2015

Should the FTC Kill the Password? The Case for Better Authentication

Daniel J. Solove
George Washington University Law School, dsolove@law.gwu.edu

Woodrow Hartzog
Samford University

Recommended Citation

Solove, Daniel J. and Hartzog, Woodrow, Should the FTC Kill the Password? The Case for Better Authentication (July 27, 2015). 14 Bloomberg BNA Privacy & Security Law Report 1353 (2015); GWU Law School Public Law Research Paper No. 2015-33; GWU Legal Studies Research Paper No. 2015-33. Available at SSRN: http://ssrn.com/abstract=2636366

Bloomberg BNA

Privacy and Security Law Report®

Should the FTC Kill the Password? The Case for Better Authentication

BY DANIEL J. SOLOVE AND WOODROW HARTZOG

Introduction

We are in a data security crisis, with data security breaches occurring at a staggering rate. A major part of the reason involves problems authenticating the identity of account holders. The most common approach to authentication is the use of passwords, but it is increasingly clear that passwords are being used incorrectly in ways that make them a weak security mechanism.[1] People select poor passwords, reuse them on many sites and have difficulty remembering them.[2] These behaviors are understandable given the fact that authentication is needed on so many sites and systems—there are too many passwords for even those with the best memories to remember. And hackers and phishers can readily trick people into revealing their passwords, and even the passwords of even the most responsible users are vulnerable to malware.[3]

There is widespread consensus about the problems with passwords.[4] Few would defend passwords alone as a good means of authentication for accessing important data. Moreover, there are alternative authentication techniques that can enhance or replace passwords. For example, two-factor authentication is hailed by experts as a big improvement over using passwords alone to authenticate identity.[5] Verizon's latest data breach investigation report estimated that two-factor authentication would be the recommended strategy to protect against 24 percent of the reported breaches in 2014.[6]

Despite widespread consensus that password authentication is weak, and despite widespread availability and the reasonable cost of alternative or additional methods of authentication, the most common practice remains using passwords alone to authenticate. For ex-

Daniel J. Solove is the John Marshall Harlan research professor of law at George Washington University Law School and the chief executive officer of TeachPrivacy, http://teachprivacy.com, a privacy and data security training company.

Woodrow Hartzog is an associate professor at Samford University's Cumberland School of Law and an affiliate scholar at the Center for Internet and Society at Stanford Law School.

The authors would like to thank TeleSign Corp. for its support and Blase Ur, a Ph.D. student at Carnegie Mellon University's School of Computer Science, for his feedback. All views in this piece are those of the authors and aren't those of any organization with which they are affiliated.

[1] J. Bonneau, et al., *The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes*, 2012 IEEE Symposium on Security and Privacy (SP), 553, 567 (May 20-23, 2012).

[2] R. Morris & K. Thompson, *Password Security: A Case History*, Comm. ACM vol. 22, no. 11, 594-97 (1979); A. Adams & M. , *Users Are Not the Enemy*, Comm. ACM vol. 42, no. 12, 41-46 (1999); C. Herley & P.C. van Oorschot, *A Research Agenda Acknowledging the Persistence of Passwords*, IEEE Security & Privacy, vol. 10, no. 1, 28–36 (2012); Blase Ur, et al., *Helping Users Create Better Passwords*, USENIX ;login:, vol. 37, no. 6, 51-57 (Dec. 2012).

[3] G. Aaron & R. Rasmussen, *Global Phishing Survey: Trends and Domain Name Use in 1H2014*, Trends and Domain Name Use (2014), *available at* http://docs.apwg.org/reports/APWG_Global_Phishing_Report_1H_2014.pdf.

[4] Bonneau, et al., *supra* note 1 ("The continued domination of passwords over all other methods of end-user authentication is a major embarrassment to security researchers. . . . Over forty years of research have demonstrated that passwords are plagued by security problems and openly hated by users.").

[5] E. Grosse & M. Upadhyay, , Security & Privacy, IEEE , vol. 11, no. 1, 15, 22 (Jan.-Feb. 2013).

[6] Verizon, *2015 Data Breach Investigation Report* ("The use of two-factor authentication for web applications—even by customers—will go a long way toward keeping your organization from being used and abused.").

