No. 11-32
August 2011

WORKING PAPER

KIDS, PRIVACY, FREE SPEECH & THE INTERNET: FINDING THE RIGHT BALANCE

By Adam Thierer

MERCATUS CENTER
George Mason University

INTRODUCTION

In the field of Internet policy, 2011 has been the year of privacy. Congress has introduced six bills related to online privacy,[1] and the Obama administration released two major reports recommending greater federal oversight of online markets.[2] The Federal Trade Commission (FTC) appears poised to step up regulatory activity on this front.[3] State-level activity is also percolating, led by California, which floated two major bills recently.[4]

These efforts would expand regulatory oversight of online activities in various ways. Some measures would institute "Fair Information Practice Principles" (FIPPS), governing the collection and use of personal information online.[5] Others would limit some types of data collection, ban certain data or advertising practices, or create new mechanisms to help consumers block online ad-targeting techniques. Another measure would mandate websites adopt a so-called Internet "Eraser Button," which would allow users to purge unwanted personal information from online sites and services.

Concerns about children's privacy are an important part of this debate. The Children's Online Privacy Protection Act of 1998 (COPPA) already mandates certain online-privacy protections for children under the age of 13. The goal of COPPA was to enhance parents' involvement in their children's online activities and better safeguard kids' personal information online. The FTC is currently considering an expansion of COPPA,[6] and lawmakers in the House of Representatives introduced legislation that would expand COPPA and apply additional FIPPS regulations to teenagers.[7] Some state-based measures also propose expanding COPPA.[8]

---

[1] Kate Kaye, "Privacy Bills: Which One Would Ad Industry Choose?" *ClickZ*, May 18, 2011, http://www.clickz.com/clickz/news/2072092/privacy-bills-industry-choose; Tim Lisko, "112th Privacy Legislation," *Privacy Wonk*, June 14, 2011, http://www.privacywonk.net/2011/06/112th-privacy-legislation.php.

[2] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change*, Federal Trade Commission Staff Report, December 2010, http://www.ftc.gov/os/2010/12/101201privacyreport.pdf; U.S. Department of Commerce, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*, U.S. Department of Commerce Internet Policy Task Force, December 2010.

[3] Emily Steel, "FTC Plans New Online-ad Rules," *Wall Street Journal*, May 27, 2011, http://blogs.wsj.com/digits/2011/05/27/ftc-plans-new-online-ad-rules.

[4] Adam Thierer, "The State of California versus the Internet," *Forbes.com*, May 22, 2011, http://blogs.forbes.com/adamthierer/2011/05/22/the-state-of-california-versus-the-internet.

[5] Federal Trade Commission, "Fair Information Practice Principles," http://www.ftc.gov/reports/privacy3/fairinfo.shtm.

[6] Berin Szoka, "FTC Announces Broad COPPA Review for Children's Online Privacy," *Technology Liberation Front*, March 24, 2010, http://techliberation.com/2010/03/24/ftc-announces-broad-coppa-review-for-childrens-online-privacy.

[7] Office of Rep. Ed Markey, "Markey, Barton Introduce Bipartisan 'Do Not Track' Kids Online Privacy Legislation," press release, May 13, 2011, http://markey.house.gov/index.php?option=content&task=view&id=4353&Itemid=125.

[8] Berin Szoka and Adam Thierer, "COPPA 2.0: The New Battle over Privacy, Age Verification, Online Safety & Free Speech," *Progress on Point* 16, no.11 (Washington, DC: The Progress & Freedom Foundation, 2009), 4-5 http://www.pff.org/issues-pubs/pops/2009/pop16.11-COPPA-and-age-verification.pdf.

While well-intentioned, efforts to expand privacy regulation along these lines would cause a number of unintended consequences of both a legal and economic nature. In particular, expanding COPPA raises thorny issues about online free speech and anonymity.[9] Ironically, it might also require that *more* information about individuals be collected to enforce the law's parental-consent provisions. There are better ways to protect the privacy of children online than imposing burdensome new regulatory mandates on the Internet and online consumers. Education, empowerment, and targeted enforcement of unfair and deceptive practices represent the better way forward.

THE COPPA REGIME

COPPA is a complicated and somewhat open-ended law and regulatory regime. COPPA requires that commercial operators of websites and services obtain "verifiable parental consent" before collecting, disclosing, or using "personal information" (name, contact information) of children under the age of 13 if either their website or service (or "portion thereof") is "directed at children" or they have actual knowledge that they are collecting personal information from a child.

Congress delegated broad authority to the FTC to devise and enforce the COPPA rule. The FTC adopted a "sliding scale" approach to obtaining parental consent.[10] This approach allows sites that might collect personal information to use a mix of methods to comply with the law, including print-and-fax forms, follow-up phone calls and e-mails, credit card authorizations, and the use of encryption certificates. The FTC has also authorized four "safe harbor" programs operated by private companies that help website operators comply with COPPA.

COPPA EXPANSION & THE "DO NOT TRACK KIDS" ACT

In recent years, some states have proposed expanding the COPPA regime in various ways.[11] These efforts would expand the COPPA parental-consent framework to include all minors up to the age of 18, broadening the range of sites covered, increasing the amount of information required to be collected to achieve "verifiable parental consent," or some combination of these. None of these reforms have been implemented yet.

