PEELING BACK THE STUDENT PRIVACY PLEDGE

ALEXI PFEFFER-GILLETT †

ABSTRACT

Education software is a multi-billion dollar industry that is rapidly growing. The federal government has encouraged this growth through a series of initiatives that reward schools for tracking and aggregating student data. Amid this increasingly digitized education landscape, parents and educators have begun to raise concerns about the scope and security of student data collection.

Industry players, rather than policymakers, have so far led efforts to protect student data. Central to these efforts is the Student Privacy Pledge, a set of standards that providers of digital education services have voluntarily adopted. By many accounts, the Pledge has been a success. Since its introduction in 2014, over 300 companies have signed on, indicating widespread commitment to the Pledge's seemingly broad protections for student privacy. This industry participation is encouraging, but the Pledge does not contain any meaningful oversight or enforcement provisions.

This Article analyzes whether signatory companies are actually complying with the Pledge rather than just paying lip service to its goals. By looking to the privacy policies and terms of service of a sample of the Pledge's signatories, I conclude that noncompliance may be a significant and prevalent issue.

Consumers of education software have some power to hold signatories accountable, but their oversight abilities are limited. This Article argues that the federal government, specifically the Federal Trade Commission, is best positioned to enforce compliance with the Pledge and should hold Pledge signatories to their promises.

INTRODUCTION

With schools across the country embracing data-driven learning, the education technology industry has taken off; recent estimates value the overall market at anywhere between $1.8 to $8 billion.[1] Many

† Associate, Robbins Geller Rudman & Dowd LLP; J.D., University of California, Berkeley, School of Law, 2016. The views expressed in this Article are my own.

[1] Michele Molnar, *K-12 Ed-Tech Platform and Tools Market Value to Increase to $1.83 Billion by 2020, Report Says*, EDWEEK: MARKET BRIEF (May 1, 2017),

administrators now incorporate online learning into their educational programs. Schools have an array of services to choose from—the industry includes heavyweights like Apple, Google, and Microsoft, as well as lesser-known upstarts offering niche services. These products appeal to administrators hoping to comply with overlapping federal, state, and local education policies that encourage tracking student data.

But as the services help schools comply with data recording requirements, they also risk compromising student privacy. Indeed, recent evidence suggests that education technology companies may employ weak security features[2] and collect potentially disturbing—and legally dubious—levels of students' personally identifiable information.[3]

Amid growing concerns from parents and educators, the education technology industry developed a guarantee in late 2014, dubbed the Student Privacy Pledge ("the Pledge"). The Pledge, which has been signed by over 300 companies,[4] provides that signatories will take certain security precautions and limit their collection of student information. These promises, however, are only meaningful to the extent that signatories are actually keeping them.

This Article seeks to shed light on the potential gap between promises and reality in regard to the Pledge. It does so by examining eight company policies—three major, publicly traded companies,[5] and five smaller, private companies that were early signatories.[6] Today, two of the five smaller companies—Brain Hive and Triumph Learning—have

---

https://marketbrief.edweek.org/marketplace-k-12/k-12-ed-tech-platform-tools-market-value-increase-1-83-billion-2020-report-says/; *SIIA Estimates $8.38 Billion US Market for PreK-12 Educational Software and Digital Content*, SOFTWARE & INFO. INDUS. ASSOC. (Feb. 24, 2015), http://www.siia.net/Press/SIIA-Estimates-838-Billion-Dollars-US-Market-for-PreK-12-Educational-Software-and-Digital-Content.

[2] *See, e.g.*, Dell Cameron, *1.3 Million K-12 Students Exposed by Now-Secured Data Breach*, DAILY DOT (Apr. 20, 2017, 2:34 PM), https://www.dailydot.com/layer8/1-3-million-american-students-exposed-data-breach-now-secured/; Natasha Singer, *Data Security Gaps in an Industry Student Privacy Pledge*, N.Y. TIMES: BITS (Feb. 11, 2015, 4:48 PM), http://bits.blogs.nytimes.com/2015/02/11/data-security-gaps-in-an-industry-student-privacy-pledge/.

[3] *See, e.g.*, Natasha Singer, *Deciding Who Sees Students' Data*, N.Y. TIMES (Oct. 5, 2013), http://www.nytimes.com/2013/10/06/business/deciding-who-sees-students-data.html.

[4] *Signatories*, STUDENT PRIVACY PLEDGE, https://studentprivacypledge.org/signatories/ (last visited Jul. 13, 2017) [hereinafter *Pledge Signatories*].

[5] These companies are Apple, Google, and Microsoft.

[6] These companies are Brain Hive, eScholar, Hapara, Schoolzilla, and Triumph Learning.

withdrawn from participation in the Pledge and are no longer listed as signatories.

My research suggests that at least seven of the eight companies examined may be violating some aspect of the Pledge,[7] with Apple potentially being the most egregious offender. Interestingly, the two companies that withdrew from participation in the Pledge are not noticeably less compliant than the six remaining sample companies.

For the sake of providing a control group, I also examined two major companies—Facebook and Pearson—that have not currently signed the Pledge. As with the former signatories, neither Facebook nor Pearson is noticeably less compliant with the Pledge's standards—at least by the standards of its customer-facing policies—than the signatories. In other words, the Pledge may be more valuable as a public relations tool than as a means of actually effecting—or reflecting—industry improvements. On the other hand, the fact that some companies are removing themselves from participation in the Pledge suggests either that the Pledge does have some power over company practices or that participation in the Pledge does not have significant value in attracting business.

Many of the Pledge's signatories do, however, use the Pledge as a selling tool—for example, by advertising Pledge participation on the company homepage.[8] Assuming the Pledge has value in influencing customer and parental decisions, it is important to know whether signatories are actually complying with the Pledge.

Although parents, educators, and third parties may be able to provide a limited check on corporate compliance, I argue that the Federal Trade Commission (FTC or "the Commission") is in the best position to address this issue and to hold companies accountable for complying with the Pledge.

In Part I, this Article provides background on the development of the Pledge. Part II discusses areas where companies' terms of service and privacy policies appear to diverge from their promises in the Pledge. In light of this assessment, Part III discusses the ways in which consumers and,

---

[7] This is based on an assumption that the companies are doing no more or less than they have agreed to in their privacy policies and terms of service. It is possible, and even likely, that the companies' actual practices deviate from those terms to which they ask users to agree. For example, a company may ask users to waive certain ownership of various pieces of data without actually taking advantage of that data. On the other hand, companies may also access data without obtaining user consent to do so.

[8] For example, one of the companies surveyed, eScholar, has a "Student Pledge Signatory Icon" featured prominently on its home page. ESCHOLAR, http://www.escholar.com/ (last visited Jul. 13, 2017).

more importantly, the FTC can hold companies accountable for violating the Pledge.

I. BACKGROUND

The Student Privacy Pledge is a sweeping self-regulatory effort led by software industry groups. It comes after years of steady growth in the education software market—driven in large part by the federal government's encouragement of data-centric education initiatives. This Section details how and why the Pledge came into being. It then examines which companies have signed on and which companies have not.

A. Increasing Demand for Education Software

Education data is an annual market with an estimated worth of well over a billion dollars.[9] And the market is continuously growing.[10] This growth is likely attributable, at least in part, to the recent pressure on schools across the country to adopt data-driven learning programs that require student progress-tracking software.[11] Much of this pressure comes from the federal government, which exerts outsize influence over education: although federal funding accounts for only about ten percent of total state education spending, federal programs like No Child Left Behind, Race to the Top, and Common Core have been extraordinarily influential in dictating state policies and encouraging more tracking of student data.[12]

No Child Left Behind (NCLB), introduced in 2001, required states to track the academic progress of their students in order to receive government funding.[13] In the wake of NCLB, student progress, or lack thereof, therefore became critical to the schools' survival—schools and school districts that did not meet adequate yearly progress requirements could be forced to close or restructure.[14]

The Obama administration introduced two other education initiatives that further incentivized tracking student data. First, Race to the

---

[9] Molnar, *supra* note 1.
[10] *Id.*
[11] Natasha Singer, *Microsoft and Other Firms Pledge to Protect Student Data*, N.Y. TIMES (Oct. 7, 2014), https://www.nytimes.com/2014/10/07/business/microsoft-and-other-firms-pledge-to-protect-student-data.html.
[12] Fred Bauer, *Revising No Child Left Behind*, NAT. REV. (Feb. 3, 2015, 1:00 PM), http://www.nationalreview.com/article/397799/revising-no-child-left-behind-fred-bauer.
[13] No Child Left Behind Act of 2001, Pub. L. No. 107–110, 115 Stat. 1425 (2002); *see also* Jules Polonetsky & Omer Tene, *Who Is Reading Whom Now: Privacy in Education from Books to Moocs*, 17 VAND. J. ENT. & TECH. L. 927, 941 (2015).
[14] David Hursh, *Exacerbating Inequality: The Failed Promise of the No Child Left Behind Act*, 10 RACE ETHNICITY & ED. 295, 297 (2007).

Top, launched in 2009, is a competitive grant program that awards funding to states that implement certain education techniques, including data tracking.[15] States submit applications, which the Department of Education grades on a 485-point scale.[16] Nearly ten percent of those points are reserved for states that implement "[d]ata systems that support instruction"[17] and "[i]ncrease the acquisition, adoption, and use of local instructional improvement systems."[18] In other words, the more that states and schools track student data, the more likely they are to receive significant federal funding.

Second, the Obama administration introduced the Common Core Standards Initiative, a plan to implement national curriculum standards.[19] The program required assessment tests to monitor student progress in both English and Math.[20] To prepare for those tests (and receive funding), many school districts needed software that could analyze student performance in greater detail.[21]

Although it is unclear what, if any, policies President Trump will employ toward technology in the classrooms, there is every reason to believe that the industry will continue to grow.[22]

There is already a federal law—the Family Educational Rights Privacy Act (FERPA)—that is designed to protect student privacy.[23] But FERPA has glaring holes, which make its ability to truly safeguard student privacy suspect at best. For example, to the question of what FERPA requires if personally identifiable information from student records is disclosed to a third-party provider, the official government guidance responds: "It depends."[24] And although FERPA generally prohibits a school or district from disclosing personally identifiable information from education records to a provider without first obtaining written consent from

---

[15] DEPT. OF ED., RACE TO THE TOP PROGRAM EXECUTIVE SUMMARY 2 (Nov. 2009), https://www2.ed.gov/programs/racetothetop/executive-summary.pdf.
[16] *Id.* at 3.
[17] *Id.* at 8.
[18] *Id.*
[19] Singer, *supra* note 3.
[20] *Id.*
[21] *Id.*
[22] *See* Adam Stone, *What Will Trump's Ed Tech Policies Look Like?*, CTR. FOR DIGITAL EDUC.: CONVERGE (Mar. 1, 2017), http://www.centerdigitaled.com/higher-ed/What-Will-Trumps-Ed-Tech-Policies-Look-Like.html.
[23] *See* 20 U.S.C. § 1232g (2012).
[24] PRIVACY TECHNICAL ASSISTANCE CTR., PROTECTING STUDENT PRIVACY WHILE USING ONLINE EDUCATIONAL SERVICES: REQUIREMENTS AND BEST PRACTICES 3 (Feb. 2014), https://tech.ed.gov/wp-content/uploads/2014/09/Student-Privacy-and-Online-Educational-Services-February-2014.pdf.

parents, recent changes to the Act created major exceptions allowing school officials to circumvent parental consent.[25] Most significantly, officials can now share personally identifiable information to vendors without parental consent so long as the vendor provides a normal school function, has a legitimate interest in educational records, is under direct control of the school or district regarding the use of the records, and only uses the records for authorized purposes.[26] In practice, this exception means that many education programs are allowed to collect student personally identifiable information without parental consent or oversight.[27]

B. Worries Over Student Privacy

As demand for education software has grown, so too has concern over the security of the ever-increasing haul of student data now in the hands of schools and education software companies. Khaliah Barnes, a lawyer at the Electronic Privacy Information Center, noted that "[s]tudents are currently subject to more forms of tracking and monitoring than ever before," but "there are too few safeguards for the amount of data collected and transmitted from schools to private companies."[28]

Parents too have begun to publicly worry that schools will not be able to protect student personal information. This fear can be seen, at least in part, as a reaction to recent date breaches at major retailers and banks.[29] And, recently, the fears have materialized: one of the companies surveyed in this Article was subject to a large data breach. In April 2017, a researcher discovered that Schoolzilla had exposed personal information, including the social security numbers of over a million students.[30] Amid this growing demand for—and skepticism over—data collection software, the industry has stepped in with the Student Privacy Pledge.