 ISSN 1538-3423

ample, businesses have been slow to adopt two-factor authentication,[7] and those that do adopt it sometimes do not encourage users to take advantage of it.[8]

The current state of affairs thus demonstrates pathology—rather widespread consensus that an existing security practice is poor yet a lack of movement toward available alternatives. We contend that situations such as this one justify regulatory intervention.

The Federal Trade Commission (FTC) is well-positioned to make this move. It has been enforcing privacy and data security for over 15 years. But to do so, the agency must further develop its nascent theory of authentication requirements. The FTC has been enforcing privacy and data security under a variety of laws and treaties, such as Section 5 of the FTC Act, the Children's Online Privacy Protection Act (COPPA), the Gramm-Leach-Bliley Act (GLB Act) and the U.S.-EU Safe Harbor arrangement, among others. Regarding data security, the FTC has generally focused on whether an entity's data security protections are ''reasonable.''

Although the FTC has filed complaints against companies that have unreasonable password practices, the agency has not brought any enforcement action contending that the use of passwords alone for authentication is unreasonable.[9] In this essay, we argue that the FTC should do so. An updated theory of reasonable authentication is one of the best ways the FTC could act to improve data security. But requiring improved authentication would be a bold step for the FTC, more aggressive than the steps it normally takes. The agency has generally been quite conservative in the practices it deems to be unfair, choosing to enforce against egregiously bad practices.

In this essay we argue that in certain circumstances, the FTC should start requiring better methods of authentication than mere passwords. The FTC has already laid the groundwork for such an approach and need only expand upon its theories requiring companies to be responsive to both online and offline attempts to compromise the integrity of user accounts. If the FTC is going to be a relevant player in the realm of data security, it must address flawed security measures even though they might be commonly used.

The Challenge of Authentication and the Failures of the Password

Authentication presents one of the greatest security challenges organizations face. How do we accurately ensure that people seeking access to accounts or data are actually whom they say they are? People need to be able to access accounts and data conveniently, and access must often be provided remotely, without being able to see or hear the person seeking access.

The predominant method of authentication thus far has been the password. People memorize a word, phrase or code, and they demonstrate that they are indeed entitled to access by providing this word or code. The advantage of passwords is that they are easy to deploy. Unlike physical items, passwords don't cost anything to create. People don't need to carry around anything such as token generators or keys. Items can readily get lost or misplaced, but passwords can stay with people wherever they go—provided, of course, that they are not forgotten. When a password is compromised, the password can readily be changed.

Unfortunately, passwords have some significant shortcomings—they depend upon human memory, which is limited. Short and simple passwords are easy to remember, but they are also easy to crack. So passwords need to be long and complex as well as easy to remember, and this combination is incredibly hard to achieve.

Making the problem even worse, people are told that all of their passwords should be unique. Password reuse dramatically increases peoples' vulnerability when their password is compromised.[10] But it is a virtually impossible feat required of human memory to remember many long and complex passwords.

According to one study, consumers have an average of 24 online accounts.[11] For those who use the Internet more robustly, the number of accounts is much higher—accounts for health insurance sites, bank sites, investment company sites, credit card company sites, utility company sites, news sites, entertainment sites, social media sites and merchant sites, among many others. Then there are logins associated with one's place of employment and logins for devices like smartphones and laptops. The number of accounts that people have can be staggering.

To make matters worse, people cannot just use dictionary words or names, as these can be cracked too easily.[12] The mainstream advice on creating passwords counsels people to use special characters, numbers, punctuation and upper and lower case. All these add complexity to passwords, but they also make passwords significantly harder to memorize.

These demands have resulted in users being given the Herculean task of creating a unique, complex password for every account. No one can remember all of these passwords, so people ignore the advice about using unique passwords and reuse the same password or draw from a pool of a few passwords. According to a study, 73 percent of accounts use duplicate passwords, and consumers use on average of only 1 unique password per every 4 accounts.[13]

But common approaches to authentication make even more unreasonable demands on human memory. Impossible isn't enough, so it must be multiplied by an-

[7] *See* John Fontana, *Two Factor Authentication in Two Years*, ZDNet, Apr. 3, 2013, http://www.zdnet.com/article/two-factor-authentication-in-two-years/.