A variety of concerns about what websites minors can visit and how much information those minors are placing online drive the concerns behind these bills. A recent survey by *Consumer Reports* estimated that as many as 7.5 million Facebook users are under the age of 13 and two-thirds of those are under the age of 10.[12] Like most other major online operators, Facebook does not allow users under the age of 13 to sign up for service. In practice, however, it is

[9] Szoka and Thierer, "COPPA 2.0: The New Battle over Privacy, Age Verification, Online Safety & Free Speech."
[10] Federal Trade Commission, *How to Comply with The Children's Online Privacy Protection Rule*, November 1999, www.ftc.gov/bcp/edu/pubs/business/idtheft/bus45.shtm.
[11] For a summary of some of these measures, see Szoka and Thierer, "COPPA 2.0."
[12] Tony Bradley, "Kids Under 13 Are Already Allowed on Facebook," *PC World*, May 21, 2011, http://www.pcworld.com/article/228348/kids_under_13_are_already_allowed_on_facebook.html#tk.mod_rel.

difficult to enforce such a restriction. This is one of the factors leading policy makers and regulatory advocates to push for expanding COPPA and other kids' privacy rules.[13]

This year, lawmakers in the State of California introduced SB 242—"The Social Networking Privacy Act"—which aims to make social networking sites private by default. It would also force sites to take down personal information upon request of users or parents of users under the age of 18 years. The bill stalled in the California Senate in late May, but it could serve as a model for other states in coming months.[14]

At the federal level, Reps. Edward Markey (D-Mass.) and Joe Barton (R-Texas) recently released the "Do Not Track Kids Act of 2011." The proposal would expand COPPA and adopt several other new regulations in an attempt to help safeguard kids' privacy online. It would apply FIPPS regulations to teenagers via a "Digital Marketing Bill of Rights for Teens" and also impose limits on collection of geolocation information from both children and teens. The bill would also mandate sites create "Eraser Buttons," a concept modeled loosely on a similar idea being considered in the European Union, a so-called "right to be forgotten" online. Specifically, the bill would require online operators "to the extent technologically feasible, to implement mechanisms that permit users of the website, service, or application of the operator to erase or otherwise eliminate content that is publicly available through the website, service, or application and contains or displays personal information of children or minors." In essence, eraser buttons would help minors wipe out embarrassing facts they have placed online but later come to regret.[15]

PROBLEMS WITH COPPA AND ITS EXPANSION

The influential child safety group Common Sense Media (CSM) floated some of the regulatory proposals discussed above in a report released December 2010.[16] It is understandable why some policymakers and child-safety advocates like CSM would favor such steps. They fear that there is too much information about kids online today or that kids are voluntarily placing far too much personal information online that could come back to haunt them in the future.

These are valid concerns, but there are both practical and principled concerns with the regulatory approach embodied in the Markey-Barton "Do Not Track Kids Act" and COPPA expansion efforts. In the name of protecting privacy, expanding regulation might actually undermine it.

---

[13] Cecilia Kang, "Lawmakers, Advocates Push Social Networks for More Protection of Youngest Users," *Washington Post*, June 10, 2011, http://www.washingtonpost.com/business/technology/lawmakers-advocates push-social-networks-for-more-protection-of-youngest-users/2011/05/27/AG7ByiOH_story.html.

[14] Patrick McGreevy, "Online Privacy Bill Fails to Pass California Senate," *Los Angeles Times*, May 28, 2011, http://www.latimes.com/news/local/la-me-social-networking-20110528,0,5345331.story.

[15] Larry Downes, "Europe Reimagines Orwell's Memory Hole," *Technology Liberation Front*, November 16, 2010, http://techliberation.com/2010/11/16/europe-reimagines-orwells-memory-hole.

[16] *Protecting Our Kids' Privacy in a Digital World* (San Francisco, CA : Common Sense Media, December 2, 2010), http://www.commonsensemedia.org/about-us/press-room/press-releases/privacy-agenda-kids-teens.

A. COPPA Isn't What It Says It Is

As written, COPPA is not the clearest of rules. First, all the terms in the COPPA law and rule are open to interpretation and challenged by ongoing technological change. Furthermore, even the FTC has its doubts about the effectiveness of COPPA. The FTC claims COPPA "has provided a workable system to help protect the online safety and privacy of the Internet's youngest visitors"[17] but also notes that "age verification technologies have not kept pace with other developments, and are not currently available as a substitute for other screening mechanisms."[18] This makes it clear that the FTC does not regard the methods it has adopted for obtaining parental consent under COPPA as the equivalent of strict age verification.

