Washington and Lee Law Review Online

Volume 73 | Issue 2 Article 9

5-1-2017

The Market's Law of Privacy: Case Studies in Privacy/Security Adoption

Chetan Gupta

The Market's Law of Privacy: Case Studies in Privacy/Security Adoption

Chetan Gupta*

Abstract

This paper examines the hypothesis that it may be possible for individual actors in a marketplace to drive the adoption of particular privacy and security standards. It aims to explore the diffusion of privacy and security technologies in the marketplace. Using HTTPS, Two-Factor Authentication, and End-to-End Encryption as case studies, it tries to ascertain which factors are responsible for successful diffusion which improves the privacy of a large number of users. Lastly, it explores whether the FTC may view a widely diffused standard as a necessary security feature for all actors in a particular industry.

Based on the case studies chosen, the paper concludes that while single actors/groups often do drive the adoption of a standard, they tend to be significant players in the industry or otherwise well positioned to drive adoption and diffusion. The openness of a new standard can also contribute significantly to its success. When a privacy standard becomes industry dominant on account of a major actor, the cost to other market participants appears not to affect its diffusion.

A further conclusion is that diffusion is also easiest in consumer facing products when it involves little to no inconvenience to consumers, and is carried out at the back end, yet

* LLB (Hons.), BCL (Oxon.), CIPP/US certified. Admitted to practice in California and in India. This paper was written under the supervision of Professor Chris Hoofnagle at UC Berkeley, and would not have been possible without his mentorship, advice and guidance. I also benefited immensely from discussing this paper with the following persons: Jim Dempsey and Prof. Narechania at the Berkeley Center for Law and Technology, Jeff Jonas at IBM, Elvin Lee at Mozilla, Helena Engfeldt at Baker & McKenzie, Ivan Rossignol, and Babak Slavoshy at Palantir Technologies. However, the views espoused in this paper are my own, and should not be attributed to them or the organizations they represent. A shorter version of this paper has previously appeared in "IEEE Security and Privacy."

results in tangible and visible benefits to consumers, who can then question why other actors in that space are not implementing it. Actors who do not adopt the standard may also potentially face reputational risks on account of non-implementation, and lose out on market share.

Table of Contents

I. Introduction

The *flâneur*[1] Nassim Nicholas Taleb provided the hypothesis for this paper, with his observation that all juice sold in the US is kosher, though only a small percentage of the population insists on kosher products.[2] Taleb hypothesizes that intransigent

1. "The figure of the flâneur [is] the stroller, the passionate wanderer emblematic of nineteenth-century French literary culture." Bijan Stephen, *In Praise of the Flâneur*, PARIS REV. (Oct. 17, 2013), https://www.theparisreview.org/blog/2013/10/17/in-praise-of-the-flaneur/ (last visited Apr. 24, 2017) (on file with the Washington and Lee Law Review). I have never met Mr. Taleb, but I believe he would approve of being described thus, as opposed to an economist, philosopher, intellectual or statistician.

2. *See* Nassim Nicholas Taleb, *The Most Intolerant Wins: The Dictatorship of the Small Minority*, MEDIUM (Aug. 14, 2016), https://medium.com/@nntaleb/the-most-intolerant-wins-the-dictatorship-of-the-

minorities can dictate standards for society as a whole.[3] This is partly due to the permeability of the chosen standard, and its unidirectional/asymmetric nature: kosher populations will only consume kosher products, but the broader population is happy to consume (knowingly or unknowingly) kosher and non-kosher products alike.[4]

This led me to wonder if the same could be said to be true of various privacy and security standards. Can a minority industry actor prompt the adoption of a standard by the broader population? This is a tempting hypothesis, and almost romantic in its appeal. Lone privacy crusaders can stand against the indomitable tide of the information age and single-handedly save society from itself[5]—and from the technology that holds us in thrall.

This paper proposes to examine the adoption patterns of technologies such as HTTPS, End-to-End encryption, and 2 Factor Authentication to see what conclusions can be drawn as to

---

small-minority-3f1f83ce4e15#.706a45fpu (last visited Apr. 24, 2017) ("A strange idea hit me. The Kosher population represents less than three tenth of a percent of the residents of the United States. Yet, it appears that almost all drinks are Kosher.") (on file with the Washington and Lee Law Review).

3. See *id.* ("It suffices for an intransigent minority—a certain type of intransigent minorities—to reach a minutely small level, say three or four percent of the total population, for the entire population to have to submit to their preferences.").

4. *See id.* ("A Kosher (or halal) eater will never eat nonkosher (or nonhalal) food, but a nonkosher eater isn't banned from eating kosher.")

5. Interestingly, empirical studies have shown that while young adults do have a fairly keen appreciation of privacy and value it, they "believe incorrectly that the law protects their privacy online and offline more than it actually does." Chris Jay Hoofnagle, Jennifer King, Su Li & Joseph Turow, *How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies?* 4 (Rose Found. for Communities and the Env't & Annenberg Sch. for Comm., Apr. 14, 2010), *available at* https://ssrn.com/abstract=1589864. I also agree with the hypothesis that privacy harms are viewed as too diffused for individuals to rationally believe that it could happen to them, and to behave accordingly. This is similar to the herd immunity problem with respect to vaccination. *See* CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 222 (2016) ("[T]o enjoy the herd immunity from vaccination, almost everyone must be vaccinated. But individuals who decide to avoid vaccination undermine this herd immunity protection. For these individuals, avoidance of vaccines is rational, so long as they can still benefit from herd immunity."); Deirdre K. Mulligan & Fred B. Schneider, *Doctrine for Cybersecurity*, 140 DÆDALUS 70, 76 (2011) (discussing the herd immunity problem).

their uptake, the factors that drove their implementation, and the role of various market participants in their adoption. Through these case studies I hope to examine situations in which the market created (or failed to create) privacy enhancing standards.

On the legal side, the adoption of privacy/security technologies can have implications for their regulation. Standards need not be set by regulatory bodies such as the FTC,[6] but can organically evolve within an industry as long as there is some diversity in attitudes towards privacy. Alternatively, it could also mean that once a standard is widely diffused, industry actors who fail to adopt or implement it are subject to regulation by the FTC under the "unfairness" doctrine. In the 2015 case of *Wyndham*,[7] the FTC brought an action against the defendant for insecure data practices under both the "unfairness" and "deception" doctrines.[8] In the Internet of Things (IoT) space, also, the FTC appears to be stepping up enforcement against companies that fail to secure their products against what the FTC views as market standards for privacy/security. For example, on January 5, 2017, the FTC brought a complaint in federal court against D-Link[9] for failing to secure its routers and IoT cameras.[10] The FTC has alleged that failures to secure the private key used to sign the defendant's software, and storing login credentials as plain text on users' mobile devices, are both practices which do not follow established market security standards, and has brought an 'unfairness' action under Section 5 of the FTC Act on this basis.[11]

---

6. US privacy avoids a prescriptive approach in general, with regulatory bodies and statutes preferring to hold regulated entities to some variant of a "reasonable measures" standard. Chandeni K. Gill, Note, *Patron Data Privacy and Security in the Casino Industry: A Case for A U.S. Data Privacy Statute*, 3 UNLV GAMING L.J. 81, 107 (2012).

7. FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015).

8. *See id.* at 240 ("The FTC filed suit in federal District Court, alleging that Wyndham's conduct was an unfair practice and that its privacy policy was deceptive.").

9. Complaint, FTC v. D-Link Corp., No. 3:17-cv-00039 (N.D. Cal. Jan. 5, 2017).

10. *Id.* at 2.

11. *See generally id.* (alleging that D-Link's practices are unfair and deceptive).

The hypothesis of particular market participants driving adoption is partially illustrated on a grander scale by the forthcoming European General Data Protection Regulation (GDPR) regime.[12] The GDPR will lead to the world catering to the European conception of privacy and its associated safeguards, such as privacy by design (PbD). The diffusion of the GDPR standard will be driven by the large market segment that Europe represents. It is the 800-pound (kosher eating) gorilla in the privacy room.