[8] Google has a very useful website for enabling its two factor authentication mechanism, but not all users see it. *See* Google Inc., *2-Step Verification*, http://www.google.com/landing/2step/.

[9] *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. 583 (2014).

[10] *See, e.g.*, Anupam Das, et al., *The Tangled Web of Password Reuse*, NDSS '14, 23-26 (Feb. 2014), *available at* http://www.jbonneau.com/doc/DBCBW14-NDSS-tangled_web.pdf; Matt Honan, *How Apple and Amazon Security Flaws Led to My Epic Hacking*, Wired Aug. 6, 2012, *available at* http://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/.

[11] TeleSign Corp., *TeleSign Consumer Account Security Report* (June 3, 2015), *available at* https://www.telesign.com/resources/whitepapers/telesign-consumer-account-security-report/.

[12] Bruce Schneier, *Choosing Secure Passwords*, Schneier on Security (Mar. 3, 2014), https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html.

[13] TeleSign Corp., *supra* note 11.

  PVLR ISSN 1538-3423

other impossible feat: Many companies want passwords to be changed frequently. So people must not only remember potentially hundreds of long and complex passwords but also must change these passwords frequently. Unsurprisingly, people often don't change their passwords. Indeed, nearly half of consumers have a password they haven't changed in more than five years.[14]

The more challenging it becomes to memorize all the passwords, the more likely people are to write the passwords down in convenient locations, thus creating additional security risks. Passwords find their way onto sticky notes near computers or in wallets or in e-mail or listed in text files in devices.

There are technical attempts to help people, such as systems that forbid people from choosing weak passwords.[15] Some systems force people to change their password every month or every few months. But these measures fail to help people remember passwords. They cannot stop people from reusing the same passwords or from writing down the passwords.

One company marketed a product called *Password Minder* and produced a hilarious infomercial that says that *Password Minder* has been designed to ''safely store passwords.''[16] It touts: ''Never lose a password. Guaranteed!'' *Password Minder* ''features a discreet leatherette-bound cover to ensure your passwords stay a secret.'' The product was ''laughed out of production'' as experts relentlessly mocked it.[17] But other similar products remain on the market, such as *The Personal Internet Address & Password Log Book*, a small tabbed book where people can write down all their login credentials.[18] It is actually the bestselling book in Amazon.com Inc.'s Internet and Telecommunications category.[19] There are several other password log books for sale on Amazon.

These solutions will make any security expert chuckle, but laughter is misguided if directed to the people who would use such a product—instead, the laughter should be at the fact that people feel the need to resort to such a means because of impossible demands being made on human cognition.

Another strategy to help people with passwords is to store them electronically in one account. This is much more sophisticated than writing them down on paper, because the account can be secured. But how is it secured? Ironically, often with a password! So if the password to this account is compromised, fraudsters can gain access to all of a person's passwords.

Locking the Front Door But Leaving the Back Door Open

The use of passwords and the advice to use unique ones for each account, to make them long and complex, is designed with a particular set of threats in mind. One such threat is a fraudster simply guessing a person's password. Many passwords are so weak that they can readily be guessed. Here is a list of the 10 most commonly used passwords:

1. 123456
2. password
3. 12345
4. 12345678
5. Qwerty
6. 123456789
7. 1234
8. baseball
9. dragon
10. football[20]

Often, passwords are compromised offline, away from the login portal. Hackers can use a brute force attack, technology that allows them to try millions of passwords in a short time. Long, complex and unique passwords are designed to prevent these kinds of attacks, and they do succeed somewhat in stopping them.

But there are other kinds of attacks where having long, complex or unique passwords won't help. For example, in a phishing attack, fraudsters try to trick users into giving away their passwords. Often, fake websites and deceptive hyperlinks look very real and easily deceive many users. As another example, malware such as keystroke loggers and other spyware can be used to obtain passwords, which seems to be how health insurer Anthem Inc. was breached last year.[21] Even when users act perfectly in adopting complex, unique passwords and avoid accidental disclosure, malware can still compromise username and password credentials.

Complex passwords and limits on login attempts do not protect against offline attacks, phishing or malware. Even the person with the world's longest and most complex password will be defeated if she turns over her password to a phisher.

