarizes the anecdotal information I have gathered over the years of working and conducting research in this area. Cross-referenced with teaching materials from computer science[43] and professional practice texts,[44] it discusses the most probable attack vectors against which complex password purport to protect and identifies why in each case a superior defensive method exists. The work done in 2007 by Florencio, Herley, and Coskun underpins this analysis.[45]

[40] *See* FLORENCIO ET AL., *supra* note 7.

[41] *See* Bhargava, *supra* note 20.

[42] *See* VERIZON, 2016 DATA BREACH INVESTIGATIONS REPORT (2016), http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf [https://perma.unl.edu/7ZMV-UYJB]; Denise Ranghetti Pilar et al., *Passwords Usage and Human Memory: A Survey Across Age and Educational Background*, 7 PLOS ONE, December 2012, at 1; Michael Kan, *Survey Says Many Companies Want to Phase Out Passwords*, CSO ONLINE (Oct 14, 2016), http://www.csoonline.com/article/3131325/security/survey-says-many-companies-want-to-phase-out-passwords.html [https://perma.unl.edu/2RB9-ZWF6].

[43] JIANXIN YAN ET AL., THE MEMORABILITY AND SECURITY OF PASSWORDS—SOME EMPIRICAL RESULTS (2000), https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-500.pdf [https://perma.unl.edu/NDK7-D4F3].

[44] *See, e.g.*, HARRIS & MAYMÍ, *supra* note 24.

[45] *See, e.g.*, FLORENCIO ET AL., *supra* note 7.

a. Password Guessing Via Authentication (Login) Interfaces

Perhaps the most commonly asserted attack vector for password guessing is the authentication interface, or login screen. This also is perhaps the most preposterous claim as to the efficacy of complex passwords as a defensive mechanism. The claim rests on the presumption that the authentication interface will allow virtually unlimited attempts to guess a user's password. This is an absolutely unnecessary condition, and techniques to defeat such attempts have existed in computer security for decades.[46] Perhaps obvious to the lay user, limiting the number of login attempts before a user's account is locked is a complete defense against this type of attack. Many permutations of this type of defense exist and can be tailored to suit the usability needs of an organization or public-facing system.[47]

b. Password Guessing Via Unprotected/Unsanitized Service

Authentication interfaces are not the only means by which password validity can be verified in real time. Various information services, most commonly web and database services, can provide means by which an attacker can send inquiries to a computer server, the response to which would indicate whether particular authentication credentials (usually username–password combinations) were valid. Such services generally allow for this inquiry–response exchange outside the traditional authentication interface and therefore theoretically may bypass the authentication-attempt-limiting techniques described above. Remediating this vulnerability, however, is simply a matter of engaging in engineering practices that require that similar authentication-attempt-limiting techniques are also applied to any service which makes use of or allows access to the general authentication service. In other words, the designers of a system should ensure that frequency limits are placed on any function that can check the validity of a username–password combination.

c. Offline Password Attacks

Offline password attacks comprise the set of techniques which involves the use of cryptanalytic techniques to determine a user's password based on some stored information to which the attacker has gained access. Most commonly, this is the password storage table—

[46] *See* HARRIS & MAYMÍ, *supra* note 24.

[47] *See* FRANCISCO CORELLA, PROTECTING A MULTIUSER WEB APPLICATION AGAINST ONLINE PASSWORD-GUESSING ATTACKS (2007), https://pdfs.semanticscholar.org/2311/75a1b87473954dea7c26f78b0a5bf41f8fba.pdf [https://perma.unl.edu/G9FD-L7CE]; FRANCISCO CORELLA, SECURE PASSWORD RESET IN A MULTIUSER WEB APPLICATION (2007), https://pomcor.com/whitepapers/secure_password_reset.pdf [https://perma.unl.edu/XM82-Z8PE].

the database or other storage structure in which a system maintains records to verify the authenticity of user passwords.[48]

A first-order critique of complex passwords as a defense against offline attacks is straightforward—if the attacker already has the password tables, the system is already compromised. More precisely, in order to acquire the stored information against which cryptanalytic techniques can be applied, the attacker must first find some vulnerability that affords privileged access to the system. In this case, while it is true that access to the password table might enable the attacker to inflict some small amount of further damage against the system or other systems,[49] the primary focus for allocating limited defensive resources should be on the original point of compromise that allowed the attacker to acquire the password tables in the first place.

Nonetheless, it remains a worthwhile question to investigate what additional net gain (even if small) in security is afforded by making difficult offline analysis of password storage tables, particularly because of the problem of password reuse.[50] Here too, however, the logic of password complexity fails—a clearly superior defense to password complexity exists.

In the context of offline attacks, the logic of password complexity as a defense mechanism is predicated on the concept that passwords are stored in some type of cryptographically complex format. Were passwords simply stored in plain text, the complexity of the password would be irrelevant to the attacker—once the password-storage system was compromised, the actual passwords would be human readable. Thus, for complex passwords to afford any benefit in the context of offline attacks, the system in question must employ some type of cryptographic technique to store other information that cannot be used as the password but can be used to check the validity of the password. The most common type of technique is a one-way hash.[51] Such techniques sometimes are collectively referred to as secure password storage (techniques).

Secure password storage has come under criticism in recent years as an insufficient defensive measure. With massive worldwide in-

[48] *See* Li Shancang et al., *Password Pattern and Vulnerability Analysis for Web and Mobile Applications*, 14 ZTE COMM. 32, 33 (2016).

[49] Password reuse is a common phenomenon in which an individual user will employ the same authentication credentials (usually username and password) across multiple information systems. *See* Shay et al., *supra* note 22, at 16–17.

[50] *See* HARRIS & MAYMÍ, *supra* note 24.

[51] *See, e.g.*, MONI NAOR & MOTI YUNG, UNIVERSAL ONE-WAY HASH FUNCTIONS AND THEIR CRYPTOGRAPHIC APPLICATIONS (1995), http://www.wisdom.weizmann.ac.il/~naor/PAPERS/uowhf.pdf [https://perma.unl.edu/K54C-MC7T]. *See generally* *Universal One-Way Hash Function*, WIKIPEDIA, https://en.wikipedia.org/wiki/Universal_one-way_hash_function [https://perma.unl.edu/KH3D-K59N] (providing a summary discussion of the principle).

creases in access to computer power, primarily through cloud-computing services, attackers are able to pre-compute many possible secure-storage equivalents for commonly used hash functions.[52] This technique, which generates large databases known as "rainbow tables," is similar to creating a large phone book. When an attack acquires a password-storage table, they simply take the stored hash and look up what password it corresponds to in the rainbow table. Proponents of complex passwords argue that such requirements reduce the efficacy of rainbow table-based attacks because the larger the space of potential passwords, the greater computation power is required and the less likely the attacker's "phone book" will contain the password.

There are two logical flaws with this argument. First, it assumes that requiring complex passwords will successfully decrease the likelihood that actual users' passwords (as opposed to potential but unused passwords) will appear in the attackers' phone books. One of the challenges of complex passwords is that they are difficult for users to remember, and one technique users employ to circumvent such memory challenges is selecting the easiest compliant password.[53] For example, under complexity rules requiring at least one lowercase letter, at least one uppercase letter, and at least one number, the password "Password1" becomes both easy to remember and widely used.[54] Attackers do not simply generate rainbow tables based on all possible combinations. The concept of dictionary attacks, well-known throughout cybersecurity, indicates that attackers create "dictionaries" of commonly used passwords. They use these not online for online guessing attacks of the forms discussed in the sections above but also for offline attacks in selecting which "words" to include in their phone books. In addition, consumers typically reuse the same password across a large number of services. Hence, once an attacker has associated a user account with a particular password hash, the probability increases that the credentials can be reused in other services or attacks. Thus, the efficacy of complex passwords in defending against these types of pre-computation attacks is limited by the psychological and usability constraints of human beings—if complex passwords are difficult to remember and attackers know users are likely to circumvent memory difficulties in a specific way, they can tailor their attacks accordingly.

Second, and perhaps more importantly, complex passwords should not be the primary line of defense against pre-computation attacks be-

[52] *See, e.g.*, *Elastic Compute Cloud (EC2)*, AMAZON WEB SERVS., https://aws.amazon.com/ec2 [https://perma.unl.edu/K23J-8LTE]; RAINBOWCRACK, http://project-rainbowcrack.com/index.htm [https://perma.unl.edu/B5EU-MVDC]; Rich Miller, *Inside Amazon's Cloud Computing Infrastructure*, DATA CTR. FRONTIER (Sept. 23, 2015), http://datacenterfrontier.com/inside-amazon-cloud-computing-infrastructure [https://perma.unl.edu/3PS4-47SN].

[53] *See* Shay et al., *supra* note 22, at 5.

[54] *See id.*

cause other techniques exist which dramatically limit the abilities of attackers to generate their rainbow table phone books successfully. For example, small modifications to the storage functions can render attackers' phone books completely ineffective.[55] Such techniques are both highly effective and more efficiently scaled to increased computing power than the approach of requiring humans to remember increasingly lengthy and complex passwords.

3. *"Defense in Depth"—Measuring Marginal Benefit*

"Defense in depth" is a term often invoked by the cybersecurity community to justify additional and often costly security measures.[56] While certainly not inherently negative, such a brute-force approach to security is not necessarily efficient. Security resources will necessarily be limited, so deploying those resources in the most effective manner is crucial. Thus, the term "costly" here becomes particularly important because, while there exists empirical research discussing the direct financial cost of security measures and estimated financial losses from data breaches,[57] such research fails to discuss other types of costs. Lost efficiency from the usability constraints of policies such as password-complexity requirements, the creation of new attack vectors, and organizations' operational impairment have yet to become a focus of empirical cost–benefit research in cybersecurity. The critical element here again is the lack of a net cost–benefit economic analysis to determine the appropriate allocation of limited security resources.

The problem with existing discussions of defense in depth, therefore, is that little (if any) attention focuses on the marginal rate of return for the next investment in or layer of defense. In certain high-reliability environments, such as strategic-weapons-control systems, commercial-aviation operations, or nuclear-energy generation, marginal rate of return may be a lower concern—or, stated differently, the value placed on additional security is sufficiently high that it justifies increased cost. However, in other environments such as consumer websites, where operational tradeoffs may introduce other vulnerabilities, the value of additional security may not be worth the additional

[55] In cybersecurity, such modifications to hash functions are referred to as "salts," hence the etymology of the term (and blog) Salted Hash. *See generally* Samuel Glibbs, *Passwords and Hacking: The Jargon of Hashing, Salting, and SHA-2 Explained*, GUARDIAN (Dec. 15, 2016), https://www.theguardian.com/technology/2016/dec/15/passwords-hacking-hashing-salting-sha-2 [https://perma.unl.edu/Y4RT-VN6L].

[56] For early work describing the benefits of this strategy, see NAT'L SEC. AGENCY, DEFENSE IN DEPTH: A PRACTICAL STRATEGY FOR ACHIEVING INFORMATION ASSURANCE IN TODAY'S HIGHLY NETWORKED ENVIRONMENTS (2001).

[57] *See, e.g.*, VERIZON, *supra* note 42; *The Global State of Information Security Survey 2017*, PwC, http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html [https://perma.unl.edu/7WKK-Z39N].

cost. This type of economic analysis, which disambiguates the security goals of high-reliability environments from other types of environments,[58] appears virtually absent from the existing cybersecurity and cybersecurity-policy literature.[59] It seems intuitively strange to apply concepts from high-reliability environments to other operational environments without considering the degree to which such concepts translate. Yet this is precisely what occurs in cybersecurity when defense in depth is invoked to justify additional security measures.

In the context of passwords, defense in depth is effectively a fallback justification applicable whenever specific justifications for password complexity are challenged. A strictly additive measure of system security would, in fact, conclude that notwithstanding the analysis in the section above, complex passwords do increase system security (even if only marginally so over other measures). However, strictly additive measures are a deeply incomplete metric for evaluating system security.

Such approaches assume that decreased usability will not drive users to circumvent system-security measures or at least that such circumvention can be limited with even more stringent security measures. For example, in the context of password complexity, concerns regarding password reuse often drive system administrators to limit the chronological time before a password can be reused, in an attempt to ensure that users do not switch from one password to a new one and then back again. This security measure is designed to enforce more strictly the requirement that users not reuse passwords.

This assumption has yet to be supported by empirical research. By contrast, the alternative hypothesis—that decreased usability *will* drive users to circumvent system-security measures—is empirically demonstrable, at least, through overwhelming anecdotal evidence. While anecdotal evidence is a poor method for drawing more concrete conclusions, such methods of qualitative analysis can inform future quantitative analysis. A simple Google search for the terms "yellow sticky note password" produces sufficient results suggestive that the concept of password-complexity circumvention should be studied empirically.[60]

[58] *See* David Thaw, *Data Breach (Regulatory) Effects*, 2015 CARDOZO L. REV. DE NOVO 151, 152–56.

[59] Some commenters on this Article suggested that, while not publicly documented, some organizations may make these types of economic-tradeoff analyses internally. While certainly a laudable approach, the focus of this Article is macro-level policy, an end generally not well served by confidential, undocumented, internal organizational choices by a sufficiently small number of organizations that neither scientific nor professional literature has yet to document such activity.

[60] GOOGLE, http://www.google.com (search for "Yellow Sticky Note Password") (last visited July 15, 2017); *see also* Alan Henry, *The Most Common Hiding Places for Workplace Passwords*, LIFEHACKER (Nov. 13, 2012), http://lifehacker.com/58526

In a well-known example of password-complexity circumvention, then-U.S. Vice Presidential Candidate Sarah Palin's Yahoo! email account was compromised via the password-reset function.[61] Most consumer websites have a function that allows a user to reset his or her password by answering a series of questions. These questions, however, typically comprise personal information which is also either a matter of or easily derivable from public record. For example, common questions include "What was your city of birth?"[62] and "What was your high school mascot?"[63] The need for such questions to be easy to recall is linked to the difficulty many users have with remembering complex passwords. Yet if a user's password can be easily reset with questions answerable from public knowledge,[64] net marginal impact of password-complexity requirements may in fact be negative, as a new attack vector is created for attackers. A similar analysis could be applied to the yellow sticky note problem described above.

I do not intend to suggest that marginal benefits from various security measures (including complex passwords) do not exist nor that such marginal benefits are never justified. Rather, this analysis focuses on disambiguating the unsubstantiated assertion that certain security measures—such as complex passwords—are *always* better and instead suggests that the integration of interdisciplinary research such as techniques from economics, psychology, and organizational science can better inform the selection of optimal security for a given operational context.

IV. IMPLICATIONS OF THE STOVEPIPING DISJUNCTURE

The example of password complexity and this revised stovepiping story suggest two key results for the process of policy making in an age of rapid technological change.

First, there must be proper connection between questions on which policy makers seek guidance and the corresponding questions that re-

67/the-most-common-hiding-places-for-workplace-passwords [https://perma.unl.edu/J9YF-3QYJ] (describing an I.T. worker's experiences finding passwords hidden on scraps of paper around offices).

[61] *See* Terry Baynes, *Sarah Palin Email Hacker Loses Appeal*, REUTERS (Jan. 30, 2012), https://www.reuters.com/article/us-palin-hacking-idUSTRE80T1UQ20120130 [https://perma.unl.edu/2ZPS-7JGH].

[62] Birth records in the United States are generally a matter of public record.

[63] Putting aside the fact that many individuals list their high school on social-networking websites such as Facebook, for a nontrivial percentage of the population (at least for the purposes of cyber adversaries), the high school they attended can be predicted from their place of birth, and birth records are a matter of public record. Most U.S. high schools have public-facing websites or Wikipedia entries that, at least, indicate their athletic mascot.

[64] The argument that many consumer websites send password-reset instructions via email is also assailable as public Internet email communications are (by definition) insecure and subject to interception with the proper equipment.

searchers answer. This is of particular import in an age of rapid technological change because policy entrenchment can occur before mistakes can be recognized and corrected.

Second, when policy change is required, whether because of underlying change in circumstances or original error, scientific evidence must not only describe the change but must characterize that change in a manner suited to overcoming policy entrenchment and the standards for policy rescission. This latter category suggests a risk-analytic framing of cybersecurity questions which currently is underdeveloped in scientific, professional, and policy literature. While comparative analysis of the efficacy of risk-analytic frameworks still requires further investigation, initial evidence suggests that a risk-analytic framework is substantially more effective at preventing cybersecurity incidents and enabling organizations to protect critical assets.[65] Cybersecurity is a particularly instructive example as security contexts often require heightened evidence to justify overcoming security theater.

A. Addressing the Same Question

If complex passwords are such a bad idea, how did they become industry standard practice?[66] The answer is cybersecurity stovepiping. While it is true that more complex passwords would, in the purely theoretical case, make passwords more difficult to attack, this answer fails to communicate the full set of relevant scientific knowledge. As discussed above, this is mathematically true—the more complex the password space (the realm of possibilities), the more difficult it is to "brute force" the password (guess it by trying every possible combination). And, under certain extremely limited conditions, the marginal additional security afforded by such complexity may have a net security benefit for the overall system. Under most circumstances, however, the marginal additional security benefit would fall well short of the marginal additional-security detriment from additional attack vectors introduced as a result of password complexity—the most notable being the password-reset function. Thus, the net cost–benefit analysis would not suggest, in most cases, that complex passwords increase system security.

Part of this breakdown came from a failure of scientific research to link the complete technical picture to a comprehensive analysis capable of overcoming policy inertia and entrenchment. Additionally, however, there was a failure of communication between scientists and policy makers as to what question was being addressed. When policy

[65] *See* David Thaw, *The Efficacy of Cybersecurity Regulation*, 30 GA. ST. U. L. REV. 287 (2014).

[66] *See* HARRIS & MAYMÍ, *supra* note 24.

makers inquired how to make passwords safer, what they really intended to ask was: What approach will make authentication interfaces more difficult to compromise? That answer, which is quite different than a brute-force-complexity analysis, involves understanding elements of network security, information-systems design, user interface and user-experience design, and which parties are most efficiently situated and equipped to bear the cost of increased security. In other words, rather than asking a cryptography question, policy makers should have been asking a question involving several subfields of computer science, psychology, organizational operations, and economic theory. Had that question been asked—and were it to be asked today—the answer most likely would be: There are ways to secure authentication processes which allow users to employ passwords the average person is capable of remembering, provided other steps are taken to secure the system.[67] The proposition of this hypothetical answer appears to be correct based on the revisions to the NIST guidance on authentication practices published in 2017.[68]

Of course, the process of policy entrenchment is well established on the issue of passwords, so this latter question would likely make little difference for password policy at this late stage.[69] The former question—what character of evidence is required to overcome policy entrenchment—is key for the current state of authentication practices and password policy. The example, however, is illustrative of a point relevant to policy-making processes more generally: before policy entrenchment occurs, when engaging scientific expertise, it is critical to ensure that the *policy* question being asked matches the *scientific* question being answered.

B. Overcoming Policy Entrenchment

Part II of this Article introduces the hypothesis that policy entrenchment explains the failure of scientific research in cybersecurity to correct erroneous policy regarding password complexity. Part III examines this problem in detail and concludes that existing research did suggest against current password complexity policies but, as virtually every Internet user is aware, such policies persist.

[67] *Cf. Usable and Secure Passwords*, *supra* note 28 (providing links to information about password security and research about password "guessability").

[68] *See* GRASSI ET AL., *supra* note 2.

[69] Given the recent changes in NIST guidance and the personal *mea culpa* of the author of those original standards (both of which occurred during the publication process of this Article), there is cause to think that seeking alternate means of securing authentication interfaces and facilitating password use may not be futile exercise. Nonetheless, there still exists substantial inertia—both in policy entrenchment and in industry adoption—to overcome in changing direction. *See id.*; McMillan, *supra* note 2.

Overcoming policy entrenchment requires more than simply showing that earlier circumstances have changed. At the time Morris and Thompson wrote their seminal piece on password-complexity issues in late-1970s UNIX systems,[70] their analysis was correct within its context. Assumptions regarding system configuration at the time suggested that passwords more complex than those in use at the time (e.g., dictionary words as short as three or four characters) were required for adequate security. By the time Florencio, Herley, and Coskun responded in 2007,[71] the landscape of information systems had fundamentally changed. As discussed in their work and in Part III of this Article, complex passwords no longer achieve net-positive security benefits in most cases.[72] Furthermore, Florencio, Herley, and Coskun were hardly the first to point out this failure in their 2007 work. What was missing was the connection to a risk-analytic framing of cybersecurity, which would allow policy makers to overcome entrenchment and justify a change in course of policy direction. More simply—policy makers lacked the relevant evidence to change direction because the scientific evidence showed only that the previous conclusion was no longer correct and not that the previous conclusion might be causing ongoing net negative effects.

C. Risk-Analytic Framework for Cybersecurity

The analysis in this section suggests the need for cybersecurity research, practice, and policy making to employ a risk-analytic framework. Stated more simply, each security measure needs to be examined in the context of an overall system in empirical practice to determine whether given measures produce a net positive or net negative effect when implemented. Current approaches variously define cybersecurity through mathematical modeling[73] or enumerated compliance,[74] with few exceptions.[75] Of particular import, these notable exceptions—applicable to the healthcare and finance industries in the United States—performed nearly four times more effectively at preventing data breaches reportable under U.S. law during the period

[70] Morris & Thompson, *supra* note 25.

[71] Florencio et al., *supra* note 7.

[72] *See id.* at 6; *supra* Part III.

[73] *See, e.g.*, Daniel M. Dunlavy et al., Mathematical Challenges in Cybersecurity (2009), http://www.cs.sandia.gov/~dmdunla/publications/SAND2009-0805.pdf [https://perma.unl.edu/F6WK-797M].

[74] *See, e.g.*, Jennifer M. Pacella, *The Cybersecurity Threat: Compliance and the Role of Whistleblowers*, 11 Brook. J. Corp. Fin. & Com. L. 39 (2016); Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy,* 114 Colum. L. Rev. 583 (2014). *See generally* William McGeveran, Privacy and Data Protection Law (2016).

[75] *See* Thaw, *supra* note 65.

from January 2000 through December 2010.[76] Collectively, this evidence and the analysis in this Article suggest an alternate, risk-analytic-based definition for cybersecurity. This definition can be phrased as a simple question: Do the risk-mitigation techniques for a given information system match the risk-tolerance level appropriate to that system's goals and functions? This question, while perhaps apparently simple, is quite complex to unpack and translate to a workable definition. A regulatory approach I call Federated Regulation, which describes a unique approach to cybersecurity regulation used in U.S. federal health-care-cybersecurity regulation, has shown substantial promise in this regard.

Federated Regulation (also known as Management-Based Regulatory Delegation) is a theory for engaging private expertise in regulation both on the front end (rulemaking) and on the back end (compliance).[77] It replaces the directly (or "checklist") style of regulation with one based on a risk-analytic framework, transforming the regulatory requirement to a four-part process: (1) regulatory authorities define general or "aspirational" areas of concern to be addressed; (2) regulated entities must conduct risk assessments of those areas and develop compliance plans consistent with reasonable management of those risks; (3) regulated entities must follow their own compliance plans; and (4) the plans must be "reasonable" and be updated periodically and with changes in the organization's risk profile. As described by Perri and Thaw:

> This process has been very successful in engaging private expertise to manage healthcare privacy and cybersecurity in the United States. Under this model, legislatures establish an organic statutory framework that calls upon an administrative agency to develop regulations in conjunction with the entities subject to that regulation (and other relevant stakeholders). The regulations then promulgated by the agency, rather than defining strict standards for compliance, instead, lay out general or aspirational goals for regulated entities to achieve. Entities then are required to develop compliance plans which reasonably achieve those goals, and to follow their own plans. This last step

[76] *Id.* at 354–55.

[77] *See id.* at 324–26 (describing Management-Based Regulatory Delegation as having two collaborative parts: the promulgation of aspirational goals by the legislators followed by the industry experts drafting compliance plans to achieve said goals). This method, as discussed in further detail elsewhere, combines Kenneth Bamberger's theory of regulatory delegation in rulemaking with Cary Coglianese and David Lazer's theory of management-based regulation for compliance to describe a process which engages private expertise to draft regulations by allowing private entities to manage their own compliance process. Pierluigi Perri & David Thaw, *Ancient Worries and Modern Fears: Different Roots and Common Effects of U.S. and EU Privacy Regulation*, 49 CONN. L. REV. (forthcoming 2017) (manuscript at 740–41) (on file with author) (citing Kenneth A. Bamberger, *Regulation as Delegation: Private Firms, Decisionmaking, and Accountability in the Administrative State*, 56 DUKE L.J. 377, 386 (2006); Cary Coglianese & David Lazer, *Management-Based Regulation: Prescribing Private Management to Achieve Public Goals*, 37 LAW & SOC'Y REV. 691, 692, 725 (2003)).

> becomes the primary compliance objective, subject to regulatory agency oversight for reasonableness of the plans and entities' adherence to those plans.[78]

The comparative-efficacy points discussed earlier in this Article are based primarily on a comparison of Federated Regulation[79] and de facto directive regulation at preventing certain cybersecurity breaches of statutorily identified "personal information" during the years 2000 through 2010. That preliminary work showed substantially improved capacity at preventing such breaches, controlling for various factors such as attractiveness of target; size, scope, and complexity of organizations; defensive capabilities of organizations; and the different time periods during which organizations first became aware of the threats facing their data in an internetworked Information Age. While preliminary, the results are pronounced and suggest the promise of Federated Regulation and similar models at addressing the types of technologically and scientifically complex problems considered in this Article.[80]

V. CONCLUSION

This Article is more expository and descriptive than it is conclusory. It does suggest a strong conclusion regarding the efficacy of a particular cybersecurity policy-making process (password complexity), and it does suggest a solution for future cybersecurity policy making (risk-management-oriented policy-making frameworks). This Article does not, however, take on the greater challenge of addressing how not to repeat that mistake within other contexts beyond cybersecurity. It *does* identify the characteristics that give rise to policy-making failures and suggests that legal scholarship—indeed the entire legal system—must consider the following factors and how to reconcile them: (1) rapid technological development and change; (2) increasing complexity of social structures (often enabled by technological development); and (3) the core and fundamental values of the deliberative policy-making processes inherent in both direct democratic systems and representative republican governmental systems. We are entering into a period of rapid technological development and change. Because the nature of the antecedent technology—information and computing technology—is such that it increases the capabilities of other scientific and technical areas, we are at the *beginning* of rapid technological change, not the end. Thus, societal structures will face technological change undermining fundamental assumptions upon which those structures rely at an ever-increasing rate. Along with this change comes complexity.

[78] Perri & Thaw, *supra* note 77 (manuscript at 741) (internal citations omitted).

[79] This concept was previously called—somewhat more awkwardly—"Management-Based Regulatory Delegation."

[80] *See generally* Thaw, *supra* note 65.

Yet our policy-making systems are designed around extended, deliberative processes. When facing a need for technical expertise, those systems assume that consensus exists as to the technical solutions and that this consensus does not change more rapidly than policy-making processes can respond. Furthermore, it assumes that when consensus is reached among technical experts, that consensus is backed with valid scientific evidence.

As this Article illustrates, the collisions of these two properties is deeply worrisome for cybersecurity and for other classes of problems that bear these characteristics. Part IV suggests that process-based regulatory structures, such as Federated Regulation, may provide at least interim solutions. But longer-term consideration of our policy-making process is necessary, lest the next fundamental error be not on the scale of irritating passwords but potentially large-scale social or economic injustices.