FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY

CHRIS JAY HOOFNAGLE

CAMBRIDGE

FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY

The Federal Trade Commission, a US agency created in 1914 to police the problem of "bigness," has evolved into the most important regulator of information privacy – and thus innovation policy – in the world. Its policies profoundly affect business practices and serve to regulate most of the consumer economy. In short, it now regulates our technological future. Despite its stature, however, the Agency is often poorly understood by observers and even those who practice before it. This volume by Chris Jay Hoofnagle – an internationally recognized scholar with more than fifteen years of experience interacting with the FTC – is designed to redress this confusion by explaining how the FTC arrived at its current position of power. It will be essential reading for lawyers, legal academics, political scientists, historians, and anyone who is interested in understanding the FTC's privacy activities and how they fit in the context of the Agency's broader consumer protection mission.

Chris Jay Hoofnagle is adjunct full professor at the University of California, Berkeley, School of Information, and faculty director of the Berkeley Center for Law & Technology at the School of Law. He teaches about the regulation of technology, focusing on computer crime law, cybersecurity, internet law, privacy law, and consumer protection law. Licensed to practice in California and Washington, DC, Hoofnagle is of counsel to Gunderson Dettmer LLP, a firm focused solely on advising global venture capital and emerging technology companies. He is an elected member of the American Law Institute.

Federal Trade Commission Privacy Law and Policy

CHRIS JAY HOOFNAGLE
University of California, Berkeley

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE
UNIVERSITY PRESS

32 Avenue of the Americas, New York, NY 10013-2473, USA

Cambridge University Press is part of the University of Cambridge.

It furthers the University's mission by disseminating knowledge in the pursuit of education, learning, and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/9781107565630

First published 2016

Printed in the United States of America

A catalog record for this publication is available from the British Library.

Library of Congress Cataloging in Publication Data
Hoofnagle, Chris Jay, author.
Federal Trade Commission privacy law and policy / Chris Jay Hoofnagle.
New York : Cambridge University Press, 2016. | Includes bibliographical references and index.
LCCN 2015048481 | ISBN 9781107126787 (hardback)
LCSH: Privacy, Right of – United States. | Data protection – Law and legislation – United States. | Consumer protection – Law and legislation – United States. | United States. Federal Trade Commission.
LCC KF1262 .H66 2016 | DDC 342.7308/58–dc23
LC record available at http://lccn.loc.gov/2015048481

ISBN 978-1-107-12678-7 Hardback
ISBN 978-1-107-56563-0 Paperback

7

Privacy of children

The FTC has a long history of intervening in the marketplace to protect children. Recall from Chapter 1 that in the seminal case *FTC* v. *R. F. Keppel & Bro., Inc.*,[1] the Agency stopped a company from marketing candy to children with lottery-like inducements. In *Keppel*, some candies were packaged with a coin, so, once opened, the candy would technically be free, while non-winners would have to pay the price on the label. The FTC saw this as a form of gambling inappropriate for children.

With the advent of the commercial internet, similar, game-like tactics were used to entice children to reveal personal information online. Targeting of children online seemed to impinge on familial rights to privacy, and the right to privacy in the home. At the same time, the US privacy regime was viewed with skepticism by Europeans, who could point to the lack of protection for children in the US framework as a serious omission and signal of a generally weak commitment to privacy rights. After all, contracts are not enforceable against children in the United States, nor do we conceive of children as rational actors who can bargain for their privacy in the marketplace.[2] For Europeans, it was laissez-faire at its worst for children to be subject to the same privacy regime and roles as adults.

Widespread adoption of the internet also created a new risk landscape for children. High-profile stories circulated in the media about children using the internet with a technical skill that exceeded their judgment.[3] Law enforcement and state attorneys general invoked horrific anecdotes of child predation and luring made easier because of the internet.[4]

[1] 291 U.S. 304 (1934).

[2] Wouter M. P. Steijn & Anton Vedder, *Privacy under Construction: A Developmental Perspective on Privacy Perception*, Sci. Tech. Hum. Val. (2015).

[3] Brad Stone & Bronwyn Fryer, *The Keyboard Kids: Chatting on the Net Is Becoming the Social Activity of Choice for Techno-Savvy Early Teens*, Newsweek, June 8, 1998.

[4] Marlise Simons, *Dutch Say a Sex Ring Used Infants on Internet*, N.Y. *Times*, July 19, 1998; Elsa Brenner, *Child Abuse on Internet Heightens Vigilance*, N.Y. Times, April 19, 1998.

With these concerns in mind, Congress quickly enacted the Children's Online Privacy Protection Act of 1998 (COPPA). It was enacted in a matter of just months. As a result, COPPA had almost no legislative history to build upon, which led it to be used by different factions as both an information privacy law and an online safety measure.

Recall from Chapter 6 that Priscilla Regan described privacy as a topic that could start a public controversy, but often privacy could not marshal Congress to action. With COPPA, privacy concerns were sufficient to create legislative concern, but the law probably would not have been enacted without the added support of online safety advocates. This coalition between both privacy and safety advocates created an inherent weakness in the COPPA. Concerns about safety caused Congress to build a framework with scant regard to how children might want to use interactive services. Safety concerns also caused Congress to try to perfect the online environment against risks of child predation.

In the legal and business community, COPPA is seen as too burdensome, causing a bimodal response. Sites either fully embrace a child-oriented status that triggers COPPA, and then comply with the rules, or eschew it completely, sometimes by declaring that individuals under a certain age cannot use the site at all. Because of the all-or-nothing approach, children have only limited and sometimes unattractive options online. COPPA created incentives to develop services that are one-way, television-like broadcasting services. Designers do this because interactivity triggers legal duties under COPPA. Children also learn to lie about their age in order to join fun, highly interactive services that are supposedly only used by adults. In joining, children lose all the protections of COPPA. Yet, many of these protections are indeed sensible and could form the building blocks of a good law for adults' privacy.

Internet businesses see COPPA as difficult and burdensome, but, at the same time, COPPA has many effective protections. Among them are the allocation of privacy responsibilities for the behavior of vendors, such as third-party trackers, to the service; limitations on how data can be used; limitations on tracking; rules on how much data can be collected; a regulatory incentive for contextual advertising and against behavioral tracking; and ceilings on how long data can be retained. Congress enacted such significant protections because we as a society agree that children are worth protecting. Yet, COPPA protects only those who are under 13 years old. Many adolescents and many adults desire similar protections for their online activities.

This chapter outlines the history of children's privacy issues and shows that privacy is sometimes a proxy for still-unresolved tensions surrounding how companies should be able to advertise to children. It charts the FTC's incremental steps to regulating children's privacy, and then to the enactment and substance of the Children's Online Privacy Protection Act, a law motivated by both online privacy and safety concerns. Finally, this chapter assesses the act, noting that its emphasis on the high-transaction-cost and ultimately unverifiable requirement of parental consent causes companies to avoid the law if possible.

CHILDREN'S PRIVACY

The privacy and security of children has been a third-rail issue for online businesses. Yet, kids' privacy issues are largely unregulated in the offline environment. The FTC's KidVid episode, where the FTC proposed banning television advertising to young children (see Chapter 2), cast a pall over government enthusiasm for similar initiatives. As a result, unresolved are issues raised by advertising to children, including an epidemic level of childhood obesity.[5] Because advertising itself is so difficult to regulate, child advocates have often used privacy to collaterally attack commercial attempts to influence children.

Until the 1990s, it was commonplace for database marketing companies to sell lists of children by age and their home addresses for advertising purposes. For instance, data brokers would sell lists of contact information for four- to six-year-old children. This practice came into scrutiny in 1996, when the longtime CNN reporter Kyra Phillips, then working for a Los Angeles television station, purchased personal information on 5,500 children from Metromail, a data broker.[6] To purchase the children's contact information, Phillips used the name of a notorious suspected child killer.[7] Phillips' stunt generated publicity but it did not result in new restrictions on children's information. Instead, data brokers avoided regulation by renaming their products. The same information was sold but labeled as databases of households with "presence of children." Such a database would be labeled the "Single Parents with Multiple Children Mailing List."

Shortly thereafter, a report by Professor Kathryn Montgomery and Shelley Pasnik showed that marketers had developed sophisticated and ethically troubling methods to interact with children online.[8] As with previous generations of marketing science – motivational research and subliminal advertising – Montgomery and Pasnik only needed to quote the advertisers themselves to show an ugly landscape of businesses planning to target children who were at an age susceptible to persuasive messaging. The duo also described the troubling information collection techniques of mainstream brands. Consider a website operated by D.C. Comics: "At the Batman Forever Web site, supplying personal information becomes a test of loyalty. 'Good citizens of the Web, help commissioner Gordon with the Gotham Census,' children are urged. Although the survey uses the guise of a virtual city's census, much of the information sought by this questionnaire pertains to purchasing habits and video

[5] Elizabeth S. Moore, *Should Marketers Be Persuading Our Children?*, *in* MARKETING AND THE COMMON GOOD (Patrick E. Murphy & John F. Sherry, Jr., eds., 2014).

[6] Gary Chapman, *Protecting Children Online Is Society's Herculean Mission*, L.A. *TIMES*, June 24, 1996, at D14.

[7] Largest Database Marketing Firm Sends Phone Numbers, Addresses of 5,000 Families with Kids to TV Reporter Using Name of Child Killer, *BUS. WIRE* (May 13, 1996).

[8] KATHRYN MONTGOMERY & SHELLEY PASNIK, WEB OF DECEPTION: THREATS TO CHILDREN FROM ONLINE MARKETING (June 1996).

preferences. For example, respondents are asked how likely they are to buy Batman Forever and Apollo 13 on video."[9]

TELEVISION AND ONLINE ADVERTISING

In the 1950s and 1960s, television content began to attract public controversy, fed by the realization that game shows were rigged by commercial sponsors and concerns that the new medium was a powerful force for influence over consumers. Even laissez-faire commissioner Lowell Mason thought television advertising was unseemly, calling it the "pitchman in the parlor." Consumer advocates found the new medium immersive, that advertising on it exploited anxieties, that it had subliminal powers, and that it was harming viewers' well-being. The FTC started enforcement actions concerning activities such as false mock-ups and demonstrations on television that had been allowed for decades in magazines and newspapers.[10]

Could online advertising be triggering new objections because it is an unfamiliar medium? Just like television advertising, online advertising's advocates wildly overstate the power of their ads. A study by Google found that half of all digital ads are never seen by consumers. Added to this, in the study Google counted an ad as "viewable" if 50 percent of the ad was on the screen for a single second.[11] A miniscule percentage of consumers actually click on ads; in fact, "fat thumbs" and fraud probably contribute to more clicks than real traffic. Are advocates overreacting to a new, unfamiliar medium based on its hype? Will we soon learn that online advertising is not much more effective than other methods?

On the other hand, skilled advocates can recast online advertising as not a problem with marketing, but rather a problem of unrestrained surveillance of individuals. Viewed from a different lens, behavioral tracking, rather than ads, becomes a modern boogeyman.

By focusing on major advertisers, Montgomery and Pasnik showed that eliciting information from children using prizes and the like was a mainstream activity. Advertisers integrated pitches into the story content, obscuring the line between entertainment and marketing. These companies also used passive tracking

[9] *Id.*

[10] Peter Braton Turk, The Federal Trade Commission Hearings on Modern Advertising Practices: A Continuing Inquiry into Television Advertising (1977) (Ph.D. dissertation, University of Wisconsin, Madison, WI).

[11] Google, The Importance of Being Seen: Viewability Insights for Digital Marketers and Publishers (November 2014).

techniques, such as cookies, to follow children over time, raising the risk that interests and desires could be profiled and used to pitch more persuasive messages.

In May 1996, Montgomery's organization, the Center for Media Education (CME), petitioned the FTC to investigate KidsCom.com, one of the sites described in the report: "The KidsCom communications playground, aimed at children 4 to 15, uses a forceful approach. In order to enter the site, each child is required to disclose his/her name, age, sex and E-mail address. The mandatory questionnaire also requests his/her favorite TV show, commercial and musical groups, as well as the name of the child who referred him/her to KidsCom. Once children have entered the playground, they are encouraged to supply additional personal information in order to win 'KidsCash,' a form of virtual money that can be used to purchase conspicuously-placed products."[12]

Just over a year later, FTC staff released a public letter concerning the company.[13] The FTC opined that it would be deceptive for KidsCom.com to collect information from children and reveal it to others without parental notice and consent. If a disclosure to third parties occurred, it could rise to an unfair practice because of the risk of child predation. Yet the FTC chose not to take enforcement action, because KidsCom changed its practices, there was no evidence that it broadly released data to third parties, and an enforcement action could have had unintended policy effects on the emerging internet marketplace.

By 1998, the FTC and the White House[14] recommended legislation to protect privacy of children online. Upon Congressional request, the FTC studied the issue and the results were dismal – almost all child-oriented websites collected personal information from children while only about half had privacy policies.[15] In the physical world, such information collection was usually mediated by a parent or another responsible adult, but online, children were being encouraged to reveal personal information about themselves and others and frequently in troubling ways. For instance, some sites made information disclosure a kind of contest, where children were rewarded for revealing data useful to marketers, and the site then posted the information for anyone to see. Another site attempted to connect kids with "pen pals," listing children's ages and contact information. Such practices made it easy for the FTC to connect the dots between child-oriented websites and

[12] *Id.*

[13] Letter from Jodie Bernstein, Director, FTC Bureau of Consumer Protection, to Kathryn C. Montgomery, President, Center for Media Education (July 15, 1997).

[14] Office of the Vice President, Vice President Gore Announces New Steps toward an Electronic Bill of Rights, July 31, 1998 ("Children's privacy: The Administration will seek legislation that would specify a set of fair information principles applicable to the collection of data from children, such as a prohibition on the collection of data from children under 13 without prior parental consent. The Federal Trade Commission would have the authority to issue rules to enforce these standards. Legislation is needed because children under 13 may not understand the consequences of giving out personally identifiable information.")

[15] Federal Trade Commission, Privacy Online: A Report to Congress (June 1998).

physical safety from child predators, strengthening the call for regulation by adding personal safety to personal privacy concerns.

The FTC began a case-by-case enforcement strategy concerning child-oriented websites. In 1999 (before COPPA was in effect), the FTC settled a matter against GeoCities, an online service provider that shared children's information with third parties despite promising not to.[16] Another pre-COPPA matter concerned sites that elicited personal information about children and their families' finances through contests and games.[17] The FTC also sued a company that promised to never sell children's personal information but then attempted to use its customer database as an asset in bankruptcy.[18]

These matters all involved deception. The FTC felt it was unable to act in situations, however, where children's information was collected but no affirmative deception was present. Because of this gap, the Agency formally supported enactment of the Children's Online Privacy Protection Act to strengthen its basis for legal action.

THE CHILDREN'S ONLINE PRIVACY PROTECTION ACT OF 1998

Introduced by Senators Richard Bryan and John McCain as S. 2326 in July 1998,[19] Congress enacted the Children's Online Privacy Protection Act (COPPA) just months later, as a rider to an emergency appropriations bill.[20] Fulfilling an observation made by Professor Priscilla Regan, a privacy rationale (protecting children online) was sufficient to raise a public debate, but overcoming policy-maker inertia to enact legislation became possible only once online safety advocates joined the cause. The law thus had both privacy and online safety attributes.

In an introductory statement,[21] and later in committee testimony,[22] Senator Bryan identified the several concerns that animated the legislation:

- Websites collected personal financial and contact information about children, sometimes using cartoon characters and games to solicit the data.
- Websites could perform this collection without parental supervision or control.
- One could not identify the recipients of these data, and the solicitation of family members' financial data suggested less than above-board marketing.

[16] *In the Matter of GeoCities*, 127 F.T.C. 94 (February 5, 1999).
[17] *In the Matter of Liberty Fin. Companies, Inc.*, 128 F.T.C. 240 (1999).
[18] *FTC* v. *Toysmart.com*, 00–11341-RGS, 2000 WL 34016434 (D. Mass. July 21, 2000).
[19] Representative Edward Markey introduced companion legislation in the House that would also protect adults as 105 Cong. H.R. 4667, the Electronic Privacy Bill of Rights Act of 1998.
[20] Pub. L. 105–277, Div. C, Title XIII, §1302, October 21, 1998, 112 Stat. 2681–728. Codified at 15 U.S.C. §6501 et seq.
[21] 105 CONG. REC. S8482 (July 17, 1988).
[22] S. Hrg. 105–1069, 105 Cong. 2nd Sess. (September 23, 1988).

- Children can easily venture into inappropriate corners of the internet, attracting the attention of sexual predators and pedophiles.
- The internet is a spectacular tool for learning and for economic progress; children should not have to take the Hobson's choice of stopping internet use in order avoid commercial or sexual predation. This conundrum was highlighted in a hearing on COPPA, at which Bryan emphasized that the measure was pro-internet, adding: "proficiency with the Internet will be a necessary skill required to succeed in the 21st Century."[23]

According to Professor Deirdre Mulligan, early drafts of the legislation defined children as anyone under the age of eighteen. As introduced, the legislation applied to individuals under the age of sixteen. This was changed to under the age of thirteen in the final bill. Chairman Pitofsky argued against the extension of COPPA to teenagers, explaining that if it were applied, the parental consent requirement should be softened or dropped.[24]

The legislative history on COPPA is thin, and, as a result, COPPA is sometimes framed as a privacy law, sometimes as a measure to stop child predation, and sometimes as both. Additionally, there is no case law concerning COPPA, aside from consent decrees approved by district courts.

As Congress typically does in consumer law and other matters, it delegated the drafting of the actual regulations to the Commission. The rules were due by October 1999. The COPPA rule appears at 16 CFR §312 and it went into effect on April 21, 2000. The FTC was given Administrative Procedure Act rule-making power to promulgate the rule.[25] A rather uninspired 2007 report on the COPPA concluded that the law was working well and recommended no changes.[26] Just a few years later, however, the Commission promulgated major changes that became effective on July 1, 2013.[27]

Scope

At a high level, COPPA regulates the collection of personal information from children on websites or other online services. A "child" is an individual under the age of thirteen.

[23] S. Hrg. 105–1069, 105 Cong. 2nd Sess. (September 23, 1988).

[24] *Id.*

[25] As opposed to its default rule-making powers under the Magnuson–Moss Act, which are popularly considered too burdensome to use. See Chapter 2.

[26] FTC, Implementing the Children's Online Privacy Protection Act: A Report to Congress (February 2007).

[27] FTC, Children's Online Privacy Protection Rule, Final Rule Amendments, 78(12) Fed. Reg. 3972, January 17, 2013.

Websites and other services are broadly construed, and can include mobile and desktop applications;[28] plug-ins on websites that capture data for metrics, social networking, or advertising purposes; advertising networks; location-based services; and services with voice over IP. COPPA does not apply to noncommercial services.

To trigger the COPPA obligations, a website or service must be directed at children, or have actual knowledge that it has collected information from children. The FTC uses a "totality of the circumstances" test to determine whether a site is child oriented. Factors include the subject matter of the site, use of animated characters, characteristics of music, whether the site uses child models or child celebrities, the use of childish fonts, and audience composition. Most of the FTC's cases thus far involve sites that are obviously child oriented, such as fan club sites for teenage celebrities,[29] and social networking services that explicitly serve children.[30] However, in the FTC's 2014 case against TinyCo, it labeled fantasy apps child oriented because they featured "brightly-colored, animated characters from little animals or zoo creatures to tiny monsters, and ... involving subject matters such as a zoo, tree house, or resort inspired by a fairy tale."[31] TinyCo is the first COPPA case to rely so heavily on an app's appearance, and this may be problematic, as many general-audience apps have childish themes.

Actual knowledge of children on a site can occur in several ways, for instance, in coming across a comment posted by a user who self-identifies as a child. Several cases alleging actual knowledge concern services that had some age-screening mechanism that nonetheless allowed children to register.[32] In some situations, this appears just to be a technical error. For instance, Yelp.com excluded children from registering on its website, but its related app for cell phones would establish an account for a child.[33] Such technical mistakes do not prevent the FTC from finding a violation of the COPPA.

Actual knowledge issues can be a double whammy for companies: They both violate COPPA for registering children, but also violate the FTC Act because the companies have typically promised not to collect children's information at all.

[28] *US* v. *W3 Innovations, LLC*, CV-11–03958-PSG (N.D. Cal. 2011); *US* v. *Bonzi Software, Inc.*, CV-04–1048 RJK (C.D. Cal. 2004).

[29] *US* v. *UMG Recordings, Inc.*, CV-04–1050 JFW (C.D. Cal. 2004).

[30] *US* v. *Jones O. Godwin, doing business as skidekids.com*, 1:11-CV-3846 (JOF) (N.D. Ga. 2011)(promoted as the "Facebook and Myspace for kids.")

[31] *US* v. *TinyCo., Inc.*, 3:14-cv-04164 (N.D. Cal. 2014).

[32] *US* v. *Path, Inc.*, 3:13-cv-00448-RS (N.D. Cal. 2013); *US* v. *Artist Arena, LLC*, 112-cv-07386-JGK (S.D. N.Y. 2013); *US* v. *RockYou, Inc.*, 312-cv-01487-SI (N.D. Cal. 2012); (*US* v. *Iconix Brand Group, Inc.*, 09-CIV-8864 (S.D.N.Y. 2009); *US* v. *Sony BMG Music Entertainment*, 08 CV 10730 (LAK) (S.D.N. Y. 2008); *US* v. *Xanga.com, Inc.*, 06-CIV-6853 (SHS) (S.D. N.Y. 2006); *US* v. *UMG Recordings, Inc.*, CV-04–1050 JFW (C.D. Cal. 2004).

[33] *US* v. *Yelp Inc.*, 3:14-cv-04163 (N.D. Cal. 2014).

Sites that are directed at children cannot eliminate COPPA liability by simply declaring that those under thirteen should not register.[34]

The updated definition of collection of personal information in the rule was comprehensive and technology-neutral. Any type of persistent identifier tracking was covered – even when done passively – meaning that plug-ins and popular analytics and advertising services are subject to the rule. Information that allows contact with a child, such as usernames and identifiers for instant messaging, and other communications platforms, were considered personal information.

A SAMPLE OF MID-CENTURY CONSUMER PROTECTION REGULATIONS

It is difficult to imagine the scope of consumer hazards that have existed in the last century. For some time, a consumer shopping for shoes may have been presented with a fluoroscope (an x-ray machine) to ensure that the shoe fitted well.[35] Cars lacked seat belts. Sliding doors often lacked safety glass. Lawn mowers lacked automatic engine shutoff switches for the time when the operator lets go of the handle. Beginning in the 1950s, Congress enacted a number of statutes to address these hazards. Debates surrounding these issues rhyme with today's – To what extent can consumer education address these risks? What is the responsibility of the consumer to use products safely? Do structural interventions that prohibit certain technologies or mandate others, in order to protect consumers, inhibit innovation?

- In 1953, a rather edentulous Flammable Fabrics Act was enacted, with a stronger version passing in 1967 to address a rash of cases where children were seriously burned by flammable clothing.
- The 1956 Refrigerator Safety Act required refrigerators to have an internal latch opening mechanism (to prevent children from suffocating when trapped inside one).
- The 1960 Hazardous Substances Labeling Act required warnings on household chemicals.
- The 1962 National Traffic and Motor Vehicle Safety Act enabled the federal government to set safety standards for cars.
- The 1972 Consumer Product Safety Act established the Consumer Product Safety Commission, an independent agency tasked with protecting against unreasonable risks of injuries associated with consumer products.

[34] *US* v. *Bigmailbox.com*, 01–605-A (E.d. Va. 2001) (site declared, "You must be at least 13 years old or have your parent's permission to join this program.")

[35] *See* Paul Frame, Shoe-Fitting Fluoroscope (ca. 1930–1940) (2010).

As consumer protection rules diffuse, some dangerous products disappear from the market, and others are redesigned to be safer. If consumer protection law is successful, it cures problematic products and practices, and memories of dangerous products fade. As a result, consumer protection is at risk of being taken for granted.

Critics have argued that the FTC exceeded the bounds of Congressional intent by defining collection to include the passive tracking of third-party services. However, these broad definitions of services and of personal information mirror Congress' dual concerns of safety and child marketing. COPPA's main thrusts concern information that allows strangers to contact children, thus justifying inclusion of usernames, as well as marketing techniques that could have a manipulative effect on children. The Agency concluded that even if a website could not name a particular user, if it could track that user over time, it could manipulate the child in ways that Congress found objectionable.

The COPPA has extraterritorial application, and thus child-directed sites hosted overseas must comply, as must sites hosted in the United States that serve children in other countries.[36]

Protections

The COPPA has five major protections for services subject to the rule: first, services must post clear privacy notices that specifically identify all the parties receiving data from the service; second, services must obtain parental consent prior to collecting data from children; third, services must provide parents with the ability to review the information collected, to object to its further use, and to use the service without sharing data with third parties (if technically possible); fourth, services must limit the amount of data collected about children; and, finally, services must both limit the duration of data retention and reasonably secure data.

COPPA also requires services directed to children to vet vendors and third parties for compliance with these obligations. In this fashion, COPPA fills gaps that exist in other regimes, causing services to inspect third parties and creating incentives for vendors to make COPPA-compliant offerings. This requirement follows greater recent attention to vendors and services provider liability under other information privacy law, such as the Gramm–Leach–Bliley Act and the health privacy laws.

[36] 15 U.S.C. §6501(2); *US* v. *Playdom, Inc.*, SACV11-00724 (C.D. Cal. 2011) (defendant transferred accounts, including those of children, to a French company).

Notice

COPPA's notice requirements include a duty to provide a general privacy notice as well as special, direct notices to parents before the service collects information from children. Notices cannot contain "confusing or contradictory" materials, by which the FTC means that there should not be marketing or fluff in the policy that would distract the decision-maker.[37]

The general privacy notice has three main requirements: First, it must list the identities of all "operators" associated with the service. Second, it must include a description of the kinds of data the operator collects, uses, and discloses. It must also state whether children can make personal information publicly available through the service. Finally, it must state that the parent can review, have deleted, and refuse to allow further collection or use of personal information.

Direct notices have four types, corresponding to four basic models of child-oriented services: first, a notice for sites that will disclose children's personal information (for instance, a child-directed social network service); second, a notice for sites that intend to contact the child repeatedly; third, a notice for sites that collect data only to protect the child; and fourth, a notice for sites that only collect contact information of parents and no data about children (this is a voluntary notice).

Parental consent

In response to concerns that the internet allowed children to interact with marketers and others without parental supervision or control, COPPA imposed a parental consent requirement *before* a website can collect or use personal information of children. Under the Rule, the consent procedure must be "reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent."[38] Thus, neither Congress nor the FTC thought that parental consent mechanisms would be foolproof.[39]

At the same time, the FTC recognized that more interactive services would require more parental involvement. Thus, social networking services and other services that disclose personal information publicly or to third parties must comply with the strongest consent mechanism. Services that only use information for internal purposes have a lower consent burden. And television-like sites with no interactivity and no information sharing need not obtain consent at all.

[37] Privacy provisions that were both in a privacy policy and in an end-user license agreement did not "document clearly, understandably, and completely disclosed its information practices, as required by the Rule." *US* v. *Bonzi Software, Inc.*, CV-04–1048 RJK (C.D. Cal. 2004).

[38] 16 C.F.R. §312.5(b).

[39] S. Hrg. 105–1069, 105 Cong. 2nd Sess. (September 23, 1988). (Chairman Pitofsky testified, "As I said once before, the FTC has vast authority, but controlling the behavior of 11-year-olds, for example, calling themselves 13-year-olds is beyond our reach.")

It is useful to think of COPPA sites as falling into three tiers ordered in high to low compliance risk. For the first tier, services that make disclosures to third parties, employ behavioral advertising, or allow children to publicly post information must obtain verified parental consent. The FTC has specified five methods to obtain parental permission: a consent form returned by mail, fax, or scan; a credit card number when used with a payment; operating a toll-free number for the parent to call; having the parent contact the company through video conference; and verifying parent consent through collecting government-issued identification.

For the middle tier, where a service only uses child data for internal purposes, it may use "e-mail plus" to gain consent. With this method, the site sends the parent an e-mail, and the parent responds giving consent and providing some other information, such as a contact phone number. Use of personal information for appropriate internal purposes includes that necessary to run and secure the site, but may also include contextual advertising.

In the lowest-risk tier, a service could be directed to children and simply not collect personal information at all (other than a persistent identifier for internal operation purposes). Such zero-interactivity sites need not obtain parental consent. Finally, consent must be obtained again whenever the site makes some material change to its privacy policy.

Parental access

Consistent with the model of fair information practices (discussed in Chapter 6), parents can request a description of the specific types of personal information collected from their child and review the actual personal information collected.

The traditional concern about access concerns security: How can a service that only interacts with people online be certain that it is revealing personal information to the right parent? What if access requests are used to cause data breaches or identity theft? Here, sites must walk a tightrope: they have to create procedures that ensure the requestor is legitimate, but at the same time not create unreasonable burdens for the parent to authenticate identity.

Excessive information collection

Businesses must allow children access to their services without conditioning it on the child "disclosing more personal information than is reasonably necessary to participate in such activity."[40] This provision is based on the concerns raised by advocates and by COPPA's sponsors about eliciting personal information from children using games and the like. The Commission takes the limitation seriously and is appearing to interpret it such that any information collection that is not

[40] 16 C.F.R. §312.7.

necessary to deliver a service is prohibited. For instance, in a case involving a company that operated a "Kids Club" that included a chance to win prizes, the company's collection of name, address, e-mail address, and day and month of birth was considered excessive. The practice was deemed excessive in light of the fact that the company collected data on 500 children yet only awarded 12 prizes.[41] Presumably, the club could have operated with just e-mail address and collected home addresses from the prize winners only.

As part of the access right described above, parents can object to specific information collection or sharing, demand that a site delete data, and yet still ask that the child be allowed to use the service.[42] The service provider can terminate the user if the information use is critical to the service. However, sharing with "third parties" for the kinds of business purposes typical on websites is not "critical" under the COPPA. Thus, a service cannot terminate a user just because it cannot collect as much advertising revenue on a child who objects.

Security and deletion

COPPA requires that services have "reasonable procedures to protect the confidentiality, security, and integrity of information collected from children."[43] The service must also take "reasonable steps" to ensure that service providers and third parties have adequate security.

In addition, the rule imposes limits on how long data can be kept ("for only as long as reasonably necessary to fulfill the purpose for which the information was collected") and requires that it be deleted with "reasonable measures."[44] These provisions do not apply to data collected offline.

Only one commission case has dealt with deletion requirements. In it, a child-oriented social networking site tried to comply with the consent requirement by allowing children to create a profile but keeping it private until a parent approved the creation of the account. However, the site failed to delete information when the parent refused (or never got around to) approving the account.[45] This was found to violate the COPPA.

[41] *US* v. *American Pop Corn Company*, C02-4008DEO (N.D. Iowa 2002). See also the "Girl's Life" case, where the FTC describes seven different website activities and follows the description with a blanket statement that the personal information collection was excessive. *US* v. *Monarch Services, Inc., et al.*, AMD 01 CV 1165 (D. Md. 2001).

[42] 16 C.F.R. §312.5(a)(2). ("An operator must give the parent the option to consent to the collection and use of the child's personal information without consenting to disclosure of his or her personal information to third parties.")

[43] 16 C.F.R. §312.8.

[44] 16 C.F.R. §312.10.

[45] *US* v. *Industrious Kid, Inc.*, CV-08–0639 (N.D. Cal. 2008).

Enforcement

There is no private right of action in COPPA. Actions can be brought by states, by the FTC, and by the regulators of specific industries (for instance, the financial regulators, the Department of Transportation, and even the Department of Agriculture have authority to enforce COPPA against companies they regulate).

The Children's Advertising Review Unit (CARU), a well-regarded self-regulatory organization, referred a number of COPPA actions to the FTC.

The FTC's internal matter tracking system classifies COPPA violations into six categories: first, where there is no privacy policy or where it is incomplete or not prominent; second, where the site misrepresents how data are used; third, where the site had no procedures for parental consent; fourth, where the parent is not given the opportunity to refuse consent to sharing of data to a third party; fifth, where the parent cannot see the child's information or where information is not deleted as requested; and, finally, where the service collects more information than necessary for an activity.

COPPA enforcement has generally concerned obvious violations of the rule, such as failing to post compliant privacy policies or failing to obtain verifiable parental consent. These cases have been uncontroversial as evidenced by unanimous commission votes to bring them. All COPPA cases have been brought in federal district court, rather than as administrative proceedings, signaling the Agency's confidence in its enforcement choices.

The FTC's first cases in any area tend to be conciliatory warnings to industry that become more punitive with time. From its first COPPA cases, the Agency included civil penalties and requirements that the sites delete the data they collected since the effective date of the COPPA rule.[46] These civil penalties averaged $30,000 in 2001 and 2002. In 2003, the FTC secured a $100,000 penalty in a settlement.[47] By 2004, it secured a $400,000 settlement against UMG Recordings.[48] The Agency's 2006 case and settlement against Xanga extracted a $1,000,000 penalty.[49] That company allowed over 1 million accounts to be created to users who indicated that they were under 13 and created profiles for them on the service. A 2011 case levied a $3,000,000 penalty.[50]

High penalties are applied in cases involving large numbers of children, where the service allowed children to post personal information, and where the

[46] See *US* v. *Ohio Art Company*, FTC File No. 022-3028 (N.D. Ohio 2002); *US* v. *American Pop Corn Company*, C02-4008DEO (N.D. Iowa 2002); *US* v. *Lisa Frank, Inc.*, 01-1516-A (E.D. Va. 2001); *US* v. *Monarch Services, Inc., et al.*, AMD 01 CV 1165 (D. Md. 2001); *US* v. *Looksmart Ltd.*, 01-606-A (E.D. Va. 2001); *US* v. *Bigmailbox.com*, 01-605-A (E.d. Va. 2001).

[47] *US* v. *Mrs. Fields Famous Brands, Inc.*, 203 CV205 JTG (D. Utah 2003) ($100,000); *US* v. *Hershey Foods Corporation*, 4CV-03–350 (M.D. Pa. 2003) ($85,000).

[48] *US* v. *UMG Recordings, Inc.*, CV-04-1050 JFW (C.D. Cal. 2004).

[49] *US* v. *Xanga.com, Inc.*, 06-CIV-6853(SHS) (S.D. N.Y. 2006).

[50] *US* v. *Playdom, Inc.*, SACV11-00724 (C.D. Cal. 2011).

service collected information aggressively or excessively (GPS information, user address books).

Starting with the suit against Xanga, the FTC started naming company principals as defendants in COPPA suits. This is because those who own or control data are considered "operators" under COPPA and thus are jointly liable. By policy, the FTC has stated it will only name principals where they participate in, facilitate, or know of COPPA rule violations. Given that CARU cajoles companies to comply with COPPA first and then refers cases to the FTC, there can be ample evidence of knowing violation of the rule.

The FTC has not brought enforcement actions using the more recent changes to the COPPA rule that went into effect on July 1, 2013. However, the Agency has sent out scores of letters to mobile application developers and others, reminding them of the new definitions of the rule. One prominently announced letter was directed to a China-based app developer that was collecting precise GPS information from children and sharing the information with advertisers.[51] The letter caused Google to temporarily suspend the company's apps from its application marketplace.

COPPA safe harbor

COPPA allows companies to apply and be certified as a "safe harbor" program. Services that meet the safe harbor's requirements are deemed compliant with COPPA.

In essence, COPPA safe harbor programs are self-regulatory bodies. However, because they must meet certain requirements and are overseen by the Commission, they do not suffer from the pathologies present in pure self-regulatory regimes (see discussion of self-regulation in Chapter 6).[52] Additionally, before passage of COPPA, the major trade groups had expressed some support for child privacy protections.[53] Thus, all participants could at least agree that the principle of protecting children was important. This consensus has made the COPPA self-regulatory effort more credible and more likely to achieve buy-in from participants.

COPPA safe harbor programs must have stated requirements for services that are at least as stringent as the COPPA rule. Safe harbor programs must assess services' compliance annually, and take disciplinary action for noncompliance with the requirements. The Commission reviews COPPA safe harbor programs. The review includes an opportunity for the public to comment, and programs must be given a

[51] Letter from Maneesha Mithal, Associate Director, Division of Privacy and Identity Protection, FTC, to BabyBus, December 17, 2014.

[52] See Ira S. Rubinstein, *Privacy and Regulatory Innovation: Moving beyond Voluntary Codes*, 6 I/S J. L. Pol. 355 (2011).

[53] S. Hrg. 105–1069, 105 Cong. 2nd Sess. (September 23, 1988) (testimony of Jull A. Lesser, Director, Law and Public Policy, America Online, Inc.).

determination within 6 months of application. The FTC has approved a handful of programs.

COPPA AS A PRIVACY MEASURE

COPPA is widely criticized as a privacy measure. Its limitation to children below the age of thirteen, the burden of parental consent, its effects on anonymity, and how it balances parental versus website responsibility have attracted the most critique.

Yet, a more fundamental problem comes from what COPPA did to children's websites. Some advocates for children's privacy wanted a kind of PBS-like experience for children online. In particular, advocates were concerned about a blending of advertising and content. Others argued from a different viewpoint that the incentives created by COPPA risked turning child-directed sites into television-like, one-way media programs.

Yet, COPPA-compliant sites are probably worse than TV and even Saturday morning cartoon TV – they are fully immersive shopping experiences. For instance, one of the most popular COPPA sites allows children to customize a seabird with clothes and other accessories, such as a pet. The site seems entirely focused on training children to shop at a mall, and the seabirds, once decorated, have a Kardashianesque quality.

Why thirteen?

As introduced, COPPA would have required parental consent until the age of sixteen. In fact, the high level of parental control over teens' internet use made the bill attractive to conservative groups, which saw COPPA and companion antipornography legislation, the Child Online Protection Act,[54] as levers to stop access to smut as well as other materials, such as information about sexual and reproductive health and abortion. Viewed in this light, parental consent becomes a tool to control children. Free speech advocates quickly realized this possibility and saw COPPA as detrimental to adolescents' freedom. They strongly opposed any precedent that created parental content requirements, for fear that they may spread into other contexts, such as learning about evolution or controversial literature.

[54] Creating fines and misdemeanor punishments for "[w]hoever knowingly and with knowledge of the character of the material, in interstate or foreign commerce by means of the World Wide Web, makes any communication for commercial purposes that is available to any minor and that includes any material that is harmful to minors ..." Pub. L. 105–277, 112 Stat. 2681–736. This law was invalidated on free speech grounds in *Am. Civil Liberties Union* v. *Mukasey*, 534 F.3d 181 (3d Cir. 2008).

CHAIRMAN PERTSCHUK'S LESSONS ON REGULATION

Chairman Michael Pertschuk was one of the most qualified FTC leaders ever. Educated at Yale Law School, he clerked for a federal district judge, practiced at a firm, and then spent fifteen years on Capitol Hill. His Hill experience brought him great expertise in consumer protection, as he was chief counsel to the Senate Commerce Committee during the expansion of consumer rights in the 1970s.

Pertschuk led the FTC during its most controversial years (see Chapter 2). In his 1982 book, *Revolt against Regulation*, he gave a personal account of lessons learned from the newfound skepticism of government regulation.[55] He offered consumer advocates seven lessons in consumer regulation. They should ask:

- Is the rule consonant with market incentives to the maximum extent feasible?
- Will the remedy work?
- Will the chosen remedy minimize the cost burdens of compliance, consistent with achieving the objective?
- Will the benefits flowing from the rule to consumer or to competition substantially exceed the costs?
- Will the rule or remedy adversely affect competition?
- Does the regulation preserve freedom of informed individual choice to the maximum extent consistent with consumer welfare?
- To what extent is the problem appropriate for federal intervention and amendable to a centrally administered national standard?

Pertschuk's book is an anomaly for Washington memoirs, which typically involve some trope about "reforming Washington," with failures attributed to intractable "bureaucracies" and the like. Pertschuk wrestles with questions fundamental to whether consumer protection is effective, and declares that his experience taught him the (albeit limited) value of cost–benefit analysis.

Young adolescents experiment with intimacy. As Professor Sherry Turkle observed, some adolescents explore sexuality online, which could be a safer venue because there is no in-person contact.[56] Adolescents seek seclusion for such activities, but COPPA does not allow any secrecy from the parent. Designed as both privacy and online safety measure, COPPA does not recognize the parent as a potential invader of privacy.

[55] Michael Pertschuk, Revolt against Regulation (1982).
[56] Sherry Turkle, Life on the Screen (1995).

A teenager who seeks advice from an emergency online hotline for depression, such as a chat or instant messaging service, would have to undergo a delay in obtaining parental consent under COPPA. In addition, the parent could use the COPPA access rights to learn about how the child interacted with the service. Civil libertarians pointed out that children need privacy protections online, but they also need some level of privacy from their parental intrusiveness as well.[57]

Still, the civil libertarians' critique may be misplaced. This is because COPPA only covers commercial services. In most circumstances, a nonprofit can safely collect personal information from children and simply not be subject to COPPA,[58] or it could design its site so that it does not collect personal information and yet provides information about sexual health, depression, or abortion services.

The bimodal compliance problem

To avoid the various duties imposed by COPPA, particularly the parental consent requirement, many services simply prohibit children from using them.[59] Congress did not provide any middle ground for compromise on parental consent. The Commission's tolerance for "e-mail plus," which allows for internal uses of personal information but not commercial ones, seems to be waning. Thus, sites tend to fully embrace COPPA, or pretend that children never visit their service.

COPPA applies to a very wide variety of services, including those that have nothing to do with social networking or otherwise posting personal information online. Thus, it prohibits offering e-mail or instant messaging services to children, tools that many families use to stay in touch.

This limitation is unfortunate for several reasons. First, parents may tell children to lie at enrollment about their age so that they can use the service.[60] Second, even without parental encouragement, children may lie because highly interactive services are so attractive. In addition to creating rewards for lying, these children are then as unprotected as adults online, sometimes with disastrous results. Consider the mobile flirting app Skout – it created a protected service for thirteen- to seventeen-year-olds and, despite its efforts, three children were attacked by older adults who were posing as teens.[61] *Consumer Reports* magazine estimated that "Of

[57] Bryce Clayton Newell, Cheryl Metoyer, & Adam D. Moore, Privacy in the Family, The Social Dimensions of Privacy (Beate Roessler & Dorota Mokrosinska, eds., 2015); Benjamin Shmueli & Ayelet Blecher-Prigat, *Privacy for Children*, 42 Colum. Hum. Rts. L. Rev. 759 (2011).

[58] An exception would be where the nonprofit was functionally operating as a for-profit (*see* Chapter 4 and *FTC* v. *California Dental Association*, 526 US 756 (1999)).

[59] Jules Polonetsky & Omer Tene, *Who Is Reading Whom Now: Privacy in Education from Books to MOOCs*, *Van. J. Ent. Tech. L.* (2014).

[60] Danah Boyd, Urs Gasser, & John Palfrey, *How the COPPA, as Implemented, Is Misinterpreted by the Public: A Research Perspective*, Berkman Center Research Pub. 2010-12 (April 29, 2010).

[61] Nicole Perlroth, *After Rapes Involving Children, Skout, a Flirting App, Bans Minors*, N.Y. *Times*, Jun 12, 2012.

the 20 million minors who actively used Facebook in the past year, 7.5 million – or more than one-third – were younger than 13 and not supposed to be able to use the site."[62]

Parental consent is both a burden for services and for parents, and it is ineffective, because consent does little to protect privacy or safety. For instance, parental consent would not have protected the older adolescents who used the Skout app from adults posing as children. In a way, COPPA might be more effective if efforts devoted to verifying parental consent were focused instead on keeping adults out of adolescent-oriented services. The social networking service Facebook realized this and has deployed extensive systems to flag suspicious activity. For instance, Facebook might flag an older man who is contacting several teenagers, because this could signal incipient child predation.[63]

COPPA's most efficacious protections come from limits on data collection and limits on commercial uses of data. While advertising is the often-invoked privacy interest, the bigger issue is the assemblage of profiles on children. Other protections, such as incentives for contextual rather than behavioral advertising, and requirements to delete data can reduce the profiling of children. Children might have much more actual privacy if all sites providing services to those under 18 had these duties and consent was reserved only for the minors using services that post profiles for others to see.

Parental consent and anonymity

Privacy and free speech advocates have expressed concern that mechanisms for verifiable parental consent implicitly identify website users, and that this identity is very reliable. As consent mechanisms spread, identity will be hardened and well authenticated across the Web. These anonymous Web arguments had some validity back in 1999, but today users are much more identifiable by web services, because of the rise of behavioral advertising. Services such as Facebook and Google have a very large number of authenticated users, and can easily identify these users and then track them ubiquitously on the Web through their advertising delivery and metrics systems, even when these users are not logged into Facebook or Google.[64] Age verification may have a corrosive effect on anonymity, but other threats to anonymity have far surpassed the COPPA.

[62] Consumer Reports Mag., That Facebook Friend Might Be 10 Years Old, and Other Troubling News (n.d. 2011).

[63] Joseph Menn, *Social Networks Scan for Sexual Predators, with Uneven Results*, Reuters (July 12, 2012).

[64] For instance, a user who signs into a real-name-required service such as Facebook can be comprehensively tracked on the Web, in an identifiable manner, on any website with a Facebook "Like" button.

The role of the parent and the state

As discussed in Chapter 2, the FTC caused widespread anger when it proposed to regulate television advertising to children. COPPA has raised some of the same concerns about government regulating family matters. Particularly in the Washington DC libertarian community, critics have pointed to the need for parental responsibility, the need for consumer education, and targeted enforcement as alternatives to COPPA. More generally, critics call for cost–benefit analyses of COPPA.

There are several problems with this nanny-state critique of the FTC. First, most parents probably welcome (or could use) help in policing children's internet use. Like television before it, internet-connected devices are often convenient babysitters, yet the internet is worse than TV because it presents a different, unpredictable risk landscape.

Some analysts cavalierly dismiss risks of child predation from online interactions. In fact, the best research suggests that such incidents are exceedingly rare.[65] The problem is that even if these incidents are rare, anecdotes about child predation are extremely powerful in the policy setting. Child safety advocates know that predators are resourceful, motivated, and even organized in their victimization of children.[66] Parents cannot supervise every moment of their children's lives: protections such as COPPA can help reduce the risk that children get into trouble online.

Second, the leave-it-to-parents and the market argument ignores the pre-COPPA history. The Center for Media Education report in 1996 illustrated that manipulative techniques were used not just by marginal actors, but that they were widespread even among reputable businesses. Advertisements of the good old days were anything but good for children.

Finally, cost–benefit analysis is often employed to argue that COPPA imposes excessive costs, and a system of user empowerment and education is more cost-effective. But how much does such empowerment and education cost? Calls for cost–benefit analysis of COPPA do not calculate these expenses, and so they are not particularly rigorous, no matter how much the term is repeated and promulgated by their advocates.

Advocates for cost–benefit analysis frame the issue improperly – counting costs that services incur in compliance, and ignoring the transaction costs and impossible burdens that a world without COPPA would impose upon parents. A world without COPPA would shift the burden of ensuring adequate privacy and security onto parents, who would have to read policy after policy to protect their

[65] DANAH BOYD, IT'S COMPLICATED: THE SOCIAL LIVES OF NETWORKED TEENS (2014).

[66] Consider *US* v. *Paul*, 274 F.3d 155 (5th Cir. 2001): "According to the government, Paul also used his e-mail to advise fellow consumers of child pornography how to 'scout' single, dysfunctional parents and gain access to their children and to solicit the participation of like-minded individuals in trips to 'visit' children in Mexico."

children.[67] There is little reason to believe that even such activity would promote privacy. Parents would have no ability to vet the activities of vendors and service providers on any given site.[68]

The argument that user education is a less costly alternative to a regulatory regime has not been verified. Education costs money: in fact, good education is expensive. Yet, these costs are never calculated by those putting forth cost–benefit critiques of COPPA.

Furthermore, education is imperfect. Education has many pitfalls. Education is often not delivered, or delivered poorly. When education fails, the user bears all the risk and the blame for making a bad privacy choice.

Thus, a proper cost–benefit analysis would view COPPA as transferring of cost from millions of parents, who are responsible for vetting different services, to the services themselves that propose to profit from using child data. These services are in a much better position to investigate and police their own activities and the actions of their vendors than parents. In other words, COPPA internalizes these costs to service providers.

Educational technology companies and COPPA

Schools across the nation, both public and private, have adopted "cloud-based" services to enhance productivity and to enable students to interact with their teachers online. Yet, the very purpose of many cloud-based services is to advertise, to create profiles of individuals, and to scan the content they produce. These purposes do not nicely align with the horizon-expanding, liberal purposes of education.

These services have to comply with both the COPPA and the Federal Educational Rights and Privacy Act of 1974, among other laws.[69] To address the COPPA consent issue, the FTC allows schools to give consent on behalf of the parent. However, school-based consent only allows the company to use information for its internal purposes, and for school purposes. It cannot employ the data for some commercial purpose, including behavioral advertising or building commercial profiles on users, without gaining verified parental consent.[70]

[67] Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S J. L. Pol'y Info. Soc'y 543, 564 (2008); George R. Milne, Mary J. Culnan, & Henry Greene, *A Longitudinal Assessment of Online Privacy Notice Readability*, 25 J. Pub. Pol'y Marketing 238, 243 (2006) (based on the growing length and complexity of privacy policies, a user would have to read eight pages of text per competitor to evaluate their privacy choices).

[68] *See generally* James P. Nehf, *Shopping for Privacy on the Internet*, 41 J. Consumer Aff. 351 (2007).

[69] Jules Polonetsky & Omer Tene, *Who Is Reading Whom Now: Privacy in Education from Books to MOOCs*, Vand. J. Ent. Tech. L. (2014).

[70] California law explicitly prohibits amassing profiles on students through educational technologies. See Cal. Bus. & Prof. Code §22584.

A 2013 report by Fordham University's Center on Law and Information Policy found widespread noncompliance with the COPPA among schools employing cloud-based services.[71] That report, the implosion of a well-funded school data management system (InBloom) over privacy issues,[72] and growing interest in the educational technology market led the Future of Privacy Forum to develop a Student Privacy Pledge in October 2014. Just months later, President Obama endorsed the Pledge, along with over 200 leading companies in education technology. The Student Privacy Pledge has significant pro-privacy commitments, such as promises to never sell student data, to not use behavioral advertising, to limit retention of data, and to limit the purposes for which data are collected.[73] It will complement COPPA by causing much of the education technology industry to make promises that can be policed under Section 5.

Missed research opportunities

The COPPA rule is now fifteen years old. Because it imposes so many requirements on websites, COPPA created a natural test bed for the performance of privacy laws. Yet, the academic literature on COPPA is as thin as its legislative history. This is a missed opportunity, as comparative studies of non-COPPA versus COPPA sights could yield insight into the efficacy of privacy law.[74] What is known about COPPA is that there appear to be many child-directed sites that are not in compliance with it. A 2015 sweep by the Global Privacy Enforcement Network found that only 31 percent of child-directed websites had "protective controls to limit collection of personal info" and 41 percent had policies that "left sweepers feeling uncomfortable."[75] A report released the same day on child-directed mobile applications found that 46 percent "had privacy policies that could be viewed from a direct link on the app store page."[76]

CONCLUSION

Privacy advocates might view children's privacy as a wedge that could drive adoption of privacy regulation for older internet users, but this is unlikely, because COPPA

[71] Joel Reidenberg, N. Cameron, Jordon Kovnot, Thomas B. Norton, Ryan Cloutier, & Daniela Alvarado, *Privacy and Cloud Computing in Public Schools*, Center on Law and Information Policy (2013).

[72] Jules Polonetsky & Omer Tene, *The Ethics of Student Privacy: Building Trust for Ed Tech*, 21 Int'l Rev. Info. Ethics 25 (July 2014).

[73] Future of Privacy Forum, K–12 School Service Provider Pledge to Safeguard Student Privacy (2014).

[74] One early, and apparently one-time, study was performed by the Annenberg Public Policy Center. Joseph Turow, Annenberg Public Policy Center, Privacy Policies on Children's Websites: Do They Play by the Rules? (2000).

[75] Global Privacy Enforcement Network, Results of the 2015 Global Privacy Enforcement Network Sweep (2015).

[76] Kristin Cohen & Christina Yeung, *Kids' Apps Disclosures Revisited* (2015).

is seen as too burdensome by service operators. Services tend to comply with the law by fully embracing child-directed status, or by attempting to ban children from services. This trains children to lie about their age in order to use highly attractive, interactive services, and leaves them protected in the same way adults are online.

COPPA's genesis as part privacy measure, part security measure drove Congress and later the FTC to create a rule that attempts to perfect children's online experience. But this is not possible. There will always be risks to children because of the persistence and guile of child predators.

Counterintuitively, the risk to children could be reduced with a *weaker* COPPA. The real privacy protection in COPPA comes from its non-consent-related provisions, such as limits on data collection, use, and retention. The responsibility of services to examine vendors and third parties for their practices and security protects privacy much more than a regime where consumers must guess about protections based on privacy policies.

Less attention to perfecting parental consent – or no parental consent at all – could result in a savings that makes COPPA's other sensible provisions in reach of sites that serve young adults. Unfortunately, however, the FTC seems to be moving toward tightening parental consent requirements. Perhaps this is because the FTC finds it easier to police consent mechanisms, which its staff can evaluate through testing, than more nuanced data issues such as how long data are retained.

In *Federal Trade Commission Privacy Law and Policy,* Chris Jay Hoofnagle explains how the FTC arrived at its current position as the most important regulator of information privacy in the world.

"The definitive book about the FTC's involvement in privacy and security."
Daniel J. Solove, John Marshall Harlan Research Professor of Law, George Washington University Law School

"A timely and insightful analysis of the FTC."
Priscilla M. Regan, Professor of Government and Politics, George Mason University

"A welcome perspective on challenges facing a great agency."
Norman I. Silber, Professor of Law, Maurice A. Deane School of Law, Hofstra University

"A landmark work."
Paul M. Schwartz, Jefferson E. Peyser Professor of Law, UC Berkeley Law

"Incisive and informative."
Astra Taylor, author of The People's Platform

"Clear, thoughtful and engaging."
Kirstin Downey, Editor, FTC:WATCH

"A fascinating, informed exploration."
William L. Wilkie, Ph.D., Aloysius and Eleanor Nathe Professor of Marketing Strategy, University of Notre Dame

Chris Jay Hoofnagle is adjunct full professor of information, University of California, Berkeley, faculty director of the Berkeley Center for Law & Technology, of counsel to Gunderson Dettmer LLP, and a member of the American Law Institute.

CAMBRIDGE
UNIVERSITY PRESS
www.cambridge.org

ISBN 978-1-107-56563-0