The current approach to passwords protects against only certain types of attacks and fails to address other threats.[22] And by asking people to do the impossible by

---

[14] *Id.*

[15] Blase Ur, et al., *supra* note 2, at 51-57.

[16] YouTube, Password Minder Infomercial, https://www.youtube.com/watch?v=sgbRbYlojm8. More information about the information is available here: Paul Lucas, *Password Minder Uses the Cutting Edge Technology of Paper to Keep You Safe*, Infomercial Hell (Mar. 11, 2013), http://www.infomercial-hell.com/blog/2013/03/11/password-minder/.

[17] Casey Johnson, *Password Minder: The Blank Notebook that Got Laughed Out of Production*, Ars Technica May 16, 2013, http://arstechnica.com/gadgets/2013/05/password-minder-the-blank-notebook-that-got-laughed-out-of-production/.

[18] Amazon.com Inc., *Personal Internet Address & Password Book*, http://www.amazon.com/Personal-Internet-Address-Password-Book/dp/1441303251.

[19] Amazon.com Inc., *Best Sellers in Internet & Telecommunications*, http://www.amazon.com/gp/bestsellers/books/3705/ref=pd_zg_hrsr_b_1_4_last (last visited July 23, 2015).

[20] Jamie Condliffe, *The 25 Most Popular Passwords of 2014: We're All Doomed*, Gizmodo, Jan. 20, 2015, http://gizmodo.com/the-25-most-popular-passwords-of-2014-were-all-doomed-1680596951.

[21] *See* Brian Krebs, *Anthem Breach May Have Started in April 2014*, Krebs on Security (Feb. 15, 2015), http://krebsonsecurity.com/2015/02/anthem-breach-may-have-started-in-april-2014/ (14 PVLR 227, 2/9/15).

[22] *See, e.g.*, David Thaw, *Cybersecurity Stovepiping* (May 10, 2015) (work-in-progress), *available at* http://ssrn.com/abstract=2572012.

creating passwords that are both unique and complicated, this approach practically forces people to engage in risky behaviors that defeat the purpose of these protections.

Hardly any expert would disagree with the problems we stated above, yet passwords remain the predominant approach to authentication. We are living in a world of ostriches, their chuckles at the absurdity of the situation muffled by the sand above their heads.

Why Aren't Better Authentication Methods Catching on More Widely?

The problems that strong passwords protect against, such as guessing attacks, can be dealt with through technologies that limit the number of unsuccessful login attempts within a particular period of time. If guessing attacks can be limited in this way, then the cost-benefit analysis of using long and complex passwords changes. However, the threat of offline attacks and phishing must also be addressed to make authentication effective.

There are other solutions to authentication problems and methods of authentication that can be used if organizations move away from their futile clinging to passwords. Many relatively cheap and easy-to-deploy methods can be used to protect against different kinds of attacks on credentials. One such example is two-factor authentication.[23] The essence of two-factor authentication is simple. In order to log in, you must have something you know (usually a password), as well as one additional factor, usually something you have (usually your cellphone) or something you are (usually a fingerprint or faceprint). Sometimes two factors are only required initially as a way to authenticate certain devices. But these systems can also require two factors for every login attempt. USB tokens that rely upon robust cryptography are more expensive and harder to use and deploy, though they provide robust protection, particularly when layered on top of each other and combined with server-side protections like hashing and salting passwords and monitoring login activity for abnormal behavior.[24]

Two-factor authentication is particularly promising to factor into a company's authentication calculus because it has already been deployed by major companies, protects against many different kinds of offline attacks and can leverage a technology that most people already constantly carry around—their cellphone.[25] Two-factor authentication is a good way to protect against both online and offline attacks. While two-factor authentication remains vulnerable to specialized phishing and malware-based attacks, those vulnerabilities are relatively narrow and typically require the fraudster to already have the user's user name and password.[26]

The multi-factor approach to authentication can also be adapted and made as strong as necessary. Companies could require three authentication factors in some contexts. As a measure of last resort, some companies and researchers have even proposed a fourth authentication factor, ''someone you know.''[27] Here, companies would require that your friends ''vouch'' for you to confirm identity. Vouching could be an effective last resort for authentication.[28]