The FTC understands that no age-verification technology is foolproof. Even credit cards, the most common method used to verify parental consent, cannot always be trusted to verify a parent-child relationship. Although credit cards may seem the most robust tool for verifying parental consent—essentially, age verifying the parent—federal courts have found, in rejecting the constitutionality of the Child Online Protection Act (COPA) that, "payment cards cannot be used to verify age because minors under 17 have access to credit cards, debit cards, and reloadable prepaid cards." Moreover, although "payment-card issuers usually will not issue credit and debit cards directly to minors without their parent's consent because of the financial risks associated with minors…there are many other ways in which a minor may obtain and use payment cards."[19]

B. Threat of Mandatory Age Verification for All Users

First, it is unclear how an expanded COPPA regulatory regime would work without requiring mandatory online age verification of *all* Internet users, which would raise serious constitutional issues. To verify the relationship between a parent and a minor when a take-down request is received, a more sophisticated identity-authentication scheme is required. A previous effort to age-verify users, the Child Online Protection Act (COPA), was found to violate the First Amendment and also to raise different privacy concerns.[20] Federal courts found that there is "no evidence of age-verification services or products available on the market to owners of websites that actually reliably establish or verify the age of Internet users. Nor is there evidence of such services or products that can effectively prevent access to web pages by a minor."[21] In January 2009, after a decade-long court battle over the constitutionality of COPA, the U.S.

---

[17] Federal Trade Commission, *Implementing the Children's Online Privacy Protection Act: A Report to Congress*, February 2007, 28, www.ftc.gov/reports/coppa/07COPPA_Report_to_Congress.pdf.

[18] Ibid., 12.

[19] *Gonzales*, 478 F. Supp. 2d at 801. COPA would have prohibited the online dissemination of material deemed harmful to minors under the age of 17 for commercial purposes, 47 U.S.C. § 231(a)(1), subject to a safe harbor for sites that made a "good faith" effort to restrict access by minors: "(A) by requiring use of a credit card, debit account, adult access code, or adult personal identification number; (B) by accepting a digital certificate that verifies age; or (C) by any other reasonable measures that are feasible under available technology," 47 U.S.C. § 231(c)(1).

[20] Adam Thierer, "Closing the Book on COPA?" *Technology Liberation Front*, January 21, 2009, http://techliberation.com/2009/01/21/closing-the-book-on-copa.

[21] *ACLU v. Gonzales*, 478 F. Supp. 2d 775, 806 (E.D. Pa. 2007).

Supreme Court rejected the federal government's latest request to revive the law, meaning it is likely dead.

There are many other concerns about age-verification mandates.[22] A 2008 report produced by the Internet Safety Technical Task Force (ISTTF), a Harvard-based blue ribbon task force assembled by state Attorneys General to study this issue, found that:

> Age verification and identity authentication technologies are appealing in concept but challenged in terms of effectiveness. Any system that relies on remote verification of information has potential for inaccuracies. For example, on the user side, it is never certain that the person attempting to verify an identity is using their own actual identity or someone else's. Any system that relies on public records has a better likelihood of accurately verifying an adult than a minor due to extant records. Any system that focuses on third-party in-person verification would require significant political backing and social acceptance. Additionally, any central repository of this type of personal information would raise significant privacy concerns and security issues.[23]

Internet security expert Bruce Schneier has similarly outlined the dangers of going down this path:

> The problem is that it won't work. Any design of the Internet must allow for anonymity. Universal identification is impossible. Even attribution—knowing who is responsible for particular Internet packets—is impossible. Attempting to build such a system is futile, and will only give criminals and hackers new ways to hide. […]
>
> Implementing an Internet without anonymity is very difficult, and causes its own problems. In order to have perfect attribution, we'd need agencies—real-world organizations—to provide Internet identity credentials based on other identification systems: passports, national identity cards, driver's licenses, whatever. Sloppier identification systems, based on things such as credit cards, are simply too easy to subvert. We have nothing that comes close to this global identification infrastructure. Moreover, centralizing information like this actually hurts security because it makes identity theft that much more profitable a crime.

---

[22] Adam Thierer, *Social Networking and Age Verification: Many Hard Questions; No Easy Solutions*, Progress on Point No. 14.5, The Progress & Freedom Foundation, March 2007; Adam Thierer, *Statement Regarding the Internet Safety Technical Task Force's Final Report to the Attorneys General*, The Progress & Freedom Foundation, January 14, 2008, www.pff.org/issues-pubs/other/090114ISTTFthiererclosingstatement.pdf; Jeff Schmidt, "Online Child Safety: A Security Professional's Take," *The Guardian*, spring 2007, www.jschmidt.org/AgeVerification/Gardian_JSchmidt.pdf.

[23] Internet Safety Technical Task Force, *Enhancing Child Safety & Online Technologies: Final Report of the Internet Safety Technical Task Force to the Multi-State Working Group on Social Networking of State Attorneys General of the United States*, December 31, 2008, 10, http://cyber.law.harvard.edu/pubrelease/isttf.

> And realistically, any theoretical, ideal Internet would need to allow people access even without their magic credentials. People would still use the Internet at public kiosks and at friends' houses.[24]

Moreover, Schneier correctly notes that "attempts to banish anonymity from the Internet won't affect those savvy enough to bypass it," which would include many teenagers.[25]

The COPPA regime partially dodged some of these problems by limiting its coverage to kids age 12 and under and stopping short of mandating strict age verification. Sites covered by COPPA are geared to small children and have very limited functionality or social networking capability. This makes them easier to identify and regulate. In proposing to extend COPPA's coverage to older minors and all websites, however, the Markey-Barton bill and state-based COPPA expansion efforts would convert COPPA into a variant of COPA by necessitating expanded age verification of all sites and users to be effective.