---

[25] *Id.*; *see also* Singer, *supra* note 3 ("Recent changes in the regulation of a federal education privacy law have also helped the industry. . . . The updated rules permit schools to share student data, without notifying parents, with companies to which they have outsourced core functions like scheduling or data management.").
[26] 34 C.F.R. § 99.31(a)(1)(i) (2012).
[27] PRIVACY TECHNICAL ASSISTANCE CTR., *supra* note 24; *see also* Natasha Singer, *Uncovering Security Flaws in Digital Education Products for Schoolchildren*, N. Y. TIMES (Feb. 8, 2015), https://www.nytimes.com/2015/02/09/technology/uncovering-security-flaws-in-digital-education-products-for-schoolchildren.html?_r=0 ("[E]xperts say [FERPA] protections do not extend to many of the free learning sites and apps that teachers download and use independently in their classrooms.").
[28] Singer, *supra* note 3.
[29] Singer, *supra* note 11.
[30] Cameron, *supra* note 2.

C. Crafting the Student Privacy Pledge

The process of developing the Pledge began somewhat organically in 2013, when a national association for school district chief technology officers published a list of security questions that it recommended schools ask before contracting with a technology vendor.[31]

The Future of Privacy Forum (FPF), a Washington, DC, industry-financed think tank, and the Software & Information Industry Association (SIIA), a trade group, spearheaded the software industry's response to these school district concerns by creating and promoting the Student Privacy Pledge.[32] The Pledge incorporated guidance from two U.S. representatives, one Democrat and one Republican, as well as school service providers and educator organizations.[33]

In addition to responding to consumer concerns, the Pledge also compensates for aspects of existing laws that the software industry views as ineffective or inscrutable. Steve Mutkoski, the government policy director for Microsoft's worldwide public sector business, stated "The Pledge addresses some of the perceived weaknesses in FERPA, . . . and does a good job consolidating many of the issues that have been raised in state legislation concerning how third-party service providers may use student data."[34] Specifically, compliance with the Pledge requires companies to agree to much stronger language regarding things like tracking student data and targeting students through behavioral advertising.[35] "We wanted to say to parents: 'No one's going to sell your kids' data; nobody's going to track your child around the Internet; no one's going to compile a profile that is used against your child when they apply for a job 20 years later,'" Jules Polonetsky, executive director of the Future Privacy Forum, told the *New*

---

[31] Singer, *supra* note 27. The group received financing from Dell, Google, Pearson, Microsoft, and other education sector companies. *Id.*

[32] Brenda Leong, *K-12 Student Privacy Pledge Announced*, FUTURE OF PRIVACY FORUM, https://fpf.org/2014/10/07/k-12-student-privacy-pledge-announced/ (last visited Nov. 18, 2017); Singer, *supra* note 11.

[33] Christopher Piehler, *Major Ed Tech Companies Sign Student Data Privacy Pledge*, THE JOURNAL (Oct. 7, 2014), https://thejournal.com/articles/2014/10/07/major-ed-tech-companies-sign-student-data-privacy-pledge.aspx.

[34] *Singer*, *supra* note 11; *see also* Associated Press, *50-State Look at How Common Core Playing Out in US*, NORTHWEST HERALD (Aug. 27, 2014), http://www.nwherald.com/2014/08/27/50-state-look-at-how-common-core-playing-out-in-u-s/a314ftf/?page=3 (noting that in Vermont, opponents of Common Core "have concerns about technology involved and protecting student data").

[35] *See Privacy Pledge: K-12 School Service Provider Pledge to Safeguard Student Privacy*, STUDENT PRIVACY PLEDGE, https://studentprivacypledge.org/privacy-pledge/ (last visited Jun. 21, 2017) [hereinafter *Student Privacy Pledge*].

York Times.[36] "We hope this is a useful way for companies that want to be trusted partners in schools to make it clear they are on the side of responsible data use."[37]

The timing of the Pledge represents a strategic move for the industry as states and the federal government consider new student privacy laws. The Future of Privacy Forum released the Student Privacy Pledge just a week after passage of a California law that, like the Pledge, prohibits companies from engaging in an array of practices, including behavioral advertising and selling student information.[38] The California law appears to be just a small part of a larger movement toward greater government oversight of student data. Indeed, Congress has in recent years considered a new, nationwide student privacy bill that could add significant new regulations to the industry.[39] Amid these potential changes, the Pledge might convince legislators that the industry can look after itself and that new regulations are unnecessary.

The industry would undoubtedly prefer this outcome because the Pledge is only as strong and binding as industry members want it to be. Unlike FERPA, which places affirmative (albeit limited) requirements on software companies with penalties for noncompliance, the Student Privacy Pledge is completely voluntary and contains no enforcement mechanisms; companies are free to sign or not sign and no entity is tasked with monitoring their compliance or administering punishments for companies that break the Pledge's promises. The Future of Privacy Forum is holding workshops to instruct signatories on how to comply with the Pledge, but there is little suggestion of continued oversight.[40]

The Pledge also provides significant wiggle room that might not be available were the industry more regulated. Indeed, some observers have criticized the Pledge for being too vague in regard to protection of student data. Bill Fitzgerald, a frequent commenter on children's privacy, noted

---

[36] Singer, *supra* note 11.

[37] *Id.*

[38] *See* S.B. 1177, 2013–2014 Leg., Reg. Sess. (Cal. 2014), available at https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB1177; Singer, *supra* note 11.

[39] Natasha Singer, *Legislators Introduce Student Digital Privacy Bill*, N.Y. TIMES: BITS (Apr. 29, 2015, 1:09 PM), http://bits.blogs.nytimes.com/2015/04/29/legislators-introduce-student-digital-privacy-bill/.

[40] Natasha Singer, *Digital Learning Companies Falling Short of Student Privacy Pledge*, N.Y. TIMES: BITS (Mar. 5, 2015, 11:54 AM), http://bits.blogs.nytimes.com/2015/03/05/digital-learning-companies-falling-short-of-student-privacy-pledge/.

"significant gray areas around what constitutes a 'protected' record and what would constitute unprotected metadata."[41]

D. Who is, and Who is Not, on the Pledge

The Pledge is intended to cover "school service providers," which are entities providing an online, student-data-collecting service or application used by teachers or other employees.[42] Many such providers have participated in the Pledge since its inception.

Microsoft was among the initial signatories when the Pledge was released in October, 2014.[43] But Apple and Google were not so eager to adopt the Pledge's promises, and the two companies received heavy criticism for months as they put off signing the Pledge.[44] Interestingly, Google initially abstained from signing the Pledge even though the company had helped finance the Pledge's main proponent, the Future of Privacy Forum.[45] The company claimed that it did not need to sign the Pledge because its own policies demonstrated a sufficient commitment

---

[41] Charley Locke, *Edtech Companies Pledge to Protect Student Data Privacy*, EDSURGE (Oct. 7, 2014), https://www.edsurge.com/n/2014-10-07-edtech-companies-pledge-to-protect-student-data-privacy.

[42] *See Student Privacy Pledge*, *supra* note 35 ("'School service provider' refers to any entity that: (1) is providing, and is operating in its capacity as a provider of, an online or mobile application, online service or website that is both designed and marketed for use in United States elementary and secondary educational institutions/ agencies and is used at the direction of their teachers or other employees; and (2) collects, maintains or uses student personal information in digital/electronic format. The term 'school service provider' does not include an entity that is providing, and that is operating in its capacity as a provider of, general audience software, applications, services or websites not designed and marketed for schools.").

[43] *Our Pledge to Safeguard Student Privacy*, MICROSOFT: MICROSOFT ON THE ISSUES (Oct. 7, 2014), http://blogs.microsoft.com/on-the-issues/2014/10/07/pledge-safeguard-student-privacy/.

[44] *See, e.g.*, Jeff Gold, *Why Google is Ignoring Obama's Challenge to Sign the Student Privacy Pledge*, SAFEGOV (Jan. 14, 2015), http://safegov.org/2015/1/14/why-google-is-ignoring-obama%E2%80%99s-challenge-to-sign-the-student-privacy-pledge; Sam Colt, *Google Wouldn't Tell Us Why It Didn't Sign President Obama's Student Privacy Pledge*, BUS. INSIDER (Jan. 13, 2015, 8:33 PM), http://www.businessinsider.com/google-why-didnt-it-sign-president-obamas-student-privacy-pledge-2015-1; Molly Hensley-Clancy, *Google, Apple, Pearson Missing From Student Privacy Pledge*, BUZZFEED (Oct. 7, 2014, 11:44 AM), http://www.buzzfeed.com/mollyhensleyclancy/whos-missing-from-new-student-privacy-pledge-google-apple-pe#.mvQGgyPnd.

[45] Alistair Barr, *Why Google Didn't Sign Obama-Backed Student Privacy Pledge*, WALL ST. J.: DIGITS (Jan. 13, 2015, 8:49 AM), http://blogs.wsj.com/digits/2015/01/13/why-google-didnt-sign-obama-backed-student-privacy-pledge/.

to protecting student privacy.[46] But eventually both Google and Apple followed Microsoft's lead—and President Obama's coaxing—and signed onto the Pledge.[47]

Not all service providers, though, have been convinced. Pearson, the largest education textbook publisher and a major distributor of online education services,[48] is the company most conspicuously absent from the Pledge. Valued at over $8 billion,[49] the company is no stranger to controversy. For example, it recently lost a contract to supply education software to Los Angeles Unified School District,[50] in part because students managed to bypass the company's security and reach blocked websites.[51] Facebook has also not signed the Pledge, even though the company undoubtedly collects data from student users.[52] Facebook, though, has not received significant pressure to sign the Pledge, perhaps because the company might not qualify as a "school service provider" under the Pledge's definition.[53] Given its pervasiveness in schools, though, Facebook

---

[46] *Id.*

[47] Hayley Tsukayama, *Google, Khan Academy Join in Student Privacy Pledge*, WASH. POST (Jan. 20, 2015), http://www.washingtonpost.com/blogs/the-switch/wp/2015/01/20/google-khan-academy-join-in-student-privacy-pledge/.