Once implemented, two-factor authentication schemes might even be upgraded to ''two-channel authentication'' to protect against phishing and malware attacks. In two-channel communication schemes, companies will not authenticate users until they actually hear back from them on the second channel (such as a cellphone) dedicated to authentication.[29]

Of course, the same method of authentication need not be used for all situations. The method of authentication should correspond to the degree of risk. This means that for low-risk situations, passwords might work well. But for high-risk situations, we need more effective means of authentication. Elements affecting risk include the sensitivity of the data, the damage that can be caused by improper access to data, the likelihood of improper access, and the costs of various methods of authentication in terms of money, time and convenience.

For example, two-factor authentication need not be used for all transactions on the same account or device. So two-factor authentication might be used when making certain sensitive transactions, such as large purchases, or accessing health or financial data.

By no means is everything about authentication well-settled and agreed upon. For example, methods of authentication involving biometrics maybe quite effective and convenient at authenticating identity, but they carry enormous risks if compromised because people cannot change biometric data such as fingerprints or eye scans.[30] If a database of people's fingerprint data was obtained by hackers, people would have no ability to fix the damage. Passwords have one leg up here because they readily can he changed.

Our point is not that there is a silver bullet that addresses all the problems with passwords. Rather, there are many better authentication techniques available, ones that are clearly a much better choice than passwords alone in certain situations, especially high-risk situations.

Although many of these techniques are widely available and inexpensive, they are often not used. This is a pathology that is undermining improved data security.

---

[23] *See, e.g.*, Emiliano De Cristofaro, *A Comparative Usability Study of Two-Factor Authentication*, USEC '14 (Feb. 23, 2014), *available at* http://www.internetsociety.org/sites/default/files/01_5-paper.pdf.

[24] *See, e.g.*, Grosse & Upadhyay, *supra* note 5, at 15, 22.

[25] *See, e.g*, De Cristofaro, *supra* note 20.

[26] *See* Bruce Schneier, *Two-Factor Authentication: Too Little, Too Late*, 48 Commc'ns of the ACM, Inside Risk (2004); Jeff Goldman, *New Spear Phishing Attack Bypasses Two Factor Authentication*, eSecurity Planet, June 22, 2015, http://www.esecurityplanet.com/network-security/new-spear-phishing-attack-bypasses-two-factor-authentication.html.

[27] *See, e.g.*, John Brainard, et. al., *Fourth-Factor Authentication: Someone You Know*, CCS '06 (Oct. 30–Nov. 3, 2006), *available at* https://www.grc.com/sn/files/The_Fourth_Factor.pdf; Stuart Schechter, et., al., *It's Not What You Know But Who You Know: A Social Approach to Last Resort Authentication*, CHI 2009 (Apr. 4-9, 2009), *available at* http://research.microsoft.com/pubs/79349/paper1459-schechter.pdf.

[28] *Id.*

[29] *See* Schneier, *supra* note 24.

[30] *See* Daniel J. Solove, *Nothing to Hide: The False Tradeoff Between Privacy and Security* 199-205 (2011); Chad Vander Veen, *Is It Time to Finally Get Rid of the Password?*, Nextgov, June 29, 2015, http://www.nextgov.com/cybersecurity/2015/06/it-time-finally-get-rid-password/116485/.

   ISSN 1538-3423

It is clear from many polls that most people are very concerned about data security, and most leaders of organizations are also very concerned.[31] It is also clear that hardly any security experts would disagree with much of our criticism of passwords.[32] Why is the movement away from passwords so slow? Organizations should be dashing away.

Part of the explanation is likely due to plain old inertia. Even sensible and cost-effective change can be difficult to do. The market doesn't just race toward any improvement that is known to be better. Organizations often wait for others to act first. Until many organizations start moving toward improved authentication and create a lemming-like effect on other organizations, it is easy for things to stagnate with the status quo.

What can organizations do better? In addition to implementing two-factor authentication, they should also ensure that users are educated about the technology and prompted to choose whether to enable it. Two-factor authentication does little good when users don't know about it or understand it.