We can now consider how well the hypothesis works with respect to other privacy and security standards.

II. "One of the Greatest Tragedies of Life is the Murder of Beautiful Theory by a Gang of Brutal Facts."[13]

Tempting as the hypothesis was, searching for real world examples soon made it clear that the diffusion of privacy/security standards worked slightly differently. While single actors/groups often do drive the adoption of a standard, they tend to be significant players in the industry or otherwise well positioned to drive adoption and diffusion.[14] The openness of a new standard can also contribute significantly to its success.[15] When a privacy standard becomes industry dominant on account of a major actor,

---

12. Regulation 2016/679 of the European Parliament and of the Council of the European Union on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 2016 O.J. L. 119 [hereinafter GDPR], *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&qid=1490558317324&from=en.

13. Variously attributed to Ben Franklin and to Thomas H. Huxley, who wrote: "[T]he great tragedy of Science—the slaying of a beautiful hypothesis by an ugly fact." JOHN BARTLETT, FAMILIAR QUOTATIONS 505 (16th ed., Justin Kaplan ed., 1992) (quoting THOMAS H. HUXLEY, BIOGENESIS AND ABIOGENESIS (1870)).

14. This is in line with Carl Shapiro's hypothesis in *Information Rules* that established players who have achieved a degree of lock-in are better able to influence standards and adoption. *See* CARL SHAPIRO & HAL R. VARIAN, INFORMATION RULES: A STRATEGIC GUIDE TO THE NETWORK ECONOMY 235–36 (1999) (discussing how "established incumbents" can influence technology standards).

15. *See id.* at 201 ("In some industries with strong network characteristics, full openness is the only feasible approach.").

the cost to other market participants appears not to affect its diffusion. This should be distinguished from "cost" to consumers, both in monetary terms and in terms of convenience.

Diffusion is also easiest in consumer facing products when it involves little to no inconvenience to consumers, and is carried out at the back end, yet results in tangible and visible benefits to consumers, who can then question why other actors in that space are not implementing it. Actors who do not adopt the standard may also potentially face reputational risks on account of non-implementation, and lose out on market share.[16]

We can see how these findings are borne out by case studies in the next section.

III. Case Studies

a) HTTPS v. HTTP

The Hyper Text Transfer Protocol (HTTP) was the default data communication protocol for the Internet. HTTP is not encrypted and is vulnerable to man-in-the-middle and eavesdropping attacks, which can let attackers gain access to website accounts and sensitive information and modify web pages to inject malware or advertisements.[17]

Hypertext Transfer Protocol Secure (HTTPS) encrypts data and is designed to withstand such attacks and is considered secure against them.[18] Interestingly, HTTPS has been around

---

16. Early adopters/first movers can design systems that play this to their advantage. SMSs received from (presumptively less secure) Android phones on (presumptively more secure) iPhones show up in a different color than messages from other iPhones. *See* Paul Ford, *It's Kind of Cheesy Being Green*, MEDIUM (Feb. 11, 2015), https://medium.com/message/its-kind-of-cheesy-being-green-2c72cc9e5eda#.jyaft5ots (last visited Apr. 24, 2017) (noting that "Apple uses a soothing, on-brand blue for messages in its own texting platform, and a green akin to that of the Android robot logo for people texting from outside its ecosystem") (on file with the Washington and Lee Law Review). The presumptively less secure messages were described to me as "puke green."

17. *See* Tony Messer, *HTTP vs. HTTPS: What's the Difference and Why Should You Care?*, ENTREPRENEUR (Sept. 15, 2016), https://www.entrepreneur.com/article/281633 (last visited Apr. 24, 2017) (discussing the vulnerabilities of the HTTP protocol) (on file with the Washington and Lee Law Review).

18. *See* Michael Hernandez, *HTTP vs. HTTPS for SEO: What You Need to*

since 1994, when Netscape Communications created HTTPS for its Netscape Navigator web browser.[19] The current version of HTTPS was formally specified in May 2000.[20] Yet adoption was not widespread, and its historical use was limited to payment transactions and other sensitive transactions in corporate information systems.[21]

On August 6, 2014, Google announced that it would start using the fact of whether a website had implemented HTTPS as a search engine optimization (SEO) criterion.[22] Simply put, if your website is on HTTPS, it is more likely to show up in a google search and be higher in the list of results.

After this, there was a rapid uptake in the implementation of HTTPS. Google proceeded to name and shame the top 100 (in web traffic terms) sites by documenting their HTTPS status in its Transparency Report.[23] In December 2014, Google advocated displaying visual browser signals to users to let them know whether the sites they were visiting were on HTTP or HTTPS.[24]

Know to Stay in Google's Good Graces, AHREFS BLOG (Aug. 13, 2015), https://ahrefs.com/blog/http-vs-https-for-seo/ (last visited Apr. 24, 2017) ("Data sent using HTTPS is secured via Transport Layer Security protocol (TLS), which provides three key layers of protection: [encryption, data integrity, and authentication].") (on file with the Washington and Lee Law Review).

19. *See* COLIN WALLS, EMBEDDED SOFTWARE: THE WORKS 344 (2005) (discussing the early history of HTTPS).

20. *Id.*

21. *See HTTPS*, DDOS-GUARD, https://ddos-guard.net/en/info/knowledge/https (last visited Apr. 24, 2017) ("Historically, HTTPS connections were primarily used for payment transactions on the World Wide Web, e-mail and for sensitive transactions in corporate information systems.") (on file with the Washington and Lee Law Review).

22. Zineb Ait Bahajji & Gary Illyes, *HTTPS as a Ranking Signal*, GOOGLE WEBMASTER CENTRAL BLOG (Aug. 6, 2014), https://webmasters.googleblog.com/2014/08/https-as-ranking-signal.html (last visited Apr. 24, 2017) (on file with the Washington and Lee Law Review).

23. *HTTPS on Top Sites*, GOOGLE TRANSPARENCY REP., https://www.google.com/transparencyreport/https/grid/ (last visited Apr. 24, 2017) (on file with the Washington and Lee Law Review).

24. *See* Gregg Keizer, *Google Wants to Turn Browser Signals of Web Encryption Upside Down*, COMPUTERWORLD (Dec. 22, 2014, 3:50 AM), http://www.computerworld.com/article/2861583/google-wants-to-turn-browser-signals-of-web-encryption-upside-down.html (last visited Apr. 24, 2017) ("Chrome security engineers have proposed that all websites that don't encrypt traffic be marked as insecure by browsers.") (on file with the Washington and Lee Law Review).

Google Chrome then began displaying a green lock next to websites that were secure on account of using HTTPS; Firefox and Internet Explorer did the same.[25]

When this paper was written in November 2016, Google indicated that 52% of all web pages loaded worldwide on Windows machines are on HTTPS; the figure is 61% for Macs, 55% for Linux, and 43% for Android.[26] The more telling figure is the percentage of browsing time spent on HTTPS sites, that is, the sites that users actually interact with significantly on HTTPS.[27] This figure is 69% for Windows, 71% for Macs, 80% for Linux, and 41% for Android.[28] Google's data is summarized in Table 1 below.

Table 1: HTTPS Uptake[29]

OS	**Percentage of web pages loaded on HTTPS in March 2015**	**Percentage of web pages loaded on HTTPS as of January 2017**	**Percentage of Browsing Time Spent on HTTPS Websites as of January 2017**
Windows	39%	52%	70%
Mac	43%	61%	72%
Android	29%	45%	43%

25. *See* Messer, *supra* note 17 (noting the "green" symbol in browsers' URL bars that indicates whether the website uses the HTTP or HTTPS protocol). Iconography seems to play an important role in privacy UX design, with designers almost seeming to want to appeal to some subliminal Neanderthal part of our brains using color signaling. For more on this idea, see *supra* note 5.

26. *HTTPS Usage*, GOOGLE TRANSPARENCY REP., https://www.google.com/transparencyreport/https/metrics/?hl=en (last visited Apr. 24, 2017) (on file with the Washington and Lee Law Review).