[48] Jennifer Reingold, *Everybody Hates Pearson*, FORTUNE (Jan. 21, 2015), http://fortune.com/2015/01/21/everybody-hates-pearson/.

[49] *Id.*

[50] Valerie Strauss, *Los Angeles School District Drops Pearson Software on iPads, Seeks Refund from Apple*, L.A. TIMES (Apr. 16, 2015), http://www.washingtonpost.com/blogs/answer-sheet/wp/2015/04/16/los-angeles-school-district-drops-pearson-software-on-ipads-seeks-refund-from-apple/.

[51] Annie Gilbertson, *LA Schools To Apple: You Owe Us*, N.P.R. (Apr. 16, 2015, 4:37 PM), http://www.npr.org/blogs/ed/2015/04/16/400161624/l-a-schools-to-apple-you-owe-us.

[52] *Data Policy*, FACEBOOK, https://www.facebook.com/policy.php (last updated Sept. 29, 2016) ("We use the information we have to improve our advertising and measurement systems so we can show you relevant ads on and off our Services and measure the effectiveness and reach of ads and services."). Facebook has not received pressure to sign the Pledge, perhaps because the company might not qualify as a "school service provider" under the Pledge's definition. *See Student Privacy Pledge*, *supra* note 35 ("The term 'school service provider' does not include an entity that is providing, and that is operating in its capacity as a provider of, general audience software, applications, services or websites not designed and marketed for schools."). Even though Facebook would not necessarily be invited to sign the Pledge, I still use the company, along with Pearson, as a "control" variable to examine non-signatory policies. I include Facebook simply because of the company's size, influence, and pervasiveness.

[53] *See Student Privacy Pledge*, *supra* note 35 ("The term 'school service provider' does not include an entity that is providing, and that is operating in its capacity as a provider of, general audience software, applications, services or websites not designed and marketed for schools.").

still provides an interesting control-group comparison to the Pledge signatories.

II. ARE SIGNATORIES COMPLYING WITH THE PLEDGE?

In Companies of all sizes have promised to abide by the Student Privacy Pledge. But the Pledge's guarantees are of little value if signatories are not actually keeping their word.[54] And the industry's adoption of the Pledge could even backfire if there is rampant noncompliance: if companies prove unable or unwilling to meaningfully self-police, state and local government could be spurred to step in with more onerous regulations.

To shed light on the issue of compliance, I analyzed the privacy policies and terms of service[55] of the largest signatories—Apple, Google, and Microsoft[56]—and five randomly chosen smaller companies that also signed—Brain Hive, eScholar, Hapara, Schoolzilla, and Triumph Learning.[57] Notably, two early participants in the Pledge, Brain Hive and Triumph Learning, have since withdrawn as signatories.

Signatories to the Pledge have already come under scrutiny for practices that potentially violate their promises in the Pledge. Google, for example, has been the subject of an FTC investigation over targeting advertising toward children, something that the Pledge seeks to prohibit.[58] And a number of other signatories have been shown to have inadequate security measures for protecting student data, as revealed by "white hat" hackers (computer security experts whose purpose is to help rather than hurt companies).[59]

The following analysis takes a different approach to testing compliance with the Pledge—analyzing privacy policies and terms of service of eight Pledge signatories—and it too finds evidence that companies may not be practicing what they preach. At the outset, it is

---

[54] For the purposes of this Article, I take the companies' terms of service and privacy policies at face value. It is certainly possible, though, that the companies are more compliant with the Student Privacy Pledge than their public statements indicate. For example, companies can shield themselves liability for noncompliance but still in fact be in compliance with the Pledge.

[55] In some instances, I also analyzed additional links found on the companies' main pages or within their terms of service and privacy policies.

[56] *See Pledge Signatories*, *supra* note 4.

[57] I chose these companies by simply clicking random signatory icons on the Pledge's listing page.

[58] *See, e.g.*, Cameron, *supra* note 2; Matt O'Brien, *FTC Says It Will Review YouTube Kids Over Advertising Concerns*, MERCURY NEWS (Apr. 7, 2015, 9:50 AM), http://www.mercurynews.com/business/ci_27867309/ftc-says-it-will-investigate-youtube-kids-over.

[59] *See* Part III.A.7, *infra*.

helpful to visualize each company's outward compliance with the Pledge's major provisions:

Company	Status	Collection, use, and maintenance of student information	Sale of student personal information	Behavioral targeting of advertisements	Notice to account holders	Retention of personal information	Access to and corrections of information	Security	Vendors	Successors
eScholar:	current signatory, small	ok	not stated	not stated	not stated	not stated	not stated	ok	not stated	not stated
Hapara:	current signatory, small	potential violation	not stated	ok	ok	ok	ok	ok	ok	ok
Schoolzilla	current signatory, small	potential violation	potential violation	ok	ok	not stated	ok	ok	not stated	potential violation
Apple	current signatory, large	potential violation	not stated	potential violation	ok	potential violation	potential violation	ok	potential violation	potential violation
Google	current signatory, large	potential violation	ok	ok	ok	ok	ok	ok	not stated	ok
Microsoft	current signatory, large	potential violation	not stated	potential violation	not stated	not stated	ok	ok	not stated	not stated
Brain Hive	former signatory, small	potential violation	ok	not stated	ok	not stated	not stated	ok	not stated	not stated
Triumph Learning	former signatory, small	ok	not stated	not stated	potential violation	not stated	not stated	ok	not stated	ok
Facebook	non-signartory	potential violation	potential violation	not stated	ok	potential violation	not stated	not stated	ok	potential violation
Pearson	non-signartory	ok	not stated	potential violation	potential violation	not stated	not stated	ok	ok	potential violation

It is clear that many signatories hold themselves to a lower standard—at least in terms of protecting against liability—than what the Pledge promotes. Only one of the eight companies surveyed, eScholar, has no clear red flags. And even the lack of red flags is not completely encouraging; eScholar has simply remained silent (as indicated in cells labeled "not stated") in regard to many aspects of the Pledge, so there is no guarantee that the company is compliant. In addition to the current signatories to the Pledge, this chart also includes two former signatories—Brain Hive and Triumph Learning—and two large companies that never signed—Facebook, the social networking platform used by millions of students, and Pearson, the major print and online education company.

Interestingly, neither Facebook nor Pearson appear, in their outward statements, to be "worse" in terms of protecting student privacy than the current and former signatories to the Pledge. (For more information on Facebook and Pearson, see Appendix A, *infra*.)

Of course, this analysis is not a perfect representation of actual company practices. For one thing, the convoluted web of policies and terms that each company uses can sometimes convey conflicting messages and obscure the true situation. Companies may also have internal policies that are not disclosed to the general public, but rather appear in intra-company documents or private contracts between the companies and educators. Lastly, companies may write terms of service that are over-protective in shielding the companies from liability, beyond the companies' current practices or even expectations of future practices. In other words, my research merely serves as an indicator of general company practices and areas of the Pledge that deserve closer scrutiny from consumers, the FTC, and other regulators. It provides evidence that participation in the Pledge does not necessarily correlate with better protections for student data.[60]

And not only are signatories potentially violating the Pledge, but they are doing so in a variety of ways. This lack of uniformity means that parents and educators, lacking time and technical knowledge, may not be equipped to enforce the terms of the Pledge. As discussed in Part III, lack of uniformity and information costs for consumers are two reasons why legislators and regulators may be better positioned to enforce compliance with the Pledge. The remainder of this Section analyzes company compliance with each of the Pledge's key terms.[61]

---

[60] The Student Privacy Pledge does not provide signatories with a forgiveness window during which they can update their practices to comply with the Pledge. This means that when a company signs the Pledge, it is essentially broadcasting to consumers that it is in full compliance with all of the Pledge's prohibitions and affirmative promises.

[61] I have limited to discussion to only the most relevant and verifiable commitments in the Pledge. For example, I have omitted the commitment to clearly disclose the types of personal data collected. *See Pledge Signatories, supra* note 4 (commitment to "[d]isclose clearly in contracts or privacy policies, including in a manner easy for parents to understand, what types of student personal information we collect, if any, and the purposes for which the information we maintain is used or shared with third parties"). Although this is an important commitment, it is impossible to verify whether companies are "clearly disclosing" the types of data they collect without having information on what data the companies are *actually* collecting.

A. Collection, Use, and Maintenance of Student Information[62]

The first element of the Pledge appears to restrict the way that companies handle student data by limiting the use of such data to only what is needed for "authorized educational/school purposes."[63] But the Pledge allows some wiggle room in that signatories, in the absence of an authorized educational purpose, can broadly use and share student data if they receive parental consent.[64] Thus, the inquiry into compliance is twofold: do the companies agree to use student data for only authorized educational purposes and, if not, did they receive parental consent to use the data for other purposes?

Two current signatories—Schoolzilla and Hapara—have privacy policies that do not expressly limit collection to uses authorized for educational purposes or approved by parents, while a third—eScholar—claims it simply does not collect any student data.[65] At Hapara, for example, "[s]tudent Information is used to provide our Services and support."[66] The vagueness in the term "provide . . . Services and support" could allow Hapara to use data in ways beyond what is needed for educational purposes or expressly authorized by parents. Hapara's policy further shields the company from culpability for collecting unauthorized student data by placing the burden on students to avoid providing such information: "We do not knowingly collect any personal information directly from children under the age of thirteen through the Website and the Services."[67] Because the

---

[62] *Student Privacy Pledge*, *supra* note 35 (commitment to "[n]ot collect, maintain, use or share student personal information beyond that needed for authorized educational/school purposes, or as authorized by the parent/student"). The Privacy Pledge also affirmatively states that companies will "[c]ollect, use, share, and retain student personal information only for purposes for which we were authorized by the educational institution/agency, teacher or the parent/student." *Id.* For the purposes of this discussion, I have conflated these two factors.

[63] *Id.*

[64] *Id.*

[65] *See Security and Privacy*, ESCHOLAR, http://www.escholar.com/company/security-privacy/ (last visited Jul. 22, 2017) ("Customers that deploy eScholar software on their own agency's servers can be assured that their data is completely under their agency's control. Their data is not transmitted to, or stored, on eScholar servers. Only a small fraction of agencies also contract with eScholar to host their data. Only in those cases does eScholar host any education data. The hosting provisions of those contracts contain clear language dictating the policies and procedures regarding access to and handling of those data.").

[66] *Privacy Policy*, HAPARA, https://hapara.com/privacy-policy/ (last updated Jul. 13, 2017).