Change is not likely to happen fast enough without some kind of precipitating event, something to set things in motion and eventually lead to a cascade. We could wait for something like this to happen, but we have no idea when it might occur. The status quo has persisted for quite a while. So rather than wait for Godot, there would be a great benefit for some kind of regulatory intervention. Perhaps a nudge, maybe a gentle push, maybe a shove and maybe even a kick in the rear. Something needs to be done.

The FTC Has Laid the Groundwork for a Better Approach to Authentication

In the U.S., the FTC is the regulatory agency in the best position to step in and require improved authentication. The FTC has the broadest range of jurisdiction of any federal agency enforcing data security. COPPA gives the FTC jurisdiction over many websites that collect data from children under the age of 13. The GLB Act gives the FTC power to regulate the data security of many types of financial institutions. Many companies voluntarily submit to FTC jurisdiction under the U.S-EU Safe Harbor arrangement, which has a principle for security: ''Organizations must take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction.''[33]

The broadest source of FTC jurisdiction is Section 5 of the FTC Act. Under Section 5, ''unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.''[34] With the exception of a few industry carve-outs, Section 5 covers the vast majority of companies doing business in the U.S.. The FTC has long maintained that failing to provide adequate data security can be a ''deceptive'' trade practice or an ''unfair'' trade practice—and in many cases, both deceptive and unfair.

When determining whether data security is satisfactory, the FTC essentially looks to whether the security measures are ''reasonable.'' This is the explicit standard under the GLB Act[35] and under Section 5.[36]

The FTC generally determines what is ''reasonable'' by looking to areas of widespread consensus. Such a consensus appears to exist regarding passwords—at least in what is being said, although it is not being done. And the foundation exists in existing FTC jurisprudence to make a movement toward improved authentication.

The FTC recently issued authentication guidance to businesses as part of its new data security education initiative.[37] One of the FTC's ''10 practical lessons businesses can learn from the FTC's 50+ data security settlements'' is that companies should ''require secure passwords and authentication.'' According to the FTC, this means that companies should: 1) insist on complex and unique passwords; 2) store passwords securely; 3) guard against brute force attacks; and 4) protect against authentication bypass.[38] Indeed, the FTC has been clear in its complaints that authentication is a critical part of the calculus for what constitutes reasonable data security practices. In our previous article about the FTC's privacy jurisprudence, we noted that several FTC complaints against companies for unfair and deceptive data security practices faulted companies for poor user name and password protocols, including allegations that companies:

- used common/known passwords;
- did not require users to change passwords;
- failed to suspend users after repeated failed login attempts;

[31] Press Release, Am. Inst. of CPAs, AICPA Survey: One-in-Four Americans Victimized by Information Security Breaches (Apr. 21, 2015, http://www.aicpa.org/press/pressreleases/2015/pages/aicpa-survey-one-in-four-americans-victimized-by-information-security-breaches.aspx; Mary Madden, *More Online Americans Say They've Experienced a Personal Data Breach, Pew Research Center*, Pew Research Center FACTANK (Apr. 14, 2014), http://www.pewresearch.org/fact-tank/2014/04/14/more-online-americans-say-theyve-experienced-a-personal-data-breach/; Ponemon Institute LLC, *Is Your Company Ready for a Big Data Breach? The Second Annual Study on Data Breach Preparedness* (Sept. 2014), *available at* http://www.experian.com/assets/data-breach/brochures/2014-ponemon-2nd-annual-preparedness.pdf; Teri Robinson, *The 2014 Survey: Guarding Against a Data Breach*, *available at* http://www.vormetric.com/sites/default/files/ar-SCMag-DataBreachSurvey.pdf.

[32] *See*Vander Veen, *supra* note 28; Bonneau, et al., *supra* note 1, at 553, 567; Morris &Thompson, *supra* note 2, at 594-97; Adams & Sasse, *supra* note 2, at 41-46; Herley & van Oorschot, *supra* note 2, at 28–36; Blase Ur, et al., *supra* note 2, at 51-57.

[33] Export.gov, *U.S.-EU Safe Harbor Overview*, http://www.export.gov/safeharbor/eu/eg_main_018476.asp (last updated Dec. 18, 2013).

[34] 15 U.S.C. § 45(a)(1).