27. As Gary Illyes, Google Webmaster Trends Analyst, pointed out in response to an article suggesting that the overall web adoption of HTTPS was still low, "it's more important to have the sites people actually use to be https. Not all live domains are actually 'sites.'" Gray Illyes (@methode), Twitter (Feb. 18, 2016 3:49 PM), https://twitter.com/methode/status/700406914639753216.

28. *HTTPS Usage*, *supra* note 26.

29. The data in the table is derived from Google. *Id.*

Linux	44%	54%	81%
Chrome OS	45%	65%	75%

Anecdotally, consider how many of the links in this paper are to HTTPS sites compared to HTTP!

Migration to HTTPS is non-trivial, particularly for sites that host content from a variety of sources, such as advertisements or other partners, as all such external content also needs to be on HTTPS for Google Chrome and other browsers to mark such sites as totally secure.[30] Otherwise, some variety of mixed content warning is displayed by browsers, such as a cross across a padlock or a red padlock.[31] As of January 2017, Google Chrome has started displaying the words "Secure" or "Not Secure" in the address bar depending on whether HTTPS is being used.[32]

HTTPS requires a SSL certificate from a Certifying Authority (CA) in order to be implemented.[33] Services such as Let's Encrypt (backed by Google incidentally) offer such certificates for free, but other providers such as Symantec charge $1,499 per year for such certificates.[34] "[E]ncrypting the

30. *See* Brian Barret, *Most Top Websites Still Don't Use a Basic Security Feature*, WIRED (Mar. 17, 2016, 8:00 AM), https://www.wired.com/2016/03/https-adoption-google-report/ (last visited Apr. 24, 2017) ("For smaller sites, HTTPS can be a relatively simple thing to embrace; if they don't implement it, it's largely because they simply don't care to. The more moving parts a site has, though, the trickier it gets.") (on file with the Washington and Lee Law Review).

31. *See, e.g.*, *Check if a Site's Connection is Secure*, CHROME HELP, https://support.google.com/chrome/answer/95617?hl=en (last visited Apr. 24, 2017) (providing the icons used in connection with a web page's security status) (on file with the Washington and Lee Law Review).

32. Danielle Wiener-Bronne, *Google Will Soon Call Out Websites for Not Being Secure*, CNN TECH (Sept. 9, 2016, 6:34 PM), http://money.cnn.com/2016/09/08/technology/google-chrome-flag-non-secure-sites/ (last visited Apr. 24, 2017) (on file with the Washington and Lee Law Review). Interestingly, CNN's own site is not marked as "Not Secure" at the time of this paper's writing.

33. *See* Messer, *supra* note 17 ("If you are familiar with the backend of a website, then switching to HTTPS is fairly straightforward in practice. The basic steps are as follows. 1. Purchase an SSL certificate and a dedicated IP address from your hosting company.")

34. *See Compare and Buy SSL Certificates*, SYMANTEC, https://www.symantec.com/page.jsp%3Fid%3Dcompare-ssl-certificates (last visited Apr. 24, 2017) (providing the prices of Symantec's SSL services) (on file

transferred data—and especially the initial handshake to enable encryption—does costs bandwidth and CPU cycles."[35] "For large websites these minor costs might add up to a substantial amount."[36]

Google provides helpful guides on how websites can transition to HTTPS, and as noted above found several ways to nudge adoption.[37] Carl Shapiro has hypothesized that open standards facilitate adoption, and where multiple standards exist, adoption follows a S-shaped curve, with rapid uptake once a market standard emerges, plateauing once market saturation is achieved.[38] This certainly seems to be true of HTTPS, as the increase in usage from March 2015 to January 2017 set out in Table 1 would demonstrate.[39] There seems to be a 10–20% increase in implementation of HTTPS across all major operating systems in less than a year. Let's Encrypt reports that when it launched in December 2015, 39.5% of page loads on the Web used HTTPS (as measured by Firefox Telemetry).[40] That number stood at 45% as of June 2016.[41]

What is the takeaway from all of this? Once a major actor decided to drive adoption, and was well situated to do so, significant privacy and security benefits were delivered to consumers, with no action or effort required on their part. Google was well situated to drive adoption, both as a web traffic funnel,

---

with the Washington and Lee Law Review).

35. Christoph Engelhardt, *We Analyzed the HTTPS Settings of 10,000 Domains and How It Affects Their SEO—Here's What We Learned*, AHREFS BLOG (Feb. 17, 2016), https://ahrefs.com/blog/ssl/ (last visited Apr. 24, 2017) (on file with the Washington and Lee Law Review).

36. *Id.*

37. *See Secure Your Site with HTTPS*, GOOGLE SEARCH CONSOLE HELP, https://support.google.com/webmasters/answer/6073543?hl=en (last visited Apr. 24, 2017) (instructing site owners how to implement the HTTPS protocol) (on file with the Washington and Lee Law Review).

38. *See* SHAPIRO & VARIAN, *supra* note 14, at 180 (noting that "the popular product with many compatible users becomes more and more valuable to each user as it attracts ever more users").

39. *Supra* note 29 and accompanying text.

40. Josh Aas, *Progress Towards 100% HTTPS, June 2016*, LET'S ENCRYPT (June 22, 2016), https://letsencrypt.org/2016/06/22/https-progress-june-2016.html (last visited Apr. 24, 2017) ((on file with the Washington and Lee Law Review).

41. *Id.*

and on account of being the designer of a very popular web browser. Google Chrome has a 59.24% market share as of October 2016.[42]

I predict that we will see a very similar scenario play out with respect to Extended Validation (EV) SSL certificates and Certificate Transparency (CT). "The [EV] identity verification process requires" an entity "to prove exclusive rights to use a domain, confirm its legal, operational and physical existence, and prove the entity has authorized the issuance of the Certificate."[43]

CT is another Google initiative meant to deal with the problem of wrongly issued certificates, and was prompted by several security incidents caused by fraudulent certificates, the most notorious of which was the DigiNotar incident in 2011.[44] The hacked DigiNotar certificates were used to impersonate numerous sites in Iran, such as Gmail and Facebook, which enabled the operators of the fake sites to spy on unsuspecting site users.[45]

As explained on the CT website, which seems to be backed by Google:

> Certificate Transparency aims to remedy these certificate-based threats by making the issuance and existence of SSL

---

42. *Browser Market Share Worldwide*, STATCOUNTER, http://gs.statcounter.com/?PHPSESSID=37o3614ksusp3gttc6kni7a461 (last visited Apr. 24, 2017) (on file with the Washington and Lee Law Review).

43. *What is an Extended Validation Certificate?*, GLOBALSIGN, https://www.globalsign.com/en/ssl-information-center/what-is-an-extended-validation-certificate/ (last visited Apr. 24, 2017) (on file with the Washington and Lee Law Review).

44. *See* Josephine Wolff, *How a 2011 Hack You've Never Heard of Changed the Internet's Infrastructure*, SLATE (Dec. 21, 2016, 11:00 AM), http://www.slate.com/articles/technology/future_tense/2016/12/how_the_2011_hack_of_diginotar_changed_the_internet_s_infrastructure.html (last visited Apr. 24, 2017) ("[DigiNotar's] whole reason for existence was to tell internet users who and what they could trust—and in 2011, it failed spectacularly in that mission.") (on file with the Washington and Lee Law Review).

45. See *id.*

> Thousands of Iranians who tried to visit Google websites in August 2011 were apparently redirected to sites that looked like Google webpages and were also certified as belonging to Google according to certificates issued by DigiNotar. . . . Why bother redirecting hundreds of thousands of Iranian Google users to fraudulent websites? Probably in order to read their email.

> certificates open to scrutiny by domain owners, CAs, and domain users. Specifically, Certificate Transparency has three main goals:
>
> - Make it impossible (or at least very difficult) for a CA to issue a SSL certificate for a domain without the certificate being visible to the owner of that domain.
> - Provide an open auditing and monitoring system that lets any domain owner or CA determine whether certificates have been mistakenly or maliciously issued.
> - Protect users (as much as possible) from being duped by certificates that were mistakenly or maliciously issued.
>
> Certificate Transparency satisfies these goals by creating an open framework for monitoring the TLS/SSL certificate system and auditing specific TLS/SSL certificates.[46]

If a website has an EV certificate and CT, you will see the full name of the entity in the address bar in green in Google Chrome, along with a green padlock. For example, Twitter.com displays as "Twitter, Inc. (US)," followed by the HTTPS URL.[47]

Google published a CT Policy in May 2016,[48] and Facebook has also advocated for the standard after discovering flaws in some of its own certificates in April 2016.[49] CAs price EV certificates at $599 per year,[50] and tout claims such as "the green

---

46. *What is Certificate Transparency?*, CERTIFICATION TRANSPARENCY, https://www.certificate-transparency.org/what-is-ct (last visited Apr. 12, 2017) (on file with the Washington and Lee Law Review). Ironically, this site is on HTTP and has no EV.

47. TWITTER, https://twitter.com/ (last visited Apr. 24, 2017) (on file with the Washington and Lee Law Review).

48. *See* Ryan Sleevi, *New CT Policy for Chrome Published - May 2016*, CABFPUB (May 4, 2016), https://cabforum.org/pipermail/public/2016-May/007573.html (last visited Apr. 24, 2017) (discussing Google's CT Policy) (on file with the Washington and Lee Law Review).

49. *See* Protect the Graph, *Early Impacts of Certificate Transparency*, FACEBOOK (Apr. 11, 2016), https://www.facebook.com/notes/protect-the-graph/early-impacts-of-certificate-transparency/1709731569266987/ (last visited Apr. 24, 2017) ("Facebook advocates for CT because it offers the ability to know the certificates a CT-enforcing browser will trust.") (on file with the Washington and Lee Law Review).

50. *What is an Extended Validation Certificate?*, *supra* note 43.

bar is proven to increase the feeling of security in 60% of shoppers."[51]

EV as a standard has been around since 2007,[52] but for the same reasons as the rapid increase in HTTPS implementation, I anticipate that it will take off and become the dominant certificate standard over the next couple of years. The only publicly available data shows that in January 2015, EV certificates accounted for only 5% of all certificates.[53]

b) It's Not About the Privacy Stupid (?)

As a coda, HTTPS has the (unintended?) benefit of preserving referrer data (where you landed on the website from) as long as you reached that page through another HTTPS page.[54] If you land on that page from a HTTP page, such referrer data is stripped away, and you are perceived as a "direct" traffic to the new page.[55]

In the world of advertising, referrer data is tremendously valuable information, and would be a factor for pricing and serving online ads. Google's ads engine is its largest single revenue source, and has been described as practically a license to print money.[56] In 2015, Google's revenue amounted to $74.54

---

51. *Extended Validation (EV) SSL Certificates*, SSL STORE, https://www.thesslstore.com/extended-validation-ssl-certificates.aspx (last visited Apr. 24, 2017) (on file with the Washington and Lee Law Review). One wonders what the FTC would make of that last claim!

52. ENTRUST DATACARD, THE BUSINESS VALUE OF EXTENDED VALIDATION 3 (2015), https://www.entrust.com/wp-content/uploads/2015/08/WP-Extended-Validation-Business-Benefits-FEB16-WEB.pdf.

53. *SSL Survey*, NETCRAFT, https://www.netcraft.com/internet-data-mining/ssl-survey/ (last visited Apr. 24, 2017) (on file with the Washington and Lee Law Review).

54. *See* Hernandez, *supra* note 18 ("When traffic passes to an HTTPS site, the secure referral information is preserved.").

55. *See id.* ("[W]hen traffic passes through an HTTP site . . . it is stripped away and looks as though it is 'direct.'"). HTTP to HTTP traffic has referrer data, as does HTTPS to HTTPS, but HTTP to HTTPS does not.

56. *See generally* ANTONIO GARCÍA MARTÍNEZ, CHAOS MONKEYS: OBSCENE FORTUNE AND RANDOM FAILURE IN SILICON VALLEY (2016) for a fascinating insight into the evolution of online advertising, ad exchange mechanisms, and the role they play in dictating the business strategies of companies such as Google, Facebook and Twitter. Though *jejune* in other respects, the book serves

billion, of which $67.39 billion was advertising revenue.[57] In this respect, widespread HTTPS adoption is arguably a less secure outcome for the end user, since it allows the users immediate browsing history to be shared between sites. Yet, it appears to have been widely adopted because of Google's efforts and popular attention focusing on benefits rather than drawbacks.

c) End-to-End Encryption (E2EE) for Instant Messaging Apps

E2EE results in messages being encrypted between the end users of instant messaging (IM) apps, rather than being sent as insecure plain text.[58] When correctly implemented, only users can read the messages, to the exclusion of the entity which operates the app, their mobile service provider, and governments.[59] A less secure version of encryption only encrypts data between the user and the chat server; this is known as encryption in transit.[60] As in the case of HTTPS, when Whatsapp introduced E2EE in

---

as a great primer on the online ad world.

57. *Google's Revenue Worldwide from 2002 to 2016 (in Billion U.S. Dollars)*, STATISTA, https://www.statista.com/statistics/266206/googles-annual-global-revenue/ (last visited Apr. 24, 2017) (on file with the Washington and Lee Law Review).

58. *See* Andry Greenberg, *Hacker Lexicon: What Is End-to-End Encryption?*, WIRED (Nov. 25, 2014, 9:00 AM), https://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/ (last visited Apr. 24, 2017) (noting that E2E "means that messages are encrypted in a way that allows only the unique recipient of a message to decrypt it, and not anyone in between") (on file with the Washington and Lee Law Review).

59. It is important to note that messages can still be accessed by third parties if they are unencrypted "at rest" on the user's device itself. My friend Alex Urbelis thinks this is what happened with Whatsapp and the Turkish coup attempt, where End-to-End encrypted messages from the coup were published by the government. *See* Jeremy Seth Davis, *WhatsApp in the Spotlight After Turkey Publishes Messages of Coup Officers*, SC MEDIA (July 25, 2016), https://www.scmagazine.com/whatsapp-in-the-spotlight-after-turkey-publishes-messages-of-coup-officers/article/529892/ (last visited Apr. 24, 2017) (detailing the incident) (on file with the Washington and Lee Law Review).

60. *See* Barb Darrow, *Security in a Time of Breaches? Microsoft Touts Beefed-up Database Encryption*, FORTUNE (May 27, 2015), http://fortune.com/2015/05/27/microsoft-sql-server-2016-encryption/ (last visited Apr. 24, 2017) (defining encryption in transit) (on file with the Washington and Lee Law Review).

November 2014[61] and delivered enhanced security for over 1 billion users, the technology was neither novel by itself, nor was it new to the IM space. Services such as Jabber had offered E2EE for many years prior to Whatsapp introducing it.[62] Apple's iMessage and twenty other IM apps out of the thirty-seven surveyed by the EFF in November 2014 offered E2EE.[63] Jabber was part of Edward Snowden's toolkit,[64] but consider how involved and convoluted the instructions were for setting up secure IM communications as late as July 2015.[65]

However, as with HTTPS, in terms of market dominance and standard diffusion, the relevant metric is the actual number of people who end up benefitting from a more secure standard. Whatsapp has a billion users.[66] Strikingly, Viber, which has 823 million users, implemented E2EE on April 19, 2016,[67] only

---

61. *See* moxie0, *Open Whisper Systems Partners with WhatsApp to Provide End-to-End Encryption*, OPEN WHISPER SYS. (Nov. 18, 2014), https://whispersystems.org/blog/whatsapp/ (last visited Apr. 24, 2017) ("Today we're excited to publicly announce a partnership with WhatsApp, the most popular messaging app in the world, to incorporate the TextSecure protocol into their clients and provide end-to-end encryption for their users by default.") (on file with the Washington and Lee Law Review). Whatsapp used the developers of Signal to help them implement E2EE. Though Signal may not have itself prompted the adoption of E2EE in IM apps, it offered an off the shelf solution when larger players did look to implement E2EE.

62. *See Frequently Asked Questions*, JABBER, https://www.jabber.org/faq.html (last visited Apr. 24, 2017) (detailing Jabber's encryption offerings) (on file with the Washington and Lee Law Review).

63. *Secure Messaging Scorecard*, EFF, https://www.eff.org/node/82654 (last updated Apr. 5, 2016) (last visited Apr. 24, 2017) (on file with the Washington and Lee Law Review).

64. I would surmise that the Snowden revelations were a key reason for many IM app developers to actually implement E2EE. This sits nicely with my original hypothesis as well.

65. *See* Micah Lee, *Chatting in Secret While We're All Being Watched*, INTERCEPT (July 14, 2015), https://theintercept.com/2015/07/14/communicating-secret-watched/ (last visited Apr. 24, 2017) (providing such instructions) (on file with the Washington and Lee Law Review).

66. Joon Ian Wong, *WhatsApp has a Billion Users, and It got There Way Quicker than Gmail Did*, QUARTZ (Feb. 2, 2016), https://qz.com/608014/whatsapp-has-a-billion-users-and-it-got-there-way-quicker-than-gmail-did (last visited Apr. 24, 2017) (on file with the Washington and Lee Law Review).

67. Michael Shmilov, *Giving Our Users Control Over Their Private Conversations*, VIBER BLOG (Apr. 19, 2016), https://www.viber.com/en/blog/2016-04-19/giving-our-users-control-over-their-private-conversations (last visited Apr.

fourteen days after Whatsapp completed rolling it out on April 5, 2016.[68] Though Viber claimed it had been working on E2EE for a long time, the timing is extraordinary. The following table summarizes E2EE/encryption in transit adoption among popular (in terms of number of users) IM apps:

Table 2: E2EE in IM Apps

App	**Users**	**Launch Date**	**E2EE Opt In or Default**	**E2EE Adoption Date**
Whatsapp	1 billion	January 2010	Default	Rollout started in November 2014. Completed on April 5, 2016.[69]
Facebook Messenger	900 million	August 2011	Opt In	October 2016[70]
Tencent QQ Mobile	883 million	February 1999	No E2EE. Encryption in Transit	March 2016[71]
Viber	823 million	December 2, 2010	Default	April 19,2016[72]

24, 2017) (on file with the Washington and Lee Law Review).

68. Jan & Brian, *End-to-End Encryption*, WHATSAPP BLOG (Apr. 5, 2016), https://blog.whatsapp.com/10000618/end-to-end-encryption (last visited Apr. 24, 2017) (on file with the Washington and Lee Law Review).

69. *Id.*

70. *See* Andy Greenberg, *You Can All Finally Encrypt Facebook Messenger, So Do It*, WIRED (Oct. 4, 2016), https://www.wired.com/2016/10/facebook-completely-encrypted-messenger-update-now (last visited Apr. 24, 2017) (discussing Facebook's introduction of encryption on its Messenger app, but noting that "the opt-in move has also drawn the scorn of privacy advocates") (on file with the Washington and Lee Law Review). Apr. 24, 2017

71. *Secure Messaging Scorecard*, *supra* note 63.

72. Shmilov, *supra* note 67.

Line	211 million	June 23, 2011	Default	October 2015[73]
Apple iMessage	>320 million [74]	October 12, 2011	Default	At Launch
Signal (earlier known as TextSecure)	1–5 million [75]	February 2014	Default	At Launch[76]

d) Two-Factor Authentication (2FA)

2FA requires users of a service to sign in using at least two of the following: something they know (their password for example), something they have (a code sent to their registered cell phone, a RFID token), and something they are (typically biometric fingerprint or iris scans).[77]

2FA provides significantly enhanced security by being an effective foil to password hacks or disclosures. Mat Honan is a

---

73. *LINE Introduces Letter Sealing Feature for Advanced Security*, LINE (Oct. 13, 2015), https://linecorp.com/en/pr/news/en/2015/1107 (last visited Apr. 24, 2017) (on file with the Washington and Lee Law Review).

74. The 320 million figure is from mid-2013 and represents the number of iCloud accounts linked to iMessage. Juli Clover, *Apple Handles 'Several Billion' iMessages and 15 to 20 Million FaceTime Calls Daily*, MACRUMORS (Feb. 28, 2014, 9:49 AM), http://www.macrumors.com/2014/02/28/apple-40-billion-imessages/ (last updated Feb. 28, 2014, 12:46 PM) (last visited Apr. 24, 2017) (on file with the Washington and Lee Law Review).Apr. 24, 2017

75. Micah Lee, *Battle of the Secure Messaging Apps: How Signal Beats Whatsapp*, INTERCEPT (June 22, 2016), https://theintercept.com/2016/06/22/battle-of-the-secure-messaging-apps-how-signal-beats-whatsapp/ (last visited Apr. 24, 2017) (on file with the Washington and Lee Law Review).

76. Michael Mimoso, *New Signal App Brings Encrypted Calling to iPhone*, THREAT POST (July 29, 2014), https://threatpost.com/new-signal-app-brings-encrypted-calling-to-iphone/107491/ (last visited Apr. 24, 2017) (on file with the Washington and Lee Law Review).

77. *See generally* Seth Rosenblatt & Jason Cipriani, *Two-factor Authentication: What You Need to Know (FAQ)*, CNET (July 15, 2015, 1:39 PM), https://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq/ (last visited Apr. 24, 2017) (explaining two-factor authentication) (on file with the Washington and Lee Law Review).

technology journalist who writes for WIRED; in August 2012, using a single hacked password, attackers were able to take over Mat Honan's "entire digital life."[78] Mat's hacking raised questions about account security, and he stated that if his accounts had been protected by 2FA, the attackers would never have gotten as far as they did.[79]

A large variety of sites and services implement 2FA, including LinkedIn, Dropbox, Apple, Facebook, Twitter, PayPal, Yahoo Mail, Steam and Microsoft Accounts.[80] As currently implemented by most popular service providers, 2FA is opt in rather than the default choice.[81]

Google introduced 2FA for its accounts in February 2011,[82] and nearly a quarter million Google account users chose to enable 2FA in the two days after the Mat Honan story broke.[83] While, no

---

78. *See* Mat Honan, *How Apple and Amazon Security Flaws Led to My Epic Hacking*, WIRED (Aug. 8, 2016, 8:01 PM), https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/ (last visited Apr. 24, 2017) ("First my Google account was taken over, then deleted. Next my Twitter account was compromised . . . . And worst of all, my AppleID account was broken into, and my hackers used it to remotely erase all of the data on my iPhone, iPad, and MacBook.") (on file with the Washington and Lee Law Review).

79. *See id.* ("Had I used two-factor authentication for my Google account, it's possible that none of this would have happened, because their ultimate goal was always to take over my Twitter account and wreak havoc.").

80. *See* Bill Garner, *Here's Everywhere You Should Enable Two-Factor Authentication Right Now*, LINKEDIN (Sept. 13, 2014), https://www.linkedin.com/pulse/20140930132117-13789516-here-s-everywhere-you-should-enable-two-factor-authentication-right-now (last visited Apr. 24, 2017) (listing "services that support two-factor authentication") (on file with the Washington and Lee Law Review).

81. On how to implement 2FA on the services that provide them, see *id.*

82. *See Advanced Sign-in Security for Your Google Account*, GOOGLE OFFICIAL BLOG (Feb. 10, 2011), https://googleblog.blogspot.com/2011/02/advanced-sign-in-security-for-your.html (last visited Apr. 24, 2017) ("[W]e've developed an advanced opt-in security feature called 2-step verification that makes your Google Account significantly more secure by helping to verify that you're the real owner of your account.") (on file with the Washington and Lee Law Review).

83. *See* Duo Labs, *Estimating Google's Two-Factor (2SV) Adoption with Pen, Paper, and Poor Math*, DUO (May 15, 2015), https://duo.com/blog/estimating-googles-two-factor-2sv-adoption (last visited Apr. 24, 2017) ("Despite having very low adoption rates in terms of % of total users, large service providers like Google, Microsoft, Apple, etc have hundreds of million[s] of users, dwarfing the 2FA deployments of even the largest enterprise

official numbers are available from Google, a 2015 guesstimate suggests that only 6.5% of Google's 600 million users use 2FA.[84] A published 2015 study, which tried to reset Google accounts to test if they had 2FA enabled, came up with a 6.4% estimate.[85]

Given the palpable benefits of this more secure standard, why isn't it the default industry norm? I would argue that the inconvenience threshold for standard adoption is pretty low. Even minor actual or perceived inconvenience to users hampers the adoption of a security standard. Scientific studies have shown that ease of use and required cognitive effort are both relevant factors in 2FA implementation.[86] I do not see 2FA becoming a market dominating standard unless the inconvenience cost is significantly lowered for end users.[87]

The following table summarizes available adoption data for 2FA:

---

use cases.") (on file with the Washington and Lee Law Review).

84. *Id.*

85. THANASIS PETSAS, GIORGOS TSIRANTONAKIS, ELIAS ATHANASOPOULOS & SOTIRIS IOANNIDIS, FORTH, TWO-FACTOR AUTHENTICATION: IS THE WORLD READY? QUANTIFYING 2FA ADOPTION 1 (2015), www.necoma-project.eu/m/filer_public/61/96/6196fc57-324b-490e-b958-44111220656a/eurosec15.pdf.

86. *See* EMILIANO DE CRISTOFARO, HONGLU DU, JULIEN FREUDIGER & GREG NORCIE, PARC, A COMPARATIVE USABILITY STUDY OF TWO-FACTOR AUTHENTICATION 2, https://pdfs.semanticscholar.org/a3d8/fab13263998bf2bbbb57f2d2d028aaae6719.pdf (finding "that three metrics—ease-of-use, required cognitive efforts, and trustworthiness—are enough to capture key factors affecting the usability of 2F technologies").

87. Tellingly, the adoption rate for 2FA on the enterprise side was more than 30% in 2014. *See More Enterprises Plan to Strengthen Access Security with Multi-factor Authentication*, GEMALTO (May 21, 2014), https://safenet.gemalto.com/news/2014/authentication-survey-2014-reveals-more-enterprises-adopting-multi-factor-authentication/ (last visited Apr. 24, 2017) ("37 percent of organizations now use [2FA] for a majority of employees—up from 30 percent last year.") (on file with the Washington and Lee Law Review). Users on the enterprise side, of course, do not enjoy autonomy in deciding whether or not to use 2FA since, when implemented, it is the default and only option, rather than an opt in. RAND published an NIST sponsored study on 2FA adoption on the enterprise side, which found that "user resistance after implementation is a nonissue" within organizations. *See* Martin C. Libicki, Edward Balkovich, Brian A. Jackson, Rena Rudavsky & Katharine Watkins Webb, *Influences on the Adoption of Multifactor Authentication*, RAND CORP. (2011), http://www.rand.org/pubs/technical_reports/TR937.html (last visited Apr. 24, 2017) (providing a link to a copy of the study) (on file with the Washington and Lee Law Review).

Table 3: 2FA Adoption

Service	**2FA Adoption Date**	**Users**	**Users who have enabled 2FA**
Google	February 2011	600 million estimated	6.4–6.5% estimated[88]
Twitter	May 2013[89]	317 million estimated[90]	0.5-2% estimated[91]

88. *See supra* notes 83–85 and accompanying text (discussing estimates of Google 2FA usage).

89. *See* jimio, *Getting Started with Login Verification*, TWITTER (May 22, 2013), https://blog.twitter.com/2013/getting-started-with-login-verification (last visited Apr. 24, 2017) ("Today we're introducing a new security feature to better protect your Twitter account: login verification.") (on file with the Washington and Lee Law Review). 2FA was implemented after a major hack in February 2013 which affected 250,000 accounts. For a detailed account of that hack, see Cass Jones, *Twitter Says 250,000 Accounts have been Hacked in Security Breach*, GUARDIAN (Feb. 1, 2013), https://www.theguardian.com/technology/2013/feb/02/twitter-hacked-accounts-reset-security (last visited Apr. 24, 2017) (on file with the Washington and Lee Law Review).

90. *Number of Monthly Active Twitter Users Worldwide from 1st Quarter 2010 to 4th Quarter 2016 (in Millions)*, STATISTICA, https://www.statista.com/statistics/282087/number-of-monthly-active-twitter-users/ (last visited Apr. 24, 2017) (on file with the Washington and Lee Law Review).

91. *See* Francis Bea, *Why We're Cautiously Optimistic about Twitter's New Authentication System*, DIGITAL TRENDS (Aug. 8, 2013), http://www.digitaltrends.com/social-media/twitter-has-introduced-a-new-authentication-system-and-were-cautiously-optimistic-about-it-heres-why/ (last visited Apr. 24, 2017) (estimating "that Twitter will face the normal 'legacy' two step adoption rate, meaning that just between 0.5 percent and 2 percent of users will bother to add this two-factor authentication method") (on file with the Washington and Lee Law Review).

Facebook	May 2011[92]	1 billion estimated[93]	No public data available, but given how involved the set-up process is, I would guesstimate the same legacy adoption rate as Twitter, i.e., 0.5 to 2%.
Dropbox	August 2012[94]	500 million	< 1%[95]

e) Loading . . . . Privacy: Why does Tor Adoption Stink?

Why does Tor adoption stink? Because it's an onion router.[96] Tor is a pro privacy service that, *inter alia*, anonymizes internet browsing by routing traffic through multiple random servers,

92. Andrew Song, *Introducing Login Approvals*, FACEBOOK (May 12, 2011), https://www.facebook.com/notes/facebook-engineering/introducing-login-approvals/10150172618258920/ (last visited Apr. 24, 2017) (on file with the Washington and Lee Law Review).

93. *Number of Monthly Active Facebook Users Worldwide as of 4th Quarter 2016 (in Millions)*, STATISTICA https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/ (last visited Apr. 24, 2017) (on file with the Washington and Lee Law Review).

94. *See* Brian Krebs, *Dropbox Now Offers Two-Step Authentication*, KREBS ON SEC. (Aug. 12, 2012), http://krebsonsecurity.com/2012/08/dropbox-now-offers-two-step-authentication/ (last visited Apr. 24, 2017) ("Online file-backup and storage service Dropbox has begun offering a two-step authentication feature to help users beef up the security of their accounts. The promised change comes less than a month after the compromise of a Dropbox employee's account exposed many Dropbox user email addresses.") (on file with the Washington and Lee Law Review).

95. *See* Brian Krebs, *Dropbox Smeared in Week of Megabreaches*, KREBS ON SEC. (June 16, 2016), http://krebsonsecurity.com/2016/06/dropbox-smeared-in-week-of-megabreaches/ (last visited Apr. 24, 2017) ("According to Dropbox's Patrick Heim, less than one percent of the Dropbox user base is taking advantage of the company's two-factor authentication feature, which makes it much harder for thieves and other ne'er-do-wells to use stolen passwords") (on file with the Washington and Lee Law Review).

96. Bazinga! (And apologies!)

which cannot read the data in transit.[97] As described on Tor's website:

> Tor's users employ this network by connecting through a series of virtual tunnels rather than making a direct connection, thus allowing both organizations and individuals to share information over public networks without compromising their privacy. Along the same line, Tor is an effective censorship circumvention tool, allowing its users to reach otherwise blocked destinations or content. Tor can also be used as a building block for software developers to create new communication tools with built-in privacy features.[98]

The Tor network forms part of both EFF's[99] and Snowden's[100] recommended privacy tools as a key privacy enhancer and anti-surveillance tool. While installing and setting up Tor is not particularly cumbersome, using it is a fairly painful experience. Firstly, to ensure total privacy protection, users have to follow digital hygiene, which is highly implausible for a typical user. Sample these recommendations from Ubergizmo for optimal Tor usage:

> Use HTTPS instead of HTTP whenever possible.
>
> Disable Java, JavaScript, and Flash because these could be used to identify your IP.
>
> Don't use your real email/name on Tor websites.

---

97. *See infra* note 98 and accompanying text (describing Tor).

98. *See Tor: Overview*, TOR, https://www.torproject.org/about/overview.html.en (last visited Apr. 24, 2017) (on file with the Washington and Lee Law Review).

99. *See How to: Use Tor for Windows*, EFF, https://ssd.eff.org/en/module/how-use-tor-windows (last updated Nov. 4, 2015) (last visited Apr. 24, 2017) ("For people who might need occasional anonymity and privacy when accessing websites, Tor Browser provides a quick and easy way to use the Tor network.") (on file with the Washington and Lee Law Review).

100. *See* mikeperry, *This is What a Tor Supporter Looks Like: Edward Snowden*, TOR PROJECT (Dec. 30, 2015), https://blog.torproject.org/blog/what-tor-supporter-looks-edward-snowden (last visited Apr. 24, 2017) (quoting Edward Snowden as stating that "Tor is a critical technology, not just in terms of privacy protection, but in defense of our publication right—our ability to route around censorship and ensure that when people speak their voices can be heard") (on file with the Washington and Lee Law Review).

> Don't download files (via P2P) using Tor.
>
> Don't log into services that can be tracked to you (official email, social media…)
>
> Prevent or Delete browser cookies which can be used to track you (Tor Browser does it automatically)
>
> Avoid using Google since it can track users by multiple ways (for example, Ads, Android, Chrome, or Search). Others do it, but no-one has a wider net as Google, and all this information could potentially be cross-referenced to identify a user.[101]

Secondly, Tor takes three to four times the time to load web pages compared to other web browsers, and can almost feel like good old dial-up at times.[102] In the world of millisecond optimizations, I would argue that this strongly impacts adoption.[103] I tried Tor and stopped using it on account of its

---

101. Dilawer Soomro, *What is Tor & How to Use It Properly*, UBERGIZMO (June 28, 2016, 5:00 PM), http://www.ubergizmo.com/articles/tor/ (last visited Apr. 24, 2017) (on file with the Washington and Lee Law Review).

102. *See* Joel Hruska, *Snowden-Approved: The 'Citizenfour' Hacker's Toolkit*, EXTREME TECH (Mar. 20, 2015, 9:23 AM), https://www.extremetech.com/extreme/201636-snowden-approved-the-citizenfour-hackers-toolkit (last visited Apr. 24, 2017) ("One caveat about using Tor for anonymous browsing is that the performance isn't going to be what you're used to from a standard connection.") (on file with the Washington and Lee Law Review).

103. It will be interesting to see how Google's open source mobile HTML webpage standard, called "AMP," will perform. AMP serves up cached content (in some cases from Google's servers) to mobile browsers at a median loading speed of 0.7 seconds. James A. Martin, *8 Things you Need to Know about Google AMP*, CIO (July 6, 2015, 5:00 AM), http://www.cio.com/article/3091071/search/8-things-you-need-to-know-about-google-amp.html (last visited Apr. 24, 2017) (on file with the Washington and Lee Law Review). AMP supporting websites get a thunderbolt icon next to their name in Google search results, and a boost in search results. *See id.* (noting that although "AMP is not directly a search engine ranking factor," an AMP website will be higher ranked than a non-AMP website if all other factors are equal). eBay is already partially implementing AMP. *See id.* (reporting that "on June 30, eBay announced that its AMP-powered mobile shopping experience was live"). AMP's chief drawback seems to be that it will interfere with analytics since it will be impossible to say with certainty where content will be served up from- Google's cache or the canonical 'original' version. *See id.* ("AMP 'creates a potential challenge on the analytics side, as it's impossible to be 100 percent sure where a publisher's content will be loaded from, as well as complications with visitor identification due to tight cookie restrictions,' says [Adobe Analytics product manager Trevor] Paulsen.") AMP also imposes cookie restrictions. *Id.* For more information about Google's AMP, see generally AMP PROJECT, https://www.ampproject.org/ (last visited

speed limitations. A 2011 market report by Kissmetrics states that 40% of people abandon a website that takes more than three seconds to load, and 47% of consumers expect a web page to load in two seconds or less.[104]

I would argue that Tor falls afoul of Ann Cavoukian's fourth foundational PbD principle of full functionality.[105] This principle encourages design, which satisfies all legitimate objectives, and not just the privacy goals.[106] Ignoring speed and user convenience is arguably a PbD fail.[107]

The following table summarizes Tor usage statistics:

Apr. 24, 2017) (on file with the Washington and Lee Law Review).

104. *See* Sean Work, *How Loading Time Affects Your Bottom Line*, KISSMETRICS, https://blog.kissmetrics.com/loading-time/ (last visited Apr. 24, 2017) (finding that "website visitors tend to care more about speed than all the bells and whistles we want to add to our websites" and providing related statistics) (on file with the Washington and Lee Law Review).

105. *See* ANN CAVOUKIAN, PRIVACY BY DESIGN: THE 7 FOUNDATIONAL PRINCIPLES 3–4 (2011), https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf (discussing the fourth principle, which Cavoukian titles "Full Functionality – Positive-Sum, not Zero-Sum").

106. *See id.* at 3 ("Privacy by Design is doubly-enabling in nature, permitting full functionality—real, practical results and beneficial outcomes to be achieved for multiple parties.")

107. In fairness, it should be noted that Tor could comport with the general PbD maxim that different privacy/security is appropriate depending on the sensitivity of the data. *See id.* at 4 (noting that "the security of personal information [is] generally commensurate with the degree of sensitivity" of the data). One might not want to use Tor for everything because of the high transaction cost, but it might be worthwhile in other scenarios (e.g., communications between political dissidents in authoritarian environments).

Table 4: Tor Usage

Number of Users in 2016	~1.7 million.[108] It may be unfair to compute percentage use based on global internet users, or number of desktop internet browser users, but it's safe to say that Tor browsing accounts for less than 1% of the desktop browsing activity since it fails to show up in any online ranking of usage share of web browsers.[109]
August 2013 estimation of Number of Daily US users	50–100 for every 100,000 users (i.e., a best use case of 0.1%).[110]

We can now turn to the regulatory implications of standards/technologies that are more successful than Tor and come to define the market.

IV. Implications for Regulation

What are the regulatory implications if a standard is widely diffused through the industry and not implemented only by a few actors? Would a website which gathers information over HTTP rather than HTTPS be exposing itself to regulatory risk?

The FTC could theoretically address such cases using both the deception and unfairness doctrines.[111] If the website has

108. *Users*, TOR METRICS, https://metrics.torproject.org/userstats-relay-country.html?start=2016-01-01&end=2016-12-31&country=all&events=off (last visited Apr. 24, 2017) (on file with the Washington and Lee Law Review).

109. *See, e.g.*, *Browser Statistics*, W3SCHOOLS, http://www.w3schools.com/browsers/ (last visited Apr. 24, 2017) (showing that, in February 2017, the browsers Chrome, IE/Edge, Firefox, Safari, and Opera accounted for 98.5% of W3Schools's web traffic combined) (on file with the Washington and Lee Law Review).

110. *Users*, TOR METRICS, https://metrics.torproject.org/oxford-anonymous-internet.html (last visited Apr. 24, 2017) (on file with the Washington and Lee Law Review).

promised that it is "secure" in its advertising or its privacy policy, failure to implement a standard security practice may be deceptive.

Non-implementation of a standard could also lead to an FTC unfairness action. In 1980, the FTC adopted the FTC Policy Statement on Unfairness, and, in 1994, Congress codified the current limitation on the Agency's power to find an act or practice unfair.[112] In relevant part, it reads:

> The Commission shall have no authority . . . to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition. In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination.[113]

Consumers are arguably unable to address the harms caused from poor privacy or security standards by themselves (short of not using the services in question). There is no real countervailing benefit to consumers from poorer security (except for potentially cheaper services). The arguments against such action under the unfairness doctrine would be the fact that there is no substantial "injury" to consumers, and that prescribing standards does seem to be based on something analogous to public policy considerations.

Market participants I spoke to were of the view that it is inequitable to expect them to be treated as having constructive notice that the non-implementation of a widely adopted standard amounts to "unfairness." The FTC has also been circumspect in its use of the unfairness doctrine, and in the context of the internet, has mostly invoked it in egregious cases.[114]

---

111. *See* 15 U.S.C. § 45(a)(1) (2012) ("Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.").

112. CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 131 (2016).

113. 15 U.S.C. § 45(n).

114. *See* J. Howard Beales, *The FTC's Use of Unfairness Authority: Its Rise,*

Nonetheless, it is not entirely far-fetched to think that the non-implementation of a widely diffused standard could form the subject matter of an FTC complaint. There are a number of cases and practices that could lend support to such a complaint. For example, the FTC has brought actions against defendants for insecure data practices that fault the standards deployed by defendants (without going a step further and prescribing the standard that they should have used instead).[115] The FTC's treatment of data security practices under the unfairness doctrine originated in 2005 with the BJ Wholesale Case,[116] where the defendant allegedly stored and transmitted customer credit card data in an insecure manner without encryption, and agreed to modify its practices under the terms of a consent order.[117]

More recently, in the 2015 case of *Wyndham*,[118] the Third Circuit upheld the FTC's authority to bring a complaint against the defendant for insecure data security practices under the unfairness doctrine.[119] The FTC also separately alleged deception.[120] The court found that the FTC's statute gave the defendant fair notice of such potential liability.[121] The statute was held to place an obligation upon the defendant to weigh the probability and magnitude of harms to consumers caused by its

---

Fall, and Resurrection, FTC (May 30, 2003), https://www.ftc.gov/public-statements/2003/05/ftcs-use-unfairness-authority-its-rise-fall-and-resurrection (last visited Apr. 24, 2017) (noting that "in order for a practice to be unfair, the injury it causes must be (1) substantial, (2) without offsetting benefits, and (3) one that consumers cannot reasonably avoid") (on file with the Washington and Lee Law Review).

115. *See, e.g.*, *In re* BJ's Wholesale Club, Inc., No. 42-3160, 2005 WL 2395788, at *4 (Sept. 20, 2005) (ordering "that Respondent obtain an assessment and report (an "Assessment") from a qualified, objective, independent third-party professional, using procedures and standards generally accepted in the profession").

116. *Id.*

117. *See id.* at *1 ("From at least November 1, 2003, until February, 2004, Respondent did not employ reasonable and appropriate measures to secure personal information collected at its stores. Among other things, Respondent . . . did not encrypt the information while in transit or when stored on the in-store computer networks.").

118. FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015).

119. *See id.* at 247 ("We are therefore not persuaded by Wyndham's arguments that the alleged conduct falls outside the plain meaning of 'unfair.'").

120. *Id.* at 240.

121. *See id.* at 256 (concluding that "Wyndham's fair notice challenge fails").

data security practices, and whether these costs outweighed any savings from not employing more secure practices.[122]

Wyndham was a fairly egregious case, because the defendant corporation had no firewall at all, failed to use any encryption for customer data, was hacked thrice, and failed to take any remedial measures after the first two hacks.[123] Nonetheless, it illustrates that market participants can be expected to read the tea leaves, and be "on notice" as to what they may perceive to be inchoate standards.

Similarly, in the 2016 ASUS Case,[124] the FTC brought an unfairness action against the defendant for lax security practices such as setting "admin" as the default username and password on all of its routers.[125] Presumably ASUS should have known that this was not a reasonable standard to deploy.

FTC attorneys also look to the SANS Institute and Open Web Application Security Project (OWASP) lists of common security vulnerabilities to identify case priorities.[126] These thus serve as a market floor in terms of security standard setting, and breaching that floor could have regulatory consequences.

All of the above precedents and practices cumulatively point to the fact that the FTC does often believe that there is a market standard that actors must meet. In view of this, industry actors should stay abreast of emerging privacy and security standards, and also consider adding a cost-benefit analysis of widely diffused security standards to their FTC cheat-sheet.

---

122. *See id.* at 255–56 (setting out the factors relating to whether an entity is on notice as to the application of § 45(n)).

123. *See id.* at 241 (discussing Wyndham's failure "to use 'readily available security measures'").

124. In the Matter of ASUSTeK Computer, Inc., No. 142-3156, 2016 WL 4128217 (July 18, 2016).

125. *See id.* at *6 (reprimanding ASUSTeK for "allow[ing] consumers to retain the weak default login credentials username 'admin' and password 'admin' for the admin console").

126. HOOFNAGLE, *supra* note 112, at 233.

V. Conclusions

A few conclusions can be drawn from the above discussion.Firstly, when a privacy standard becomes industry dominant on account of a major actor, the cost to other market participants appears not to affect its diffusion. This should be distinguished from "cost" to consumers, both in monetary terms and in terms of convenience. Standards should be designed to as seamless as possible from a consumer standpoint in order to encourage their adoption. When standards can be introduced through routine updates, their uptake is significantly higher. Product designers and engineers should consider using a modified version of Gandhi's Talisman:[127] Will the feature being introduced improve the privacy or security of the least tech savvy user you have ever encountered?[128]

Secondly, individual market actors have the capacity to significantly improve the privacy and security of a disproportionate number of people on account of network domino effects.[129] This should encourage those trying to build more secure

---

127. *See* 2 MAHATMA GANDHI, THE LAST PHASE 65 (1958).

> I will give you a talisman. Whenever you are in doubt, or when the self becomes too much with you, apply the following test. Recall the face of the poorest and the weakest man [woman] whom you may have seen, and ask yourself, if the step you contemplate is going to be of any use to him [her]. Will he [she] gain anything by it? Will it restore him [her] to a control over his [her] own life and destiny? In other words, will it lead to swaraj [freedom] for the hungry and spiritually starving millions? Then you will find your doubts and your self melt away.

128. In a fascinating study, it was found that when Signal users were subjected to an artificial man in the middle attack, twenty-one out of twenty-eight users in the study failed to compare and verify their public keys to defeat the attack; indeed, a majority of study participants believed they had succeeded when they had failed. *See generally* SVENJA SCHRODER, MARKUS HUBER, DAVID WIND & CHRISTOPH ROTTERMANNER, WHEN SIGNAL HITS THE FAN: ON THE USABILITY AND SECURITY OF STATE-OF-THE-ART SECURE MOBILE MESSAGING (2016), https://www.internetsociety.org/sites/default/files/09%20when-signal-hits-the-fan-on-the-usability-and-security-of-state-of-the-art-secure-mobile-messaging.pdf (providing the results of the experiment).

129. Though this paper does not consider enterprise technologies, it is interesting to note that there, as well, individual actors such as Jeff Jonas and Palantir Technolgies (Palantir)—both of whom are in the security and surveillance sector—can bake in features such as privacy by design, revocability (revoked credentials are reflected upstream and downstream across all data)

systems. Privacy advocates should also focus their efforts on those who already are, or are likely to become, significant actors in their digital spaces.

Finally, it is worth trying to keep pace with and drive such innovation; if nothing else, you could end up financially benefiting by helping implement new standards on the backend.

---

and audit logs (who looked at what, when, and for what purpose) into their products, and set the tone for that segment of the market. This is despite the fact that features such as audit logs can significantly increase costs since multiple copies of the same data set are required for audit logs, and even with cheap storage, these data sets are very large. The co-founder of Palantir, Alex Karp, claims they walk away from as high as 20% of projects for ethical reasons, and has expressed a commitment to privacy, stating, "We have to find places that we protect away from government so that we can all be the unique and interesting and, in my case, somewhat deviant people we'd like to be." Grgory Maus, *A (Pretty) Complete History of Palantir*, SOC. CALCULATIONS (Aug. 11, 2015), http://www.socialcalculations.com/2015/08/a-pretty-complete-history-of-palantir.html (last visited Apr. 24, 2017) (on file with the Washington and Lee Law Review).