C. Raises Unforeseen Privacy & Security Issues

Ironically, another problem with these efforts is that expanding COPPA would require the collection of *more* personal information about kids and parents. For age verification to be effective at the scale of the Internet, the collection of massive amounts of additional data is necessary.

Who will collect, process, and retain all the data collected to verify ages, identities, and relationships? As the ISTTF noted of age-verification mandates, "Any central repository of this type of personal information would raise significant privacy concerns and security issues."[26]

Such databases would present an attractive target for hackers and scam artists. Recent data-breach incidents highlight the dangers of excessive data collection by companies.[27] Age-verification mandates would force companies to expand datasets about individuals during a time when many privacy advocates and security experts are encouraging data minimization instead.

D. Free Speech Rights of Teens in Play

There are also important free speech rights in play in these debates, including the rights of teens. While the First Amendment rights of teens are not on par with those of adults, they *do* have the right to access certain types of information and express themselves in certain ways.[28]

---

[24] Bruce Schneier, "The Internet: Anonymous Forever," *Forbes*, May 12, 2010, http://www.forbes.com/2010/05/12/privacy-hackers-internet-technology-security-anonymity.html.
[25] Ibid.
[26] Internet Safety Technical Task Force, *Enhancing Child Safety & Online Technologies: Final Report of the Internet Safety Technical Task Force to the Multi-State Working Group on Social Networking of State Attorneys General of the United States*, December 31, 2008, 10, http://cyber.law.harvard.edu/pubrelease/isttf.
[27] Matt Liebowitz, "2011 Set to Be Worst Year Ever for Security Breaches," *Security News Daily*, June 9, 2011, http://www.securitynewsdaily.com/2011-worst-year-ever-security-breaches-0857.
[28] Theresa Chmara and Daniel Mach, *Minors' Rights to Receive Information Under the First Amendment*, Memorandum from Jenner & Block to the Freedom to Read Foundation, February 2, 2004, www.ala.org/ala/aboutala/offices/oif/ifissues/issuesrelatedlinks/minorsrights.cfm.

Collecting information and learning from serious online sites clearly has great value to children. But teens also benefit from being able to participate in online interactions. As a recent MacArthur Foundation study of online youth Internet use concluded:

> Contrary to adult perceptions, while hanging out online, youth are picking up basic social and technological skills they need to fully participate in contemporary society. Erecting barriers to participation deprives teens of access to these forms of learning. Participation in the digital age means more than being able to access "serious" online information and culture.[29]

Finally, practically speaking, it is unclear whether it would be sensible to expect parents to verify their children for every website they wished to visit. For example, it seems like overkill—and certainly an annoyance—to require parental verification before a 17-year old can access *The New York Times* website or ESPN.com. Yet, a strict reading of the Markey-Barton bill and some state-based COPPA expansion efforts would require such parental verification. That might also encourage many older teens to lie about their age and seek to circumvent the regulations, which could drive many kids off of more "mainstream" sites and into less visible—and less safe—sites and forums.

PROBLEMS WITH THE "ERASER BUTTON" CONCEPT

The Internet "Eraser Button" concept raises many of the same practical and principled concerns as COPPA.[30]

A. Conflict with the First Amendment

First, an Eraser Button mandate could conflict with free speech rights and press freedoms. Enshrining into law such expansive privacy norms places stricter limits on others' rights to speak freely or to collect and analyze information they find online. The ramifications for journalism are particularly troubling. Good reporting requires that journalists gather and report facts, even many of a personal nature. Could a public figure claim "a right to be forgotten" or ask to hit the Eraser Button when a journalist or historian pens an article about important matters about them?

Emma Llansó, a fellow at Center for Democracy & Technology, argues that, "read literally, [the Markey-Barton bill] would, for example, permit any user to demand that NYTimes.com remove any article that refers to Sasha or Malia Obama."[31] That would be a direct affront to the First Amendment as journalistic freedoms apply even when minors are the subject of reports or histories.

---

[29] John D. and Catherine T. MacArthur Foundation, *Living and Learning with New Media: Summary of Findings from the Digital Youth Project*,2, http://digitalyouth.ischool.berkeley.edu/files/report/digitalyouth-WhitePaper.pdf.

[30] Adam Thierer, "Erasing Our Past On The Internet," *Forbes.com,* April 17, 2011, http://blogs.forbes.com/adamthierer/2011/04/17/erasing-our-past-on-the-internet.

[31] Emma Llansó, "Do Not Track for Kids Act: Good Idea Raises Real Challenges" (Washington, DC: Center for Democracy & Technology, May 16, 2011), http://cdt.org/do-not-track-for-kids.

B. Security Issues

The Eraser Button concept also raises security concerns. Is there an ironclad way for sites to verify someone's identity before processing a deletion request? Mandating the creation of eraser buttons would, ironically, require an identity verification system that would be used for potentially even more sophisticated online "tracking" than we see at work today.

An Eraser Button could open dangerous backdoor vulnerabilities to hackers or others with malicious intentions. Teens often share a great deal of personal information (including passwords) with friends and family members, which could lead to a disastrous scenario if others request deletion of information that should not be theirs to control.

C. Complexities Associated with Shared Content

Shared content also presents problems for the Eraser Button concept. Many photographs, blog posts, or social networking entries include multiple people and are copied and reposted on multiple sites (and often archived). Facebook says users submit around 650,000 comments on the 100-million pieces of content served up every minute on its site.[32] If one person decides to hit their Eraser Button on a site, would others have to delete content if it is shared? Must digital-archiving and data-storage services all comply with the same deletion requests a site receives? What about news sites or blogs that may have clipped some of the data?

There are other thorny enforcement issues to take into account. Who actually owns the data collected by online sites and services? Websites or data collection services might use personal information uploaded by individuals to run website analytics, serve up advertising to support "free" online content, or just improve the user experience. Untangling who technically owns what can be complicated, especially in light of the sheer volume of information uploaded every day.

D. Conflict with 47 U.S.C. §230 ("Section 230")

The Eraser Button concept could also lead to a flood of bogus takedown requests. Every blogger could conceivably be asked at any time to delete any comment on any post ever written if someone does not like the commentary written online about them. If that occurs, an Eraser Button mandate would be in conflict with 47 U.S.C. §230, otherwise known as "Section 230."

Section 230 was part of the Telecommunications Act of 1996. It shielded "interactive computer services" from intermediary liability for information posted or published on their systems by third parties.[33] Importantly, it also shielded them from liability if they took steps to restrict access to "objectionable" materials that traveled over their systems.[34] This means online

---

[32] Ken Deeter, "Live Commenting: Behind the Scenes," Facebook.com, February 7, 2011, http://www.facebook.com/note.php?note_id=496077348919.

[33] "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."47 U.S.C. Sec. 230(c)(1).

[34] "No provider or user of an interactive computer service shall be held liable on account of any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or any action taken to enable or make available to information content providers or others the technical means to restrict access to [objectionable] material…"47 U.S.C. Sec. 230(c)(2).

intermediaries have generous leeway to determine what content and commerce travels over their systems without the fear that they will be overwhelmed by lawsuits if other parties object to some of that content.

Online speech and commerce would likely be severely stifled if not for the broad immunities granted by Section 230. For example, user-generated content and "Web 2.0" social networking sites and services would have been less likely to develop as rapidly or robustly as they have.[35]

The Eraser Button concept would contradict the spirit of Section 230 and lead to confusion about what types of content must be taken down versus what could remain online without fear of liability. If the threat of liability encourages site administrators to begin removing massive amounts of content or blocking communications and social networking functionality, the chilling effect on the free exchange of views/information would likely be quite profound.

CONSTRUCTIVE ALTERNATIVES TO REGULATION

Some of the concerns that motivate the "Do Not Track Kids Act" and COPPA expansion efforts are understandable, but there is a superior framework for dealing with these concerns. "Educate and Empower" would address problems far more effectively and safely than the "Legislate and Regulate" approach.

Personal and parental responsibility must be part of this discussion. Education is the key and parents are the first line of defense, but schools, companies, and other institutions also have a role. This mentoring includes media-literacy courses and "digital citizenship" efforts aimed at encouraging better social norms.[36] Teaching our kids smarter online hygiene and "Netiquette" is vital. "Think before you click" should be lesson #1.They should also be encouraged to delete unnecessary online information occasionally.[37]

The FTC hosts a collaborative effort with other federal agencies called "OnGuard Online," which represents a savvy approach to raising awareness about various online threats.[38] Many companies and trade associations are also taking steps to raise awareness among their users about how they can better protect their privacy and security. Other non-profits—including many privacy advocates—offer instructional websites and videos explaining how privacy-sensitive consumers can take steps to protect their personal information online.

Companies also have an important role to play in creating "well-lit neighborhoods "online where kids will be safe. Online operators should also be careful about what (or how much)

---

[35] Adam Thierer, "The Greatest of All Internet Laws Turns 15," *Forbes*, May 8, 2011, http://blogs.forbes.com/adamthierer/2011/05/08/the-greatest-of-all-internet-laws-turns-15.

[36] *Digital Literacy and Citizenship in the 21st Century* (San Francisco, CA : Common Sense Media, March 2011), http://www.commonsensemedia.org/sites/default/files/DigitalLiteracyandCitizenshipWhitePaper-Mar2011.pdf; Anne Collier, "From Users to Citizens: How to Make Digital Citizenship Relevant," *Net Family News*, November 16, 2009, www.netfamilynews.org/2009/11/from-users-to-citizen-how-to-make.html; Nancy Willard, "Comprehensive Layered Approach to Address Digital Citizenship and Youth Risk Online," Center for Safe and Responsible Internet Use, November 2008, www.cyberbully.org/PDFs/yrocomprehensiveapproach.pdf.

[37] Anne Collier, "'Delete Day': Students Putting Messages That Matter Online," *NetFamilyNews.org*, May 6, 2011, http://www.netfamilynews.org/?p=30376.

[38] http://www.onguardonline.gov.

information they collect—especially if they primarily serve young audiences. Most widely trafficked social networking sites and search engines already offer a variety of privacy controls. And accounts can always be deleted.

Many excellent online safety and privacy-enhancing tools already exist for parents and teens to better safeguard their online privacy.[39] A host of tools are available to block or limit various types of data collection, and every major web browser has cookie-control tools to help users manage data collection. Consider some of the privacy-enhancing tools and systems already available on the market today:

- "Ad preference managers" have caught on with major search companies. Google,[40] Microsoft,[41] and Yahoo![42] all offer easy-to-use opt-out tools and educational web pages that clearly explain to consumers how digital advertising works.[43] Meanwhile, DuckDuckGo offers an alternative search experience that blocks data collection altogether.[44]
- Major browser providers also offer "private browsing" modes, which allows users to turn on a "stealth browsing mode" to avoid data collection/tracking. This functionality is available as a menu option in Microsoft's Internet Explorer ("InPrivate Browsing"),[45] Google's Chrome ("Incognito"),[46] and Mozilla's Firefox ("Private Browsing").[47] Firefox also has many add-ons available that provide the functional equivalent to stealth mode or offer additional functionality.[48] "With just a little effort," notes Dennis O'Reilly of *CNET News.com*, "You can set Mozilla Firefox, Microsoft Internet Explorer, and Google Chrome to clear out and block the cookies most online ad networks and other Web trackers rely on to build their valuable user profiles."[49]
- Users can also take advantage of many supplemental tools and add-ons to better protect their privacy online by managing cookies, blocking web scripts, and so on. Like the marketplace for parental-control technologies, a remarkable amount of innovation continues in the market for privacy-empowerment tools, so much so that it is impossible

[39] Adam Thierer, *Public Interest Comment on Protecting Consumer Privacy in an Era of Rapid Chang*e, Mercatus Center at George Mason University, February 18, 2011, 24-28, http://mercatus.org/publication/public-interest-comment-protecting-consumer-privacy-era-rapid-change.
[40] http://www.google.com/ads/preferences.
[41] http://choice.live.com/Default.aspx and https://choice.live.com/AdvertisementChoice/Default.aspx.
[42] http://info.yahoo.com/privacy/us/yahoo/opt_out/targeting/details.html.
[43] Microsoft Advertising AdCenter: http://advertising.microsoft.com/home?s_cid=us_msn_footer; Yahoo! Privacy Center: http://info.yahoo.com/privacy/us/yahoo; Google Privacy Center: http://www.google.com/privacy/ads.
[44] http://duckduckgo.com/privacy.html. See also Jennifer Valentino-DeVries, "Can Search Engines Compete on Privacy?" *Wall Street Journal*, January 25, 2011, http://blogs.wsj.com/digits/2011/01/25/can-search-engines-compete-on-privacy.
[45] http://www.microsoft.com/windows/internet-explorer/features/safer.aspx?tab=6.
[46] http://www.google.com/support/chrome/bin/answer.py?hl=en&answer=95464.
[47] http://support.mozilla.com/en-US/kb/Private%20Browsing.
[48] https://addons.mozilla.org/en-US/firefox/tag/incognito.
[49] Dennis O'Reilly, "Add 'Do Not Track' to Firefox, IE, Google Chrome," *CNetNews.com*, December 7, 2010, http://news.cnet.com/8301-13880_3-20024815-68.html.

to document everything. However, some of the more notable ones include: Ghostery,[50] NoScript,[51] Cookie Monster,[52] Better Privacy,[53] Track Me Not,[54] and the Targeted Advertising Cookie Opt-Out or "TACO" for Firefox;[55] No More Cookies for Internet Explorer;[56] Disconnect for Chrome;[57] AdSweep for Chrome and Opera;[58] CCleaner for PCs;[59] and Flush for Mac.[60]

- New empowerment solutions are constantly turning up.[61] In particular, the "online-reputation management" market continues to grow. Google recently launched a free online-reputation management tool that allows users to get regular reports about what others are saying about them online.[62] Meanwhile, for $4 to $8 per month, Reputation.com's new "MyPrivacy" service lets users remove their information from various websites or data-collection services.[63]
- Adblock Plus, which lets users block advertising on most websites, is the most downloaded add-on for both the Firefox and Chrome web browsers.[64] As of June 2011, roughly 125 million people (roughly 86,000 per day) had downloaded the Adblock Plus add-on for the Firefox web browser.[65] Incidentally, both Adblock Plus and NoScript, the third most popular download on Firefox, support the Do Not Track protocol.[66]
- Finally, pressured by the FTC and privacy advocates, all three of the major browser-providers—Microsoft,[67] Google,[68] and Mozilla[69]—have now agreed to include some

[50] https://addons.mozilla.org/en-US/firefox/addon/ghostery.
[51] https://addons.mozilla.org/en-US/firefox/addon/noscript.
[52] https://addons.mozilla.org/en-US/firefox/addon/cookie-monster.
[53] https://addons.mozilla.org/en-US/firefox/addon/betterprivacy.
[54] https://addons.mozilla.org/en-US/firefox/addon/trackmenot.
[55] There are multiple versions of the TACO add-on available for Firefox web browser.
[56] http://download.cnet.com/No-More-Cookies/3000-2144_4-10449885.html.
[57] http://www.disconnectere.com.
[58] https://addons.opera.com/addons/extensions/details/adsweep/2.0.3-3/?display=en.
[59] http://www.piriform.com/ccleaner.
[60] http://www.macupdate.com/app/mac/32994/flush.
[61] David Gorodyansky, "Web Privacy: Consumers Have More Control Than They Think," *The Huffington Post*, December 30, 2010, http://www.huffingtonpost.com/david-gorodyansky/web-privacy-consumershav_b_799881.html.
[62] Sarah Kessler, "Google Launches Tool for Online Reputation Management," *USA Today*, June 16, 2011, http://content.usatoday.com/communities/technologylive/post/2011/06/google-launches-tool-for-online-reputation-management/1; Andreas Tuerk, "Me, Myself and I: Helping to Manage Your Identity on the Web," *Google Public Policy Blog,* June 15, 2011, http://googlepublicpolicy.blogspot.com/2011/06/me-myself-and-i-helping-to-manage-your.html.
[63] http://www.reputation.com/myprivacy.
[64] https://adblockplus.org/en.
[65] https://addons.mozilla.org/en-US/firefox/addon/adblock-plus.
[66] http://hackademix.net/2010/12/28/x-do-not-track-support-in-noscript.
[67] Dean Hachamovitch, "IE9 and Privacy: Introducing Tracking Protection," Microsoft *IE Blog*, December 7, 2010, http://blogs.msdn.com/b/ie/archive/2010/12/07/ie9-and-privacy-introducing-tracking-protection-v8.aspx; Dean Hachamovitch, "Update: Effectively Protecting Consumers from Online Tracking," Microsoft *IE Blog*, January 25, 2010, http://blogs.msdn.com/b/ie/archive/2011/01/25/update-effectively-protecting-consumers-from-online-tracking.aspx.

variant of a Do Not Track mechanism or an opt-out registry in their browsers to complement the cookie controls they already offered. These developments build on industry-wide efforts by the Network Advertising Initiative and the "Self-regulatory Program for Online Behavioral Advertising"[70] to make opting-out on targeted advertising simpler. A collaboration of the leading trade associations in the field announced that effort last Fall. They include: American Association of Advertising Agencies, American Advertising Federation, Association of National Advertisers, Better Business Bureau, Digital Marketing Association, Interactive Advertising Bureau, and Network Advertising Initiative.[71] Their program uses an "Advertising Option Icon" to highlight a company's use of targeted advertising and gives consumers an easy-to-use opt-out option. It was accompanied by an educational initiative, www.AboutAds.info, which offers consumers information about online advertising.[72] The independent Council of Better Business Bureaus will enforce compliance with the system.

Empowerment efforts such as these have the added advantage of being more flexible than government regulation, which tends to lock-in sub-optimal policies and stifle ongoing innovation.

What these developments illustrate is a well-functioning marketplace that is evolving to offer consumers greater control over their privacy without upending online markets or destroying the quality of the browsing experience. It would be difficult to claim any sort of "market failure" exists when such a robust marketplace of empowerment tools exists to serve the needs of privacy-sensitive web surfers.

Just as most families leave the vast majority of parental control technologies untapped, many households will never take advantage of these privacy-enhancing empowerment tools.[73] That fact does not serves proof of "market failure" or the need for government regulation, however. What matters is that the tools exist for those who wish to use them, not the actual uptake/usage of those tools.

---

[68] Sean Harvey and Rajas Moonka, "Keeping Your Opt-outs," *Google Public Policy Blog*, January 24, 2010, http://googlepublicpolicy.blogspot.com/2011/01/keep-your-opt-outs.html.

[69] Stephen Shankland, "Mozilla Offers Do-Not-Track Tool to Thwart Ads," *CNet News Deep Tech*, January 24, 2011, http://news.cnet.com/8301-30685_3-20029284-264.html; Julia Angwin, "Web Tool On Firefox To Deter Tracking," *Wall Street Journal*, January 24, 2011, http://online.wsj.com/article/SB10001424052748704213404576100441609997236.html.

[70] http://www.aboutads.info.

[71] Network Advertising, "Major Marketing/Media Trade Groups Launch Program to Give Consumers Enhanced Control over Collection and Use of Web Viewing Data For Online Behavioral Advertising," Press release, October 4, 2010, www.networkadvertising.org/pdfs/Associations104release.pdf.

[72] http://www.aboutads.info/principles.

[73] Adam Thierer, "Who Needs Parental Controls? Assessing the Relevant Market for Parental Control Technologies," *Progress on Point* 16.5, The Progress & Freedom Foundation, February 27, 2009, http://www.pff.org/issues-pubs/pops/2009/pop16.5parentalcontrolsmarket.pdf.

REGULATION IS NOT COSTLESS

This "Educate and Empower" approach also makes sense because of the cost associated with regulation. The vast majority of online sites and services are free of charge to the consumer. This did not happen by magic—advertising and data collection made it possible.[74]New privacy rules could result in online pay walls, subscriptions, micropayment schemes, or tiered services.[75] Web developers might have no choice but to raise prices to cover costs or cut back service.[76] Regulation could also destroy opportunities for new or smaller website operators to break into the market and offer competing services and innovations, thus contributing to consolidation of online content and services by erecting barriers to entry.

The overall health of modern media marketplace and the digital economy—and the aggregate amount of information and speech that can be produced or supported by those sectors—is fundamentally tied up with the question of whether policymakers allow the online advertising marketplace to evolve in an efficient, dynamic fashion.[77]A recent study by Avi Goldfarb and Catherine Tucker found that "after the [European Union's] Privacy Directive was passed [in 2002], advertising effectiveness decreased on average by around 65 percent in Europe relative to the rest of the world."[78] They argue that because regulation decreases ad effectiveness, "this may change the number and types of businesses sustained by the advertising-supporting Internet." Regulation of advertising and data collection for privacy purposes, it seems, can affect the global competitiveness of online firms.

Targeted forms of online advertising could improve this effectiveness. A March 2010 study on "The Value of Behavioral Targeting," conducted by Howard Beales on behalf of the Network Advertising Initiative, demonstrates how this could be the case.[79] Beales, the former director of

---

[74] Adam Thierer, "Unappreciated Benefits of Advertising and Commercial Speech," *Mercatus on Policy* 86 (Arlington, VA: Mercatus Center at George Mason University, January 2011), http://mercatus.org/publication/unappreciated-benefits-advertising-and-commercial-speech.

[75] Daniel D. Castro, "'Do-Not-Track'" Legislation: Is Now the Right Time?" Testimony Before the Committee on Energy and Commerce Subcommittee on Commerce, Trade, and Consumer Protection, December 2, 2010, http://democrats.energycommerce.house.gov/documents/20101202/Castro.Testimony.12.02.2010.pdf; Lauren Weinstein, "Do-Not-Track, Doctor Who, and a Constellation of Confusion," *Lauren Weinstein's Blog,* April 30, 2011, http://lauren.vortex.com/archive/000848.html; Adam Thierer, *Public Interest Comment on Protecting Consumer Privacy in an Era of Rapid Change*, Mercatus Center at George Mason University, February 18, 2011, 12-14, http://mercatus.org/publication/public-interest-comment-protecting-consumer-privacy-era-rapid change.

[76] Adam Thierer, "Birth of the Privacy Tax," *Forbes.com*, April 4, 2011, http://www.forbes.com/2011/04/02/privacy-tax-social-networking-advertising-opinions-contributors-adam-thierer.html.

[77] Larry Downes, *The Laws of Disruption: Harnessing the New Forces that Govern Life and Business in the Digital Age* (New York: Basic Books, 2009), 83-84. "Much of the valuable information content available on the Internet, and so many of the useful services we use every day, is free not because of some utopian dream of inventors or even because of the remarkably low transaction costs of the digital economy. The content is free because the costs of the services—blogs, stock quotes, even home movies posted on YouTube—are underwritten by advertisers. If we don't read and respond to ads, we'll have to pay for these services some other way."

[78] Avi Goldfarb and Catherine Tucker, "Privacy Regulation and Online Advertising," 57 *Management Science* 1, January 2011, 57-71, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1600259.

[79] Howard Beales, "The Value of Behavioral Targeting," Network Advertising Initiative, March 2010, www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf.

the Bureau of Consumer Protection at the FTC, found that advertising rates are significantly higher for behaviorally targeted ads, with the average return on behaviorally targeted advertising being just over twice that of other advertising. The reason that greater return on investment is important, Beales notes, is because:

> Advertising using behavioral targeting is more successful than standard run of network advertising, creating greater utility for consumers from more relevant advertisements and clear appeal for advertisers from increased ad conversion. Finally, a majority of network advertising revenue is spent acquiring inventory from publishers, making behavioral targeting an important source of revenue for online content and services providers as well as third-party ad networks.[80]

This illustrates how more effective advertising can cross-subsidize and sustain online content and culture. More and better advertising means more and better content and services will be made available to consumers. Beales concluded his study by noting, "Increasingly, advertising is the financing mechanism that makes online content and services possible as well. As content traditionally provided offline (such as newspapers) continues to move to the Internet, the link between online advertising and content is likely to become increasingly vital to the provision of information and services that we have long taken for granted."[81]

CONCLUSION

Thus, expanding COPPA or imposing solutions like an Internet Eraser Button will have a deleterious economic impact on Internet companies and online consumers. Those who call for expanded regulation should be required to provide a strict cost-benefit analysis of the restrictions they would impose upon America's vibrant digital marketplace.

COPPA expansion or an Internet Eraser Button mandate will raise serious free speech concerns. In particular, limitations on the collection and reporting of facts about individuals could come into conflict with press freedoms and raise First Amendment issues as a result.

COPPA expansion could also give rise to unanticipated privacy problems. In the name of protecting children's privacy, these rules could require the collection of *more* information about minors and their parents since ages and identities would need to be strictly verified.

Parents and guardians can protect kids' privacy without resorting to unworkable and costly regulatory schemes. The key to that process is education and empowerment of parents and minors alike. Targeted law enforcement efforts can also play a role at the margin when unfair and deceptive practices are shown to exist.

[80] Ibid., 1.

[81] Ibid., 18.