[67] *Id.*

Pledge, unlike federal child privacy laws,[68] contains no mental state requirement, Hapara's agreement not to "knowingly" collect student data does little to avoid a conflict with the Pledge's terms: a violation is a violation regardless of knowledge or intent. Nor does the Pledge distinguish, as Hapara does, between students under or over age thirteen. And rather than waiting for affirmative parental consent, as the Pledge requires, Hapara merely allows parents to opt out of data collection for students under the age of thirteen.[69]

Meanwhile, Schoolzilla broadens the contractual definition of an authorized education purpose to a nearly limitless degree. The company states that schools may provide Schoolzilla with "access to certain information about or related to You and/or the school or district You are affiliated with ("School"), including "without limitation" personally identifiable and/or performance data regarding the students and staff thereof," and instructs the school or administrator that "[y]ou hereby grant Schoolzilla an irrevocable, perpetual, non-exclusive, worldwide, royalty-free right and license to use and exercise all rights in the Data in connection with providing and improving its products and Services."[70] The language conflicts with the Pledge, which requires not only school authorization in order for companies to collect data, but also that companies only collect data for "authorized educational/school *purposes*, or as authorized by the parent/student."[71] School authorization alone is insufficient when the collection goes beyond authorized educational/school purposes.

Of the two companies that initially signed the pledge but later withdrew, one does not collect students' personally identifiable information and so would not be at risk of violating this provision.[72] The other, Brain Hive, may collect data in a way that is impermissible under the Pledge. The company requires parents to opt out of, rather than affirmatively opt in to, collection of data for non-authorized purposes. The company states that it will "advise the parent or guardian of the *right to tell us* that the personally identifiable information which we have collected for the child is not to be

---

[68] COPPA, for example, only applies to web sites that are directed at children or which have "actual knowledge" that they are collecting personal information from children. 15 U.S.C. § 6502.

[69] *Privacy Policy*, HAPARA, *supra* note 66 ("If you have reason to believe that a child under the age of 13 has provided personal information to us, please contact us . . . , and we will endeavor to delete that information from our databases.").

[70] *Terms of Service and Privacy Policy*, SCHOOLZILLA, https://schoolzilla.org/terms-privacy (last updated Apr. 28, 2017).

[71] *Student Privacy Pledge*, *supra* note 35.

[72] *Student Privacy Policy*, TRIUMPH LEARNING, http://www.triumphlearning.com/assets/page/student-privacy-policy.html (last visited Jul. 21, 2017) ("Triumph Learning does not collect personal information directly from Children online at any point.").

used for any activity other than the activity for which it was collected."[73] The policy further notes that it "may" ask for consent from a parent or guardian "before collecting or using any personally identifiable information from a child under the age of 13."[74] The company also states that it may collect student personally identifiable information for the purpose of seeking parental consent.[75] Brain Hive's policy makes no mention of whether such collection will be for authorized educational purposes. Notably, by the time Brain Hive actually obtains parental consent to collect student data for non-education purposes, the company may have already collected student data for non-education purposes—in violation of the Pledge's terms.

The big companies—Apple, Google, and Microsoft—are no better (and may actually be worse) when it comes to student data. Not only does Apple stipulate that it may collect and use personally identifiable information, it actually requires customers to supply this information as a condition of using Apple services.[76] On top of that, Apple gives itself complete latitude to disclose information "when Apple determines that applicable law requires *or permits* such disclosure."[77] And, unlike some smaller companies, Apple does not allow users to opt out of the company's use of collected personal information, "because this information is important to [users'] interaction with Apple."[78] Apple does claim that it will "take steps" to delete personally identifiable information of students under thirteen years old, "if [Apple] learns" that it has done so.[79] But there are two problems with this narrow protection: First, the Student Privacy Pledge does not allow companies to collect personally identifiable information, regardless of whether the collection was intentional or knowing. Second, the Pledge's protections are not limited to students who are under thirteen years old.

Microsoft's policy closely resembles Apple's. The company "block[s] users under 13 or will ask them to provide consent from a parent

---

[73] *Privacy Policy*, BRAIN HIVE, http://www.brainhive.com/Pages/Privacy-Policy.aspx (last visited Jun. 21, 2017) (emphasis added).
[74] *Id.*
[75] *Id.*
[76] *Privacy Policy*, APPLE, https://www.apple.com/legal/privacy/en-ww/ (last updated Sept. 19, 2017) ("You are not required to provide the personal information that we have requested, but, if you chose not to do so, in many cases we will not be able to provide you with our products or services or respond to any queries you may have.").
[77] *Apple Website Terms of Use*, APPLE, https://www.apple.com/legal/internet-services/terms/site.html (last updated Nov. 20, 2009) (emphasis added).
[78] *Privacy Policy*, APPLE, *supra* note 76.
[79] *Id.*

or guardian before they can use it."[80] And, like Apple, Microsoft only states that it will not "knowingly" collect more data than necessary for the education service.[81] Such policies may encourage willful ignorance: A company like Microsoft can collect all sorts of information from young students, so long as the company never asks about or otherwise learns the students' ages. Moreover, in Microsoft's case, once a child or parent gives consent, "the child's account is treated much like any other account . . . ."[82] This means that Microsoft could, by its own terms, use the data "(1) to operate [its] business and provide . . . products [Microsoft] offer[s], (2) to send communications, including promotional communications, and (3) to show advertising . . . ."[83]

Depending on how one interprets the Pledge's language, Google may be on stronger footing. Unlike Apple and Microsoft, Google does not state that it will collect and use student data. The company does, however, scan emails—including those in its "Google Apps for Education Service"—to perform tasks like auto-detection of calendar events and provide "relevant search results."[84] It is unclear whether a "100% automated" process"[85] alleviates potential privacy concerns, but the Pledge certainly makes no explicit exception for such automated data collection and monitoring.

Overall, companies that sign the Pledge assure consumers that they will only use data for education purposes or with parental consent; yet many of these companies nonetheless ask consumers to consent—or affirmatively opt out of default consent—to a potentially much broader usage of student data.

B. Sale of Student Personal Information[86]

The Pledge contains strong, unequivocal language prohibiting companies from selling student personal information.[87] Unlike the collection term discussed above, the Pledge absolutely prohibits sales of student personal data regardless of parental consent.[88] Compliant companies

---

[80] *Microsoft Privacy Statement*, MICROSOFT, https://privacy.microsoft.com/en-US/privacystatement/ (last updated Oct. 2017).
[81] *Id.*
[82] *Id.*
[83] *Id.*
[84] *Privacy and Security*, GOOGLE, https://edu.google.com/k-12-solutions/privacy-security/?modal_active=none (last visited Jul. 22, 2017).
[85] *Id.*
[86] *Student Privacy Pledge*, *supra* note 35 (commitment to "[n]ot sell student personal information").
[87] *Id.*
[88] *See id.*

should therefore be able to state, unequivocally, in their consumer-facing policies that they do not sell student data. Yet Google is the only company that does this.[89] Many companies, instead, are simply silent as to their policy in regard to selling data.

A number of signatories may be in violation of the prohibition on selling student information. Schoolzilla tells users that it does not sell any personally identifiable data, "except as You've requested or authorized Schoolzilla to do so through the Services."[90] Although this may be a reasonable policy, it is not allowed by the Pledge because it turns on consent whereas the Pledge absolutely prohibits such sales. Most of the small signatories, however, have simply remained silent as to whether they sell student information. Interestingly, a former signatory, Brain Hive, actually provides greater protection than the smaller companies that remain as signatories.[91]

All of the large companies are either silent (Microsoft and Apple) or expressly state that they will not sell student data (Google). But these companies are so diversified in the services they offer that the primary value of data from students may be for use in delivering other intra-company services rather than for selling to third parties. The silence as to the sale of data to third parties may therefore reflect a business model not concerned with sales of student data to third parties. If so, the third-party sale term of the Pledge may not be completely effective. Google, for example, would seemingly be compliant even if it transferred data from its education services to other departments within the company, like Google Shopping. On the other hand, the silence could also reflect noncompliance: Apple, for example, has been accused of conduct that would violate the Pledge's ban on selling personal information, although the alleged conduct occurred before Apple signed onto the Pledge.[92]

Either way, the sale of student information warrants further attention from consumers and regulators.

---

[89] *See Privacy and Security*, GOOGLE, *supra* note 84 ("We don't sell your G Suite data to third parties, and we do not share personal information placed in our systems with third parties, except in the few exceptional circumstances described in the G Suite agreement and our Privacy Policy, such as when you ask us to share it or when we are required to do so by law.").

[90] *Terms of Service and Privacy Policy*, SCHOOLZILLA, *supra* note 70.

[91] *Privacy Policy*, BRAIN HIVE, *supra* note 73, ("The information is used exclusively by Brain Hive and its publishing partners and is not shared with other organizations for commercial purposes.").

[92] *See Apple Accused of Selling Customers' Personal Information*, RT (Jan. 21, 2014, 8:39 PM), http://rt.com/usa/apple-zip-code-lawsuit-987/.

C. Behavioral Targeting of Advertisements[93]

As with the sale of personal information, the Pledge also takes a hard line against targeting advertisements toward students, i.e., using behavioral student data to tailor advertisements to their preferences. Such advertisements are prohibited, regardless of whether the targeting draws on personal or non-personal information.[94] Interestingly, there is a noticeable difference between the ways that small companies and large companies address behavioral targeting of advertisements.

None of the smaller companies include language in their policies that indicates they might be violating the provision on behavioral targeting. The companies that do mention the issue, Hapara and Schoolzilla, expressly state that they do not engage in behavioral targeting for advertising purposes.[95]

By contrast, at least two of the three large companies surveyed expressly state that they *do* use data for behaviorally targeted advertisements. Apple "may use 'cookies' and other technologies such as pixel tags and web beacons . . . [to] better understand user behavior, tell us which parts of our websites people have visited, and facilitate and measure the effectiveness of advertisements and web searches."[96] Apple "treat[s] information collected by cookies and other technologies as non−personal information. . . . [and] use[s] cookies and other technologies to remember personal information when [customers] use [Apple's] website, online services, and applications."[97] The company requires users to opt out if they do not want to be tracked for advertising purposes.[98] And Apple also tracks "click-through data" to help the company "determine interest in particular topics and measure the effectiveness of [its] customer communications."[99] The only means of avoiding such tracking, according to Apple, is for users to not click links in Apple email messages.[100] Similarly, Microsoft uses

---

[93] *Student Privacy Pledge*, *supra* note 35 (commitment to "[n]ot use or disclose student information collected through an educational/school service (whether personal information or otherwise) for behavioral targeting of advertisements to students . . . [or] build a personal profile of a student other than for supporting authorized educational/school purposes or as authorized by the parent/student").

[94] *Id.*

[95] *See Privacy Policy*, HAPARA, *supra* note 66 ("We do not behaviourally target advertising."); *Terms of Service and Privacy Policy*, SCHOOLZILLA, *supra* note 70 ("We will not use the Data for any purpose that is not disclosed in these Terms, including, without limitation, for any targeted advertising.").

[96] *Privacy Policy*, APPLE, *supra* note 76.

[97] *Id.*

[98] *Id.*

[99] *Id.*

[100] *Id.*

cookies to send targeted advertisements, and the company requires users to opt out if they wish to avoid being tracked for advertising.[101] It is worth noting that Apple and Microsoft's policies are not specific to education. But, in the absence of any education-specific policies to the contrary, the companies' seeming noncompliance with the Pledge is troubling.

Google, by contrast, does not collect or use student data for advertising in its Apps for Education service.[102] Nor does Google conduct automatic scans of student users' accounts for advertising purposes.[103] However, "there are additional services outside of the G Suite [educational] core services that G Suite users can access . . . . [that] are not governed by the Student Privacy Pledge or the G Suite agreement, so Google may use information in these services in ways we would not for G Suite core services." [104] Thus, students using one type of Google service may avoid behaviorally targeted advertising, but as soon as they switch to another service, Google may use their data for advertisements. Although this may not constitute a violation of the Pledge, it raises practical questions for schools and students who may not distinguish, as Google does, between Google Apps for Education ("G Suite") and Google's free services.

Despite my reliance on a small sample size, the disparity between large and small companies is notable, and may indicate that large, diversified companies place a higher value on advertising than small companies that provide only specific education services. Parents and educators may want to keep this difference in mind when large companies offer significantly lower prices for services: the trade-off for low prices could be opening up easily-influenced students to significant targeted advertising.[105]

---

[101] *Microsoft Privacy Statement*, *supra* note 80 ("When we display online advertisements to you, we will place one or more cookies in order to recognize your computer when we display an ad to you. Over time, we may gather information from the sites where we serve ads and use the information to help provide more relevant ads. . . . You can opt out of receiving interest-based advertising from Microsoft as described in the Access and Control section of this privacy statement.").

[102] *Privacy and Security*, GOOGLE, *supra* note 84.

[103] *Id.* ("We do NOT scan G Suite emails for advertising purposes.").

[104] *Id.*

[105] *See, e.g.*, Natasha Singer, *How Google Took Over the Classroom*, N.Y. TIMES (May 13, 2017), https://www.nytimes.com/2017/05/13/technology/google-education-chromebooks-schools.html?mcubz=0 (discussing Google's rapid infiltration of the education technology market and lingering questions about Google's use of student data for advertising purposes).

D. Notice to Account Holders[106]

The Pledge prohibits signatories from making material changes to privacy policies "without first providing prominent notice to the account holder(s)" and allowing account holders "choices" *before* their data is used in any manner inconsistent with the initial terms.[107] Most companies, large and small, take the basic step of providing users with notice if and when they make changes to their privacy policies. Some even guarantee that they will post notice for two weeks before actually implementing the changes.[108]

But none of the companies surveyed make any promise to give account holders "choices" before using their data in accordance with changes to terms of service as required by the Pledge. Instead, it appears the only choice users have if they do not like the new policy is to simply stop using the service, regardless of whether that policy is consistent with "terms they were initially provided."[109] Schoolzilla, for example, tells users that, after changes to its policies, "If you continue using our services (and we hope you do!), your continued use of Schoolzilla means you've accepted those changes."[110] Likewise, Apple simply states, "When we change the policy in a material way, a notice will be posted on our website along with the updated Privacy Policy."[111]

One former signatory is even worse: Triumph Learning's policy says the company may make changes to its privacy policy "at any time," and, rather than provide notice, a user's continued use of the service constitutes acceptance of the changes.[112] Triumph Learning therefore

---

[106] *Pledge Signatories*, *supra* note 4 (commitment to "[n]ot make material changes to school service provider consumer privacy policies without first providing prominent notice to the account holder(s) (i.e., the educational institution/agency, or the parent/student when the information is collected directly from the student with student/parent consent) and allowing them choices before data is used in any manner inconsistent with terms they were initially provided; and not make material changes to other policies or practices governing the use of student personal information that are inconsistent with contractual requirements").

[107] *Student Privacy Pledge*, *supra* note 35.

[108] *See, e.g.*, *Privacy Policy*, HAPARA, *supra* note 66 ("When material changes are made to this privacy policy, Hapara customers will be notified through the contact email given to us at least two weeks prior to modification taking effect."); *Privacy and Security*, GOOGLE, *supra* note 84 ("Changes will not apply retroactively and will become effective no sooner than fourteen days after they are posted.").

[109] *See Student Privacy Pledge*, *supra* note 35.

[110] *Terms of Service and Privacy Policy*, SCHOOLZILLA, *supra* note 70.

[111] *Privacy Policy*, APPLE, *supra* note 76.

[112] *Triumph Learning, LLC, Online Policy*, TRIUMPH LEARNING, http://www.triumphlearning.com/learn-more/privacy-policy (last visited Nov. 27, 2017).

recommends that its users check the privacy policy for updates "on occasion."[113]

Of course, companies may in practice give users the kind of choices envisioned in the Student Privacy Pledge. But because none of these companies affirmatively include this right in their privacy policies, consumers will likely have little recourse if the companies do offer the changes on a take-it-or-leave-it basis.[114]

E. Retention of Personal Information[115]

As with collection of student data, signatories to the Student Privacy Pledge also agree not to retain student personal information beyond the time period required to support a school purpose, or as authorized by the parent or student.[116] But, unlike the terms for data collection, signatories only violate this provision if they "knowingly" retain the information.[117] The terms also allow signatories wide latitude in deciding what would be "required" for educational purposes.

Only one small company mentions a data retention policy. This company, Hapara, appears to be compliant, stating that it retains student information "only for the period of time required to load the information into the cloud platform of the educational institution, our App, and in some instances, to accommodate support / troubleshooting activities."[118]

Among the large companies, Apple's retention policy is the most alarming. Although the company initially states it will only retain personally identifiable information for "the period necessary to fulfill the purposes" of its privacy policy, Apple then qualifies that statement "unless a longer retention period is required *or permitted* by law."[119] In other words, Apple asks users to contractually allow the company to retain data for as long as Apple is legally allowed to do so.

Google may also be in violation of the Pledge, putting the onus on schools and parents to affirmatively opt out of data retention. The company

---

[113] *Id.*

[114] For the purposes of this analysis and its corresponding chart, I do not consider companies' omission of a right to make changes to qualify as raising a red flag that a company is violating the Pledge. Instead, I only list Triumph Learning, with its affirmative statement that it can make changes without providing notice to users, as outwardly violating the Pledge.

[115] *Student Privacy Pledge*, *supra* note 35 (commitment to "[n]ot knowingly retain student personal information beyond the time period required to support the authorized educational/school purposes, or as authorized by the parent/student.").

[116] *See id.*

[117] *See id.*

[118] *See Privacy Policy*, HAPARA, *supra* note 66.

[119] *Privacy Policy*, APPLE, *supra* note 76 (emphasis added).

states, in regard to its educational services, that it "only keep[s] . . . personal information as long as [users] ask us to keep it" and "[i]f an education department, school or university decides to stop using Google, we make it easy for them to take their data with them."[120]

Thus, it appears that larger companies may be more likely to retain student information beyond the time required to provide educational services. This difference between large and small companies further suggests that larger companies may place a higher premium on obtaining student data for purposes beyond merely providing education services. It may be that these companies, with their sophisticated algorithms and diversified services, are able to extract more value from students' data than smaller companies.

F. Access to and Corrections of Information[121]

The Pledge requires companies to "[s]upport access to and correction of student personally identifiable information by the student or their authorized parent,"[122] and a number companies at least make the possibility of access and correction available to users. Hapara, upon request, will provide "confirmation as to whether [the company is] processing [users'] personal information, and have the data communicated to [users] within a reasonable time."[123] Users have the right to correct, amend, or delete their personal information if it is inaccurate or has been processed in violation of Hapara's privacy policy.[124] Schoolzilla states that, once users cease using its service, "[w]e will delete all student records in our possession using industry standard data deletion practices."[125]

Both Google and Microsoft likewise provide at least some means for users to access and edit personal information.[126] By contrast, Apple

---

[120] *Privacy and Security*, GOOGLE, *supra* note 84.

[121] *Student Privacy Pledge*, *supra* note 35 (commitment to "[s]upport access to and correction of student personally identifiable information by the student or their authorized parent, either by assisting the educational institution in meeting its requirements or directly when the information is collected directly from the student with student/parent consent").

[122] *Id.*

[123] *Privacy Policy*, HAPARA, *supra* note 66.

[124] *Id.*

[125] *Terms of Service and Privacy Policy*, SCHOOLZILLA, *supra* note 70.

[126] *Google Terms of Service*, GOOGLE, https://www.google.com/policies/terms/ (last updated Oct. 25, 2017) ("Some Services may offer you ways to access and remove content that has been provided to that Service."); *Microsoft Privacy Statement*, *supra* note 80 ("If you cannot access certain personal data collected by Microsoft via the links above or directly through the Microsoft products you use, you can always contact Microsoft by using our web form. We will respond to requests to access or delete your personal data within 30 days.").

provides significantly less encouraging language in its terms of service. Although the company allows users access "for any purpose including to request that we correct the data if it is inaccurate or delete the data," Apple will only comply if it "is not required to retain [the data] by law or for legitimate business purposes."[127] And Apple may deny requests when access "is not required by local law."[128] Although the language might sound progressive, the totality of Apple's commitment to access amounts to the company guaranteeing it will not break local laws. Thus, the company has given itself the widest legal latitude to reject any and all requests for access to data—in seeming violation of both the Student Privacy Pledge's spirit and letter.

Neither of the non-signatories state any policy in regard to accessing user information. This may be a mere coincidence, or it may show that the Pledge at least encourages participants to make representations of compliance with the Pledge's provisions. Regardless, it appears that most companies are receptive to requests to access and modify student information, possibly because education software companies depend on having accurate information for reporting student results. And in the event that companies are selling student information or otherwise using it for profit, there is also significant benefit in ensuring that information is accurate. Thus, most companies likely welcome volunteered corrections to student information.

G. Security[129]

Every Pledge signatory examined at least claims to have strong security measures in place.[130] And, although there is variety among the companies in terms of the security measures they claim to use, as well as the specificity with which they discuss their security, the Student Privacy Pledge is so vague—it stipulates only that security be "reasonably designed" to protect student information—that seemingly any company could argue that its system is compliant.[131] Notably, the Pledge does not include any requirements for encryption or other specific technologies for

---

[127] *Privacy Policy*, APPLE, *supra* note 76.

[128] *Id.*

[129] *Student Privacy Pledge*, *supra* note 35 (commitment to "[m]aintain a comprehensive security program that is reasonably designed to protect the security, privacy, confidentiality, and integrity of student personal information against risks -- such as unauthorized access or use, or unintended or inappropriate disclosure -- through the use of administrative, technological, and physical safeguards appropriate to the sensitivity of the information").

[130] I am not an expert on encryption and computer security, so this section will not go into the technical merits of each company's stated security measures. Instead (and as with the rest of the analysis), I take each company at its word.

[131] Singer, *supra* note 3.

protecting student data.[132] Thus, although companies may be compliant with the Pledge, parents and educators should not assume that such compliance necessarily means strong security protections.

Many of the companies I examined place their security measures in the context of complying with state and federal laws. Hapara, for example, "will implement reasonable and appropriate security measures to protect . . . personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into account the risks involved in processing and the nature of such data, and comply with applicable laws and regulations."[133] In addition to asserting compliance with state and federal laws, some companies also note their compliance with the Student Privacy Pledge as a circular means of proving their security bona fides.[134] Beyond noting compliance with applicable security laws and the Pledge, both small and large companies frequently note their use of encryption.[135]

Although the companies are likely compliant with the Pledge, their security measures may not be adequate to actually protect student personal information. Indeed, a *New York Times* examination revealed that roughly one-fifth of the initial signatories to the Pledge did not use encryption at the login stage of their platforms,[136] and many companies had not even begun full encryption at the time they signed, a relatively fundamental security step.[137] Zearn.org, for example, collects an array of information on student competency at mathematical skills, and requires children to provide the site with their birth dates, first and last names, and email addresses.[138] But even as Zearn (which is not one of the surveyed companies in this Article) was collecting this sensitive information—and after the company had signed the Privacy Pledge—the *New York Times* found that Zearn had failed to add

---

[132] *See id.*

[133] *Privacy Policy*, HAPARA, *supra* note 66.

[134] *See, e.g.*, *id.* ("[Hapara] has also committed to comply with the Student Privacy Pledge, coordinated by FutureofPrivacy.org."); *Privacy and Security*, GOOGLE, *supra* note 84 ("In order to reaffirm the commitments we've made to schools, Google has signed the Student Privacy Pledge.").

[135] *See, e.g.*, *Privacy Policy*, GOOGLE, https://www.google.com/policies/privacy/ (last modified Oct. 2, 2017) ("We encrypt many of our services using SSL."); *Privacy Policy*, HAPARA, *supra* note 66 ("On our website we gather information from visitors via webforms. These webforms use Secure Socket Layer (SSL) encryption technology to provide an industry standard safeguard against access by other users of the Internet.").

[136] Singer, *supra* note 3.

[137] Singer, *supra* note 40.

[138] Singer, *supra* note 3.

"important security protection."[139] Meanwhile, Raz-Kids.com, another signatory, was revealed to be using unencrypted and plain text passwords.[140]

The lack of specific security measures for the safety of students' personally identifiable information is concerning. And noncompliance with the Pledge, by its earliest adopters, is a worrisome indication that companies may be overstating the safety of their online platforms.

H. Vendors[141]

One of the most sweeping, and perhaps least realistic, aspects of the Student Privacy Pledge is that signatories must require vendors (i.e., subcontractors) to also comply with the Pledge in regard to any information shared by the company.[142] Many online companies today rely on array of outside services such as Google Analytics, Adobe Flash), making it difficult for the contracting companies—particularly smaller ones with limited resources—to ensure compliance by each individual subcontractor. Not surprisingly, then, very few companies make any guarantees in this regard. Only one company surveyed, Hapara, affirmatively states that it requires its vendors to comply with the Pledge.[143]

Moreover, many of the companies—both current and former signatories— expressly claim no responsibility for third party links that appear on their websites.[144] It is unclear whether such a disclaimer violates the Pledge, which only applies to vendors with whom information is shared "in order to deliver the educational service."[145] Signatories could potentially argue that the Pledge requires compliance from subcontractors providing education services, but not from subcontractors that serve other purposes.

---

[139] *Id.*

[140] Singer, *supra* note 27.

[141] *Pledge Signatories*, *supra* note 4 (commitment to "[r]equire that our vendors with whom student personal information is shared in order to deliver the educational service, if any, are obligated to implement these same commitments for the given student personal information").

[142] *See id.*

[143] *Privacy Policy*, HAPARA, *supra* note 66 ("All . . . third parties function as our agents, performing services at our instruction and on our behalf pursuant to contracts which require they provide at least the same level of privacy protection as is required by this privacy policy and implemented by Hapara.").

[144] *See, e.g.*, *id.* ("Hapara has no control over the privacy practices of [linked third party websites]."); *Privacy Policy*, BRAIN HIVE, *supra* note 73 ("We Are Not Liable for nor Do We Endorse Content on Links Found on OUR Site . . . "); *Triumph Learning, LLC, Online Policy*, *supra* note 112 ("The Linked Sites do not imply Triumph Learning's endorsement of material on any Linked Site, and Triumph Learning expressly disclaims all liability with regard to your access to such Linked Sites.").

[145] *See Student Privacy Pledge*, *supra* note 35.

Apple is the only company, though, that demonstrates an affirmative willingness to violate vendor provision of the Pledge. The company's privacy policy includes sweeping language absolving Apple of liability for third party links and services, with Apple instead putting the burden on users to vet third parties. [146]

Because monitoring third parties requires a potentially exponential increase in compliance monitoring—just one of the more-than-three-hundred signatories might use an array of different vendors, which may themselves use other vendors—enforcement may be unrealistic. That the Pledge contains such an unrealistic and essentially unenforceable provision does not reflect well on its overall trustworthiness.

I. Successors

There is significant disparity among the surveyed companies in regard to outward compliance with the provision that signatories may only allow data to go to a successor company if the successor is subject to the same commitments to student data privacy.[147] One of the smaller companies, Hapara, appears to be compliant with this provision. Hapara uses language that mirrors the Student Privacy Pledge: "All . . . transfers shall be subject to our commitments with respect to the privacy and confidentiality of such personal information as set forth in this privacy policy."[148] In contrast, Schoolzilla states that it "may transfer and assign any of its rights and obligations under this Agreement freely and without consent to an acquirer or an affiliate."[149]

Despite no longer being a signatory, Triumph Learning nonetheless appears to remain compliant with this aspect of the Pledge. The company says that, in the event of changes to its corporate structure, the company will "take steps to assure that the personal information is used in a manner consistent to this Policy."[150]

---

[146] *Privacy Policy*, APPLE *supra* note 76 ("Information collected by third parties, which may include such things as location data or contact details, is governed by their privacy practices. We encourage you to learn about the privacy practices of those third parties.").

[147] *Student Privacy Pledge*, *supra* note 35 (commitment to "[a]llow a successor entity to maintain the student personal information, in the case of our merger or acquisition by another entity, provided the successor entity is subject to these same commitments for the previously collected student personal information").

[148] *Privacy Policy*, HAPARA, *supra* note 66.

[149] *Terms of Service and Privacy Policy*, SCHOOLZILLA, *supra* note 70.

[150] *Triumph Learning, LLC, Online Policy*, *supra* note 112. Similar language appears in Google's privacy policy. *Privacy Policy*, GOOGLE, *supra* note 135 ("If Google is involved in a merger, acquisition or asset sale, we will continue to ensure the confidentiality of any personal information and give affected users notice before

Of the larger companies, Apple again is the most likely to be in violation of the Pledge, as its privacy policy places no conditions on Apple's freedom to transfer information to separate entities. The policy states that "in the event of a reorganization, merger, or sale we may transfer any and all personal information we collect to the relevant third party."[151]

Interestingly, both Facebook and Pearson, the two non-signatory companies surveyed, also allow themselves seemingly unlimited discretion in transferring data to successors. Facebook provides that "[i]f the ownership or control of all or part of our Services or their assets changes, we may transfer your information to the new owner" [152] and that all the company's rights are "freely assignable by us in connection with a merger, acquisition, or sale of assets, or by operation of law or otherwise."[153] Pearson, likewise, may share information with third parties "in the event that Pearson itself or any of its subdivisions or units goes through a business transition, such as a merger, divestiture, acquisition, liquidation or sale of all or a portion of its assets."[154]

Most signatories and former signatories do not reserve the uninhibited right to transfer student information to third party successors, while both non-signatories surveyed do. This could provide some limited evidence that the Pledge is effective in influencing the representations made to consumers in signatory companies' terms of service and privacy policies.

III. ENFORCING THE PLEDGE

Signatories to the Pledge potentially benefit from the positive publicity associated with being viewed as responsible corporate citizens who respect student privacy. However, very little has been done to hold these companies accountable for complying with the Pledge. This Section first discusses the ways in which the public—including parents and school administrators—can apply pressure to both the Pledge's signatories and non-signatories. Although public pressure may have some utility, the effectiveness of such pressure is limited. In the second half of this Section, I recommend that the FTC investigate the level of compliance with the Pledge, because the FTC can hold signatories accountable for deceptive practices discussed in the preceding section.

---

personal information is transferred or becomes subject to a different privacy policy.").

[151] *Privacy Policy*, APPLE, *supra* note 76.

[152] *Data Policy*, FACEBOOK, *supra* note 52.

[153] *Statement of Rights and Responsibilities*, FACEBOOK, https://www.facebook.com/terms.php (last updated Jan. 30, 2015).

[154] *Privacy Statement*, PEARSON, https://www.pearson.com/us/privacy-statement.html (last updated May 15, 2014).

A. Public Accountability

States, school districts, individual schools, and parents all have some discretion over which educational services they choose to purchase. In a completely transparent world, these interested parties could choose to award contracts to companies that adequately protect student privacy while denying contracts to companies that do not. But, in practice, it is not so easy to distinguish between responsible and irresponsible companies. As discussed above, many of companies' policies are vague or in direct conflict with the Pledge's terms. And, even with perfectly clear policies, it would be unreasonable to expect consumers of education software to comb through every single term from what could be a multitude of companies providing services to their students.

Despite the difficulties in determining whether companies are adequately protecting student data, public pressure has at times been an effective means of policing student data security. For example, a recent controversy involved inBloom, an education services provider (not a signatory to the Pledge) that sought to standardize data storage for school districts implementing Common Core.[155] In theory, standardizing data storage was an attractive possibility because it would reduce costs for schools. InBloom initially achieved great success, securing seed money in excess of $100 million from the Bill and Melinda Gates Foundation and the Carnegie Corporation.[156] And, soon after, nine states signed on to work with the company.[157]

While using inBloom, though, parents and educators discovered that the platform collected an incredible array of personal information about students, including the revelation that the site allowed students to be labeled with designations such as "perpetrator," "victim," or "principal watch list."[158] These designations could remain in inBloom's possession indefinitely.[159] Furthermore, inBloom's service agreements did not guarantee student data was protected from intrusion or attack.[160] Amid public uproar, many states subsequently broke ties with inBloom. In Louisiana, for example, state administrators removed all student data from inBloom servers after parents raised protested the company's collection of

---

[155] Singer, *supra* note 3.
[156] *Id.*
[157] *Id.*
[158] *Id.*
[159] *Id.*
[160] *Id.*

student social security numbers.[161] After Louisiana stopped using inBloom, at least five of the other nine states using the service cut ties.[162]

The inBloom example illustrates the way the public can rally around student privacy and punish companies who put sensitive student data in jeopardy. Interpreting the inBloom incident as a warning, other education service providers have implemented stronger data security measures. For example, ClassDojo (a signatory to the Pledge) claims that its apps are encrypted and regularly subjected to audits by security experts.[163]

Still, public enforcement is only completely effective if consumers understand what companies are doing with student data *before* they enter into contracts with education providers. And parents and educators may lack the resources and expertise necessary to verify whether companies are complying with the privacy pledge. Furthermore, once they have an agreement with education service providers, the contractual language may bar lawsuits.[164] For example, even though Apple, by signing the Pledge, agreed to allow a successor to maintain student personal information only if the successor is subject to the same privacy commitments as Apple,[165] the company's own terms of service—to which any user must consent—seems to prevent any private action should Apple break this promise: "[W]e may transfer any and all personal information we collect to the relevant third party."[166] More importantly filing a claim for breach of contract will not resolve the problem of leaked personal student information. After a breach, the damage to student privacy will have been done, and suing the companies or ceasing to do business with them would be little consolation.

---

[161] *Id.*

[162] *See id.*; Todd Engdahl, *CDE Cuts its Ties with inBloom Data Project*, CHALKBEAT (Nov. 13, 2013), http://co.chalkbeat.org/2013/11/13/cde-cuts-its-ties-with-inbloom-data-project/ (Colorado cut ties with inBloom); Mary Jo Madda, *Where inBloom Wilted*, EDSURGE (Feb. 5, 2014), https://www.edsurge.com/n/2014-02-05-where-inbloom-wilted ("Massachusetts is still deliberating over whether to use inBloom's services, according to inBloom representative Adam Gaber. New York and Illinois (with the exception of Chicago) are moving forward in their partnerships with inBloom.").

[163] Singer, *supra* note 27.

[164] *But see* C. Connor Crook, *Validity and Enforceability of Liability Waiver on Ski Lift Tickets*, 28 CAMPBELL L. REV. 107, 120–21 (2005) ("Courts are generally reluctant to enforce exculpatory clauses, especially those that include the negligence of the party attempting to enforce the clause. However . . . courts can take very nuanced approaches . . . .").

[165] *Student Privacy Pledge*, *supra* note 35.

[166] *Privacy Policy*, APPLE, *supra* note 76. On the other hand, courts have at times been willing to ignore exculpatory provisions in contracts.

B. The FTC's Role

Given the limits of consumer oversight—namely the lack of transparency among education service providers—the FTC can and should regulate Pledge signatories. The FTC's purpose is to "prevent business practices that are . . . deceptive or unfair to consumers" and "enhance informed consumer choice and public understanding of the competitive process."[167] To accomplish these goals, the FTC seeks to ensure that consumers have "access to accurate information."[168]

When companies break their public promises, the FTC can hold them accountable.[169] A good model for FTC enforcement of the Pledge can be seen in how the FTC oversees the transfer of data from the United States from the European Union,[170] The FTC provides a safe harbor framework, currently referred to as the "EU-U.S. Privacy Shield Framework," which is a streamlined process for U.S. companies to transfer data from the EU to the United States in a way that is consistent with EU Data privacy laws.[171] Participating companies benefit from the safe harbor's process by self-certifying that they are compliant with a number of requirements.[172] The

---

[167] FED. TRADE COMMISSION, ABOUT THE FTC 1 (2012), https://www.ftc.gov/about-ftc (last visited Nov. 18, 2017).

[168] *Id.*

[169] *See TRUSTe Settles FTC Charges It Deceived Consumers Through Its Privacy Seal Program*, FED. TRADE COMMISSION (Nov. 17, 2014), https://www.ftc.gov/news-events/press-releases/2014/11/truste-settles-ftc-charges-it-deceived-consumers-through-its; *see also* CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION: PRIVACY LAW AND POLICY 175–181 (2016) (describing how the FTC can leverage self-regulatory frameworks to sanction companies who break a public promise); Steven Hetcher, *The FTC as Internet Privacy Norm Entrepreneur*, 53 VAND. L. REV. 2041, 2057 (2000) ("Making representations to consumers, and then acting contrary to these representations, is apparently the sort of behavior the FTC is more inclined to take action against.").

[170] *Federal Trade Commission Enforcement of the U.S.-EU and U.S.-Swiss Safe Harbor Frameworks*, FED. TRADE COMMISSION, https://www.ftc.gov/tips-advice/business-center/guidance/federal-trade-commission-enforcement-us-eu-us-swiss-safe-harbor (last updated Dec. 2012). As of July 12, 2016, the Safe Harbor Framework was replaced with the Privacy Shield Framework. *See Privacy Shield*, FED. TRADE COMMISSION, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/privacy-shield (last visited Oct. 12, 2017). The FTC plays the same role it played under the Safe Harbor Framework in the new Privacy Shield Framework. Lesley Fair, *FTC Cases Affirm Commitment to Privacy Shield*, FED. TRADE COMMISSION (Sept. 8, 2017), https://www.ftc.gov/news-events/blogs/business-blog/2017/09/ftc-cases-affirm-commitment-privacy-shield.

[171] *Federal Trade Commission Enforcement of the U.S.-EU and U.S.-Swiss Safe Harbor Frameworks*, *supra* note 170; *Privacy Shield*, *supra* note 170.

[172] *Privacy Shield*, *supra* note 170.

FTC then enforces companies' Safe Harbor compliance, and noncompliant companies can be subject to FTC prosecution.[173]

For example, the FTC filed a complaint against Google in 2011 for violating its Safe Harbor promise when Google failed to notify users or allow them to opt out of data collection by two Google programs: Google Buzz and Gmail. According to the FTC, this lack of notice constituted a deceptive practice.[174] The case resulted in a settlement, which "bars [Google] from future privacy misrepresentations, requires it to implement a comprehensive privacy program, and calls for regular, independent privacy audits for the next 20 years."[175] More recently, the FTC settled another Safe Harbor case against TES Franchising for deceiving consumers about dispute resolution procedures.[176] TES Franchising stated on its website that Safe Harbor-related disputes would be settled in Connecticut by an arbitration agency, and parties to the dispute would split costs, whereas the Safe Harbor agreement required participating companies to "resolve disputes through the European data protection authorities, which do[es] not require in-person hearings and resolve[s] disputes at no cost to the consumer."[177]

The Student Privacy Pledge, like the Safe Harbor Agreement, invites FTC enforcement: "A company's security and other commitments made under the Student Privacy Pledge are legally enforceable. Under Section 5 of the Consumer Protection Act, the Federal Trade Commission (FTC) can take action against companies that commit deceptive trade practices."[178]..Commentators have likewise acknowledged that the FTC can and should FTC to enforce the Pledge: "Bottom line, both the Federal Trade Commission and the Education Department could and should ramp up their student privacy enforcement."[179] "Students have little recourse against current abuses."[180] Even the executive director of the industry-financed think tank, Future of Privacy Forum—which helped to develop the Pledge—acknowledged that "[c]ompanies that have security practice[s] that

---

[173] *Id.*

[174] *Google, Inc.*, 152 F.T.C. 435 (2011).

[175] *FTC Gives Final Approval to Settlement with Google over Buzz Rollout*, FED. TRADE COMMISSION (Oct. 24, 2011), https://www.ftc.gov/news-events/press-releases/2011/10/ftc-gives-final-approval-settlement-google-over-buzz-rollout.

[176] *FTC Settles with Two Companies Falsely Claiming to Comply with International Safe Harbor Privacy Framework*, FED. TRADE COMMISSION (Apr. 7, 2015), https://www.ftc.gov/news-events/press-releases/2015/04/ftc-settles-two-companies-falsely-claiming-comply-international.

[177] *Id.*

[178] *The Student Privacy Pledge and Security*, STUDENT PRIVACY PLEDGE (last visited Jan. 4, 2017), https://studentprivacypledge.org/the-student-privacy-pledge-and-security/.

[179] Singer, *supra* note 27.

[180] *Id.*

fall short [of the Pledge] can face legal liability."[181] The extent to which signatories are violating the Pledge's terms may constitute a "deceptive" practice that warrants an investigation by the FTC, which could ultimately lead to charges against companies that have engaged in deceptive practices.[182]

1. Deception Analysis

As the FTC has done with Safe Harbor participants, the Commission could conclude that some of the signatories to the Student Privacy Pledge are engaging in deceptive practices. The first prong of this analysis asks whether there has been a "representation, omission or practice that is likely to mislead the consumer."[183] A company signing the Pledge has expressly represented to the public that it complies with the Pledge's terms,[184] but the previously discussed evidence indicates that companies may not actually be doing so. This dissonance between the Pledge's terms and companies' actual terms of service certainly could support finding that the symbolic gesture of signing the Pledge is likely to mislead consumers. The situation is similar to the FTC's case against TES Franchising, where the company's claimed compliance with the Safe Harbor Agreement—specifically the Safe Harbor's proscribed arbitration procedures—was misleading because the company forced users to agree to an arbitration process that violated Safe Harbor arbitration rules.[185]

Under the second prong of the analysis, the representation is examined from the perspective of "a consumer acting reasonably in the circumstances."[186] "When a seller's representation conveys more than one meaning to reasonable consumers, one of which is false, the seller is liable for the misleading interpretation."[187] In the case of signing the Pledge, there is only one meaning any consumer could derive from a company

---

[181] Singer, *supra* note 2.

[182] In theory, the FTC could use its preventative powers to bring an action against companies for simply representing compliance with the Pledge but simultaneously disclaiming liability for noncompliance. However, it would be difficult to show any detriment to consumers, so the FTC would likely choose to save its resources for cases that would result in greater remedies.

[183] *FTC Policy Statement on Deception*, FED. TRADE COMMISSION (Oct. 14, 1983), https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception.

[184] *See Student Privacy Pledge*, *supra* note 35 ("We pledge to carry out responsible stewardship and appropriate use of student personal information according to the commitments below and in adherence to all laws applicable to us as school service providers.").

[185] *FTC Settles with Two Companies Falsely Claiming to Comply with International Safe Harbor Privacy Framework*, *supra* note 176.

[186] *FTC Policy Statement on Deception*, *supra* note 183.

[187] *Id.*

"committing" to follow the Student Privacy Pledge's guidelines: the company is compliant with the Pledge. Noncompliance in the face of such an unambiguous representation would certainly mislead a consumer acting reasonably under the circumstances.

Lastly, the representation must be material, i.e., "likely to affect the consumer's conduct or decision."[188] The FTC presumes that express claims, like publicly signing the Student Privacy Pledge, are material.[189] This presumption is bolstered by the extent of public pressure consumers, politicians, and analysts applied to Google and Apple to convince the companies to sign the Pledge.[190] Adding to the inference of materiality is the strong evidence that consumers—parents and educators—base their software decisions in substantial part on companies' ability to protect student privacy. The previously discussed example of inBloom, where states abandoned the company in response to public concerns about student privacy, shows the central importance of student privacy.[191] Likewise, independent research groups have criticized companies for failing to sign the Pledge.[192]

And the companies themselves treat the Pledge as material by advertising it.[193] Some companies, for example, list participation in the Pledge on their main webpage.[194] Others include the Pledge in their terms of service as evidence of their rigorous protections.[195] Such representations show that the companies perceive the Student Privacy Pledge as potentially

---

[188] *Id.*

[189] *See id*.