[35] FTC, Final Rule—Standards for Safeguarding Customer Information, 16 C.F.R. pt. 314.

[36] FTC, *Commission Statement Marking the FTC's 50th Data Security Settlement* (Jan. 31, 2014), http://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf (''The touchstone of the Commission's approach to data security is reasonableness: a company's data security measures must be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities.'').

[37] FTC, *Start With Security: A Guide for Businesses* (June 30, 2015), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business (14 PVLR 1236, 7/6/15).

[38] *Id.*

- allowed user name and password sharing;
- permitted users to store passwords in unsafe cookies;
- failed to require user information such as passwords to be encrypted in transit; and
- allowed new user credentials to be created without checking them against previously obtained legitimate credentials.[39]

Like the FTC's authentication guidance to businesses, these complaints are focused almost entirely on passwords as a means of authentication. But a deeper look reveals that the FTC has actually laid the groundwork for a more complete theory of authentication. For example, in targeting limitations on login attempts and easy-to-guess passwords, the FTC is trying to protect against online guessing attacks. In targeting password sharing, failure to encrypt passwords in transit and stale passwords, the FTC is trying to protect against the many different ways passwords can be compromised offline or away from the login page. The FTC has signaled that companies should respond to authentication requests in a reasonable way. As authentication threats evolve, so should the FTC's requirements for reasonable authentication.

Should the FTC Start Requiring Improved Authentication?

The recent wave of data breaches shows that industry should be nudged so that standards can evolve. Improved authentication is the ideal place for FTC intervention because there is an increasing consensus from industry and data security experts that passwords alone are no longer sufficient for many kinds of users accounts. Moreover, as described above, many new identity-verification techniques like two-factor authentication are not radical concepts.

The FTC's authentication jurisprudence supports moving beyond passwords to embrace new, effective and popular techniques. Although passwords alone might still be sufficient for certain kinds of systems, the FTC might consider where improved authentication approaches such as two-factor authentication might be more appropriate for high-risk contexts.

The FTC should not create a one-size-fits-all standard. A holistic approach to authentication would consider the relevant threats, the costs of deployment, the toll on use and the relative security benefits of relevant authentication strategies. The FTC can begin by holding that in certain high-risk contexts, improved authentication methods should be employed. The FTC need not necessarily choose which method. The test should be pragmatic: How well does the method work? What are the costs and benefits? The FTC can conclude that as long as alternatives exist that are reasonable in cost and ease of deployment, the use of passwords alone is insufficient.

In the most high-risk situations, the FTC can reach the strong conclusion that the use of passwords alone will not suffice. An example is the authentication of a company's employees who are accessing sensitive data about consumers.

In other situations, the FTC might conclude that improved authentication methods should be available or strongly encouraged. An example would be requiring a financial company to make available to consumers better authentication methods. Ultimately, it would be up to the consumers to choose. In some cases, the FTC might promote a stronger requirement that the companies do more than merely make alternative authentication methods available but also more actively encourage their use. And it might be that for many low-risk accounts, complex passwords and limitations on login attempts are still sufficient.

Ultimately, the right amount of nudging versus pushing is a detail that can be worked out as this area of FTC jurisprudence develops. The important point is that the FTC intervene and take a stand. This will have an enormous effect on industry, which looks to the FTC for guidance and moves to respond to avoid being subjected to FTC enforcement in the future.

Some might object that the FTC would be too aggressive to start pushing improved authentication when most companies still use passwords alone. Deference to industry standards has been the hallmark of FTC's approach to data security.[40] However, there is a danger to