[190] *See, e.g.*, Hayley Tsukayama, *More than 70 Companies Just Signed a Pledge to Protect Student Data Privacy—With Some Notable Exceptions*, WASH. POST: THE SWITCH (Jan. 12, 2015), http://www.washingtonpost.com/blogs/the-switch/wp/2015/01/12/more-than-70-companies-just-signed-a-pledge-to-protect-student-data-privacy-with-some-notable-exceptions/; Tracy Mitrano, *Should Google Be a Signatory to Student Privacy Pledge?*, INSIDE HIGHER ED. (Oct. 7, 2014), https://www.insidehighered.com/blogs/law-policy-and-it/should-google-be-signatory-student-privacy-pledge.

[191] *See* Madda, *supra* note 162.

[192] *See generally* JONAS PERSSON, CTR. FOR MEDIA AND DEMOCRACY, PEARSON, ETS, HOUGHTON MIFFLIN, AND MCGRAW-HILL LOBBY BIG AND PROFIT BIGGER FROM SCHOOL TESTS A CMD REPORTERS' GUIDE (Mar. 30, 2015), https://www.prwatch.org/files/updated_03-30-15_pearson_ets_houghton_mifflin_and_mcgraw-hill_lobby_big_and_profit_bigger.pdf.

[193] *See, e.g.*, *Kraft, Inc. v. F.T.C.*, 970 F.2d 311, 323 (7th Cir. 1992) (concluding that the FTC reasonably inferred materiality on the basis of cheese-manufacturer's continued use of false advertisement about product's nutritional benefits).

[194] *See, e.g.*, ESCHOLAR, http://www.escholar.com/ (last visited Jun. 21, 2017).

[195] *See, e.g.*, *Privacy Policy*, HAPARA, *supra* note 66 ("Hapara has . . . committed to comply with the Student Privacy Pledge, coordinated by FutureofPrivacy.org.").

influencing consumer decisions. These representations support a conclusion that the information is "material" to consumers. With the three prongs of deception analysis satisfied, the threat of FTC enforcement could go a long way toward keeping companies compliant with the Pledge's terms.

2. Remedies

By pursuing companies for misrepresenting their compliance with the Pledge, the FTC can compensate for the downsides of consumer enforcement. For example, whereas private claims against the companies might be barred where users agreed to exculpatory language in the companies' terms of service, the FTC is not constrained by such waivers. Signatories cannot shield themselves from liability under the FTCA simply on the basis that their terms of service waive liability for acts that would violate the Pledge.

Furthermore, the FTC can prevent companies from violating the Pledge in the future, instead of simply punishing companies for past violations. For example, when the FTC settled a case against the security certification service, TRUSTe, the agency went beyond monetary damages (of $200,000), also prohibiting the company from making further misrepresentations about its certification process or timeline, its corporate status, or whether an entity participated in the TRUSTe program.[196] The FTC also placed new requirements on TRUSTe's recordkeeping and its communications with other companies and the FTC.[197] Because of the FTC's broad powers to investigate and craft remedies that go beyond those obtainable by private claimants, the agency is in the best position to enforce compliance with the Student Privacy Pledge.

CONCLUSION

Collection of student data has become ingrained in American education. And in an age when large-scale data leaks and identity thefts have become the norm, the protection of student privacy has rightly become a major concern. Although the Student Privacy Pledge represents a promising start, parents and educators need to know that signatories are not just paying lip service to the goal of protecting students.

Unfortunately, the companies surveyed in this Article do not appear completely committed to the Pledge's ideals. Instead, they enjoy the public approval that comes with participation in the Pledge but simultaneously disclaim liability for using data in ways that would violate both the spirit and letter of the Pledge.

---

[196] *See TRUSTe Settles FTC Charges it Deceived Consumers Through Its Privacy Seal Program*, *supra* note 169.
[197] *See id.*

If companies are indeed complying with the Pledge, then perhaps expansive state and national student privacy laws are not necessary. But this Article suggests that the Pledge may be a mirage, consoling consumers while providing little actual benefit. As legislators and regulators begin to lay a new national framework for protecting student data privacy, better understanding the role and value of the Student Privacy Pledge will be essential. The FTC is in the best position to shed light on companies that have misrepresented their compliance with the Pledge and to take prophylactic measures to protect student data.[198]

APPENDIX A: FACEBOOK AND PEARSON

A. COLLECTION, USE, AND MAINTENANCE OF STUDENT INFORMATION

Facebook:

- "We collect the content and other information you provide when you use our Services, including when you sign up for an account, create or share, and message or communicate with others. This can include information in or about the content you provide, such as the location of a photo or the date a file was created. We also collect information about how you use our Services, such as the types of content you view or engage with or the frequency and duration of your activities."[199]
- "To protect minors, we may put special safeguards in place (such as placing restrictions on the ability of adults to share and connect with them), recognizing this may provide minors a more limited experience on Facebook."[200]

Pearson:

---

[198] Reports suggest that the FTC is at least aware that the Student Privacy Pledge is a hot topic and that enforcement may be necessary. *See* Meghan Ottolini, *Complying With The 'Pledge To Protect Student Privacy,'* CRN (Jun. 17, 2015, 9:58 AM), http://www.crn.com/news/security/video/300077149/ftc-monitors-behavior-of-vendors-that-signed-student-privacy-pledge.htm.

[199] *Data Policy*, FACEBOOK, *supra* note 52.

[200] *Minors and Safety*, FACEBOOK, https://www.facebook.com/about/privacy/minors (last visited May 25, 2017).

- "We may use this User Content and Service Usage Information in combination with your personally identifying information to customize your experience using the Service by, among other things, making recommendations or forecasts. We may also use your User Content and Service Usage Information to suggest other features on the Service that we believe may be interesting to you."[201]
- "We will never request personally identifiable information from a Child in any of our public postings areas. We will not require a Child to disclose more personally identifiable information than is reasonably necessary to participate in any online activity."[202]
- "We do not knowingly collect personally identifiable information from Children either directly or passively except when a Child voluntarily submits such information through a 'Contact Us' link or a public posting area within the Service, if such feature is available."[203]
- "[I]f we have actual knowledge that a Child is sending or posting personally identifiable information on any area of the Service, we will use commercially reasonable efforts to delete such personally identifiable information as soon as practicable."[204]

B. SALE OF STUDENT PERSONAL INFORMATION

Facebook:

- "Here are the types of third parties we can share information with about you: Advertising, Measurement and Analytics Services (Non-Personally Identifiable Information Only)[,] . . . Vendors, service providers and other partners."[205]
- "We do not share information that personally identifies you (personally identifiable information is information like name or email address that can by itself be used to

---

[201] *Privacy Statement*, PEARSON, *supra* note 154.
[202] *Id.*
[203] *Id.*
[204] *Id.*
[205] *Data Policy*, FACEBOOK, *supra* note 52.

contact you or identifies who you are) with advertising, measurement or analytics partners unless you give us permission."[206]

C. BEHAVIORAL TARGETING OF ADVERTISEMENTS

Facebook:

- "we use *all* of the information we have about you to show you relevant ads."[207]

Pearson:

- "By using the service, you agree that Pearson may use, license and otherwise distribute any such non-personally identifiable information (anonymized data) available on this service, whether collected by Pearson or a third party, to assist in market evaluation, product assessment and improvement, educational research, and for other marketing and commercial purposes as reasonably determined by Pearson."[208]

D. NOTICE TO ACCOUNT HOLDERS

Facebook:

- "We'll notify you before we make changes to these terms and give you the opportunity to review and comment on the revised terms before continuing to use our Services."[209]

Pearson:

- "Pearson reserves the right to revise this privacy statement at any time, including to address new issues or reflect changes to our service. Such revisions become effective immediately upon notice to you. Notice may be given by any means including, but not limited to, posting the revised privacy statement on this service."[210]

---

[206] *Id.*
[207] *Id.*
[208] *Privacy Statement*, PEARSON, *supra* note 154.
[209] *Data Policy*, FACEBOOK, *supra* note 52.
[210] *Privacy Statement*, PEARSON, *supra* note 154.

E. RETENTION OF PERSONAL INFORMATION

Facebook:

- "Information associated with your account will be kept until your account is deleted, unless we no longer need the data to provide products and services."[211]
- "When you delete IP content, it is deleted in a manner similar to emptying the recycle bin on a computer. However, you understand that removed content may persist in backup copies for a reasonable period of time (but will not be available to others)."[212]

F. SECURITY

Facebook:

- "We use the information we have to help verify accounts and activity, and to promote safety and security on and off of our Services, such as by investigating suspicious activity or violations of our terms or policies. We work hard to protect your account using teams of engineers, automated systems, and advanced technology such as encryption and machine learning. We also offer easy-to-use security tools that add an extra layer of security to your account."[213]

Pearson:

- "Our servers use Secure Sockets Layer (SSL), an advanced encryption technology that works with most major browsers. This technology safeguards your personal information and privacy. However, you should understand that 'perfect security' is never guaranteed."[214]

---

[211] *Data Policy*, FACEBOOK, *supra* note 52.
[212] *Statement of Rights and Responsibilities*, FACEBOOK, *supra* note 153.
[213] *Data Policy*, FACEBOOK, *supra* note 52.
[214] *Privacy Statement*, PEARSON, *supra* note 154.

G. VENDORS

Facebook:

- "We transfer information to vendors, service providers, and other partners who globally support our business, such as providing technical infrastructure services, analyzing how our Services are used, measuring the effectiveness of ads and services, providing customer service, facilitating payments, or conducting academic research and surveys. These partners must adhere to strict confidentiality obligations in a way that is consistent with this Data Policy and the agreements we enter into with them."
- "Information collected by these apps, websites or integrated services is subject to their own terms and policies."

Pearson:

- "When you conduct a purchase transaction through this Service, you are providing transaction information to our third party suppliers (such as transaction processors and financial institutions) who will use the information solely for the purpose of processing a purchase transaction. There may also be other third party vendors who supply software applications, web hosting and other technologies and/or other services for this Service that may have access to your personal information but they will not use such information for any other purpose except to provide services in connection with this Service."[215]

H. SUCCESSORS

Facebook:

- "If the ownership or control of all or part of our Services or their assets changes, we may transfer your information to the new owner."[216]
- "All of our rights and obligations under this Statement are freely assignable by us in connection with a

[215] *Id.*

[216] *Data Policy*, FACEBOOK, *supra* note 52.

> merger, acquisition, or sale of assets, or by operation of law or otherwise."[217]

Pearson:

- "We will not share any personally identifying information about you with any third party (a party not affiliated with Pearson) except as otherwise stated herein and in the following circumstances: . . . (iv) in the event that Pearson itself or any of its subdivisions or units goes through a business transition, such as a merger, divestiture, acquisition, liquidation or sale of all or a portion of its assets, your personal information will, in most instances, be part of the assets transferred . . . ."[218]

[217] *Statement of Rights and Responsibilities*, FACEBOOK, *supra* note 153.
[218] *Privacy Statement*, PEARSON, *supra* note 154.