[39] For a detailed exploration of the FTC's interpretation of proper password protocol, *see* Decision and Order at 2, *In re Twitter, Inc.*, FTC File No. 092 3093, No. C-4316 (F.T.C. Mar. 11, 2011), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2011/03/110311twitterdo.pdf (9 PVLR 934, 6/28/10); *see also* Complaint at 10-12, *FTC v. Wyndham Worldwide Corp.*, No. 2:12-cv-01365-PGR (D. Ariz. filed Aug. 9, 2012) (detailing deficiencies in security measures), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809wyndhamcmpt.pdf (11 PVLR 1069, 7/2/12); Complaint at 9-11, *FTC v. LifeLock, Inc.*, No. 2:10-cv-00530-MGM (D. Ariz. filed Mar. 8, 2010) (same), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2010/03/100309lifelockcmpt.pdf (9 PVLR 386, 3/15/10); Complaint, *In re Lookout Servs., Inc.*, 151 F.T.C. 532, 535 (2011) (same) (10 PVLR 694, 5/9/11); Complaint at 3-4, *In re Reed Elsevier Inc.*, FTC File No. 052 3094, No. C-4226 (F.T.C. July 29, 2008) (same), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2008/08/080801reedcomplaint.pdf (7 PVLR 1192, 8/11/08); Complaint at 2, *In re TJX Cos., Inc.*, FTC File No. 072 3055, No. C-4227, 2 (F.T.C. July 29, 2008) (same), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2008/08/080801tjxcomplaint.pdf (7 PVLR 1192, 8/11/08); Complaint at 2, *In re Guidance Software, Inc.*, FTC File No. 062 3057, No. C-4187 (F.T.C. Mar. 30, 2007) (same), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2007/04/0623057complaint.pdf (5 PVLR 1586, 11/20/06)(5 PVLR 1586, 11/20/06); Complaint at 2, *In re CardSystems Solutions, Inc.*, FTC File No. 052 3148, No. C-4168 (F.T.C. Sept. 5, 2006) (same), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2006/09/0523148cardsystemscomplaint.pdf (5 PVLR 1307, 9/18/06); Complaint, *In re BJ's Wholesale Club, Inc.*, 140 F.T.C. 465, 467 (2005) (same) (4 PVLR 789, 6/20/05).

[40] Kristina Rozan, *How Do Industry Standards for Data Security Match Up With the FTC's Implied ''Reasonable'' Standards—And What Might This Mean for Liability Avoidance?* IAPP Privacy Advisor (Nov. 25, 2014), https://privacyassociation.org/news/a/how-do-industry-standards-for-data-security-match-up-with-the-ftcs-implied-reasonable-standards-and-what-might-this-mean-for-liability-avoidance (''The industry standards for data security are more than just a reference. Indeed, the commission has threatened to take action against companies for 'failure to abide by self-regulatory programs they join.' And according to the FTC, even if 'you don't say anything specific about what you do with users' information . . . Under the law, you still have to take reasonable steps to keep sensitive data secure.' Based on the comparison

  PVLR ISSN 1538-3423

over-relying on what is considered reasonable according to industry. Although deference to industry standards is important, it is not enough to simply enforce only obvious and ubiquitous data security practices. The FTC should push industry ahead in a reasonable and pragmatic manner. It should look for security problems that are significant, and it should look to solutions that have wide support.

Taking on passwords would affect an enormous number of companies, and the FTC might be nervous about putting itself in a position of pushing against very common practices. But the common wisdom about passwords is clearly at odds with current practice. Thus, in some ways such a move would actually be conservative, as the FTC would be following widespread consensus.

Moreover, standards like the National Institute of Standards and Technology's Special Publication (SP) 800-53 and the International Organization for Standardization's ISO 27001 help shape what the FTC considers reasonable,[41] and these standards require more than mere passwords under certain circumstances. NIST has issued authentication guidelines that articulate levels of assurances from 1-4, with assurance escalating according to the level of risk.[42] Level 3, the next to highest level of authentication assurance, provides multi-factor remote network authentication. The FTC should more fully embrace this tiered approach for authentication.

Of course the FTC should not be reckless in requiring robust authentication. Cost and other considerations might caution the agency from requiring stronger authentication outside of contexts involving sensitive data or workforce authentication. Such a broader requirement might require more industry support and adoption rates. But a bold first step for the FTC would be to hold that companies must go beyond passwords for workforce authentication when the data are sensitive.

It is time to start moving beyond the password. The FTC should not kill passwords, but it should not let them continue their reign as the king of authentication. The FTC should make passwords share their throne with better forms of authentication.

---

made here, the industry standards are being used by the FTC to decide what these 'reasonable steps' look like.'').

[41] *Id.*

[42] NIST Special Publication 800-63-2, *Electronic Authentication Guide* (Aug. 2013), *available at* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf.