Journal of Civil Rights and Economic Development

Volume 16
Issue 3 *Volume 16, Fall 2002, Issue 3*

Article 6

The Current State of Online Privacy

Andrew Shen

THE CURRENT STATE OF ONLINE PRIVACY

ANDREW SHEN*

My name is Andrew Shen and I work for the Electronic Privacy Information Center. My goal as the first speaker of the afternoon is to set the stage for the rest of the speakers whose own legal expertise on COPPA (Children's Online Privacy Protection Act) far exceeds mine. I am also here to describe the current Internet privacy environment including: what challenges consumers face when they surf the Internet; how privacy can be protected on the Internet; and finally provide some background on the passage of COPPA. Lastly, I will address the prospect for future privacy law – whether we will have a similar law protecting the privacy of adults.

We heard from Commissioner Thompson at lunch about many of the current trends in the Internet space. One phenomenon he addressed specifically was the drive towards personalization and customization. For example, when you visit a Web site like Amazon.com, it's ready to provide recommendations on what books you should buy based on previous purchases. The presumption behind this marketing technique is that if you see these recommendations, you'll be more likely to purchase an item and return to the site in the future.

This drive towards personalization and customization does not require identifying website visitors, but it does involve the collection of clickstream data - information about purchases on that site and pages that a consumer visited. This level of personalization is unique to the Internet. While some personalization has always been attempted through mass media, the Internet has taken it to another level.

The architecture of the Internet facilitates passive information collection from website visitors. In the off-line world, most of the

* Andrew Shen is a Senior Policy Analyst at the Electronic Information Center. He works on privacy issues with a special focus on the Internet.

information provided to any company or any person is provided affirmatively. For example, when I attend conferences, I hand out my business card so that you can contact me later. I am affirmatively providing you my personal information.

Something different about the Internet – and I can't emphasize this enough – is that it can collect a lot of information passively. What web pages you go to are constantly being recorded. What products you see on particular pages are constantly being recorded. What sort of news stories you read is also being recorded. You do not have to affirmatively provide this information and thus most people tend to be unaware of its collection. This information can be collected at an extremely granular level so that it is even possible to time how long someone is reading a particular story. This experience is quite different from what most consumers expect. If you go to an off-line bookstore such as Barnes & Noble or Borders, you are used to browsing the shelves, picking up a book, scanning the back cover, and maybe choosing to purchase the item. But Barnes & Noble or Borders, no matter how much they try, will never know that you looked at that particular book while in their physical store. But an online bookseller will know – even if you choose not to purchase any items. This architectural difference of the Internet is important to understand.

So we have a couple of factors to consider. We have a drive from many companies to collect more information about you than they have ever been able to do so before. They're using these techniques in an attempt to bring customers to their doorsteps. Also, the architecture of the Internet allows this to happen.

What limits currently exist for this information collection? Commissioner Thompson also addressed this earlier today and that is the concept of self-regulation.[1] Self-regulation basically

[1] *See* Angela J. Campbell, *Self-Regulation and the Media*, 51 FED. COMM. L.J. 711, 714 (1999) (defining "self-regulation" narrowly to refer only to those instances "where the government has formally delegated the power to regulate, as in the delegation of securities industry oversight to the stock exchanges, and broadly when dealing with the private sector's need to regulate itself in order to enhance industry reputation," and to level the market playing field); *see also* Stephanie Byers, Note, *The Internet: Privacy Lost Identities Stolen*, 40 BRANDEIS L.J. 141, 145 (2001) (describing self-regulation under Clinton's administration as "the best means of protecting the personal privacy of online users without burdening industry with government interference."). *But see* Ruth Hill Bro, Brian Hengesbaugh & Mark Weston, *And You Thought HIPAA was the Tough Part; European Union Cracks Down on Information Sharing*, BUS. L. TODAY, Dec. 11, 2001 at 25-26 (discussing how even though U.S. has preferred use of self-regulation to legislation

requires companies to describe what they're doing with your information through privacy policies or notices. Such privacy policies will describe the basic types of information collected and hopefully how that information will be used and secured.

Self-regulation lets companies write the rules for their own behavior. It lets companies dictate what procedures and practices they are going to follow. The Federal Trade Commission is then responsible for ensuring that companies follow through on their stated practices. That is, once a company makes a public statement about what it's doing, that Section 5 of the Federal Trade Commission Act, which prohibits unfair and deceptive practices, holds company to that statement.[2]

The absence of baseline standards, and allowing companies to write the rules, has lead to many problems. Importantly, in addition to the Federal Trade Commission Act, self-regulation relies on the presumption that major companies will want to provide a high level of privacy to keep consumers comfortable. If a company does not respect the privacy of its customers and visitors, then it is thought that customers and visitors will choose to shop at different sites. But I think there are a couple of important caveats to that presumption.

Even though many companies, especially large ones, do want to protect their privacy-respecting reputations, not all companies make privacy a priority. Also, many people do not read privacy policies or notices so many consumers don't know what protections are or are not offered. In addition, many companies get away with a lot in the fine print. For example, on the matter of fine print, I visited Amazon.com yesterday and took a look at its privacy policy. Towards the very end of its privacy policy is the following statement: "Our business changes constantly. This notice and conditions of use will change also, and use of information that we gather now is subject to the privacy notice in effect at the time of use."

Now is that fair for consumers? Can information a company is collecting from you now be subject to terms that you have not yet seen? That seems tremendously unfair to me and I'm not sure how the Federal Trade Commission Act may apply.

on issues of privacy, there is now federal protection emerging on private information).

[2] 15 U.S.C. § 45(a)(1) (2002).

So I think we have a problem. I think that companies have many incentives to collect as much information as possible and existing protections tend to be weak or unfair for consumers.

EPIC (Electronic Privacy Information Center) has a two part-answer to the question of how to protect privacy online – law and technology. First, there must be a high legal standard for privacy protection rather than total reliance on the Federal Trade Commission Act.[3] Even with the Children's Online Privacy Protection Act, any Internet privacy laws do not protect most consumers.[4] Most of us have no legal protections governing how our personal information can be used.

The measuring stick for evaluating privacy law is a concept called "fair information practices."[5] Fair information practices encompass some of the principles discussed earlier today such as notice, choice, access and security - but that's only one iteration of these principles. Another version has been developed by the

[3] *See* Major R. Ken Pippin, *Consumer Privacy on the Internet: It's "Surfer Beware"*, 47 A.F. L. REV. 125, 135 (1999) (discussing how Commission "endorses self-regulation as best option available," because of "difficulties for federal government in responding quickly to technological advancements, as well as fear of hindering electronic commerce."); *see also* Jeffrey B. Ritter et al., *Emerging Trends in International Privacy Law*, 15 EMORY INT'L L. REV. 87, 107 (2001) (stating how FTC in past situations encouraged self regulation on privacy matters). *But see* Robert Pitofsky, *Privacy Online: Fair Information Practices in the Electronic Marketplace: Before the Senate Comm. on Commerce, Sci., and Transp.*, (2000) *at* http://www.ftc.gov/os/2000/05/testimonyprivacy.htm (discussing FTC's change of view for establishing federal regulations in certain business areas for privacy matters).

[4] *See* Ethan Haywar, *Legislative Updates: The Federal Government as Cookie Inspector: The Consumer Privacy Protection Act of 2000*, 11 DEPAUL-LCA J. ART & ENT. L. & POL'Y. 227, 238 (2001) (discussing need for safeguarding against inadvertent information disclosure to unaffiliated third parties for adult internet users, similar to COPPA in place for children). *But see* Fred H. Cate, *The Changing Face of Privacy Protection in the European Union and the United States*, 33 IND. L. REV. 174, 211 (1999) (discussing how "Congress has enacted variety of laws addressing protection of personal information in private industry sectors"); Neil Weinstock Netanel, *Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory*, 88 CAL. L. REV. 395, 475-76 (2000) (discussing how self regulation gives Internet "users choice between website rule regimes that protect data privacy and those that do not.").

[5] *See* Jordan M. Blanke, *"Safe Harbor" and The European Union's Directive on Data Protection*, 11 ALB. L.J. SCI. & TECH. 57, 72-73 (2000) (discussing alternative government regulations to ensure fair information practices); *see also* Pippin, *supra* note 3, at 133 (stating how self-regulation is efficient means to ensure fair information practices, given rapidly evolving nature of internet and technology). *See generally* John MacDonnell, *Exporting Trust: Does E-Commerce Need a Canadian Privacy Seal of Approval?*, 39 ALBERTA L. REV. 346, 358 (2001) (listing United State's five-part Code of Fair Information Practices); Center for Democracy and Technology, *Comments on the Draft 'Principles for Providing and Using Personal Information*, March 21, 1995, *at http://www.cdt.org/privacy/comments_iitf.html* (last visited March 31, 2002) (stating that "Code of Fair Information Practices . . . served as model for privacy legislation in this country and worldwide.").

OECD (Organization for Economic Cooperation and Development).[6] These guidelines were developed through an international effort and their international character is important to note.

The OECD's fair information practices include further privacy protections such as accountability – assuring that companies are living up to their stated practices.[7] A company should also specify the purposes for information collection and obtain the consent of the user before collecting and using data. Companies should also limit the use of that personal information. Information should be kept accurate and up-to-date. Consumers should be able to access and review information that has already been collected from them. And individuals should be able to bring complaints against a company if they believe it is not living up to its public statements.

But, in addition to these legal standards, I think it is important to think about the technology behind the Internet. More than any other medium, and several distinguished legal scholars have addressed this, the Internet is a flexible medium. The Internet does not have a set architecture and its design can be changed. Privacy enhancing technologies can make the Internet more anonymous and privacy protective. These privacy enhancing technologies would allow a consumer to limit the information collected and allow companies to fulfill their obligations of the fair information practices more easily. I'll mention briefly one example of these technologies.

In the Center for Media Education report released yesterday, the organization found that COPPA spurred privacy innovation

[6] *See* Daniela Ivascanu, *Part II: Speeches and Annex: Legal Issues in Electronic Commerce in the Western Hemisphere*, 17 ARIZ. J. INT'L & COMP. LAW 219, 225 (2000) (discussing how OECD is drafting guidelines for consumer protection for electronic commerce); *see also* Jonathan P. Cody, Comment, *Protecting Privacy Over The Internet: Has The Time Come to Abandon Self-Regulation?*, 48 CATH. U. L. REV. 1183 (2000) (discussing OECD's development of guidelines for protection of private information, in light of rapid development of Internet and growth of electronic commerce throughout world); Laura J. Nicholson et. al., *Computer Crimes*, 37 AM. CRIM. L. REV. 207, 258 (2000) (discussing how OECD's member countries plan to formulate policies and legislation to guard against computer crimes, including privacy issues).

[7] *See* Ivascanu, *supra* note 6, at 232-55 (discussing how OECD is drafting guidelines for consumer protection for electronic commerce); *see also* Cody, *supra* note 6, at 1190 (discussing OECD's development of guidelines for protection of private information using self regulation methods); Pippin, *supra* note 3, at 133 (using self-regulation to monitor assurance and accountability).

among some websites.[8] Many websites have tried to comply with COPPA in a way that does not interfere with their business models. One-way companies have found that they can achieve both goals is by collecting information based on a pseudonym or user name. The use of pseudonyms is an option on the Internet but not typically in the off-line world. In the off-line world, I have to use the name Andrew Shen as an identifier but with a pseudonym, online companies can personalize their content to a target individual without tying it to an off-line identity. This is an innovative way to meet legal requirements and protect privacy. In addition, many companies may not have taken these privacy protection steps without being encouraged to do so by the legal requirements of COPPA.

To return to a bit more to the topic of today's discussion let me examine why we currently have COPPA. It's important to understand the policy context for why we have this law.

My first point is quite obvious and that is that kids are different. It's easy for a Congressman in Washington, DC to say: "I want to protect the privacy of kids," without anyone opposing such an issue, thus making it an easy issue to push forward. Moreover, we have a tradition of protecting children from undue privacy invasions, unfair marketing practices, and aggressive advertising.[9]

In addition to this tradition of protecting children, there were a couple of studies that helped shed light on the particular issue of

[8] *See* Melanie L. Hersh, *Is COPPA a Cop Out? The Child Online Privacy Protection Act as Proof That Parents, Not Government, Should Be Protecting Children's Interests on The Internet*, 28 FORDHAM URB. L.J. 1831, 1833-34 (2001) (discussing how growing awareness of online predators has focused parental and governmental attention on dangers Internet poses for children and apparent need for protection). *See generally* Joshua Warmund, *Can COPPA Work? An Analysis of the Parental Consent Measures in the Children's Online Privacy Protection Act*, 11 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 189, 193-95 (2000) (stating that FTC's guidelines for data collection from children on Internet for first time was established in May 1996 Center for Media Education petition to FTC to investigate online website KidsCom.com ("KidsCom") and bring enforcement action against it); Jennifer Zwick, Comment, *Casting a Net Over The Net: Attempts to Protect Children in Cyberspace*, 10 SETON HALL CONST. L.J. 1133 (2000) (discussing FTC opinion brought forward by petition of Center for Media Education, and creation of COPPA thereafter).

[9] *See, e.g.*, Electronic Privacy Bill of Rights Act of 1999, H.R. 3321, 106th Cong. § 8(1) (1999) (providing for review of the efficacy of Act specifically relating to information collected from children); Children's Defense Act of 1999, H.R. 2036, 106th Cong. (1999) (proposing amendment whose purpose is to protect children from advertising through many forms of media); Children's Privacy Protection Act and Parental Empowerment Act of 1999, H.R. 369, 106th Cong. § 2 (1999) (requiring written parental consent before collecting information from children).

children's privacy online. The first was a report titled "Web of Deception" produced by the Center for Media Education in 1996.[10] It was one of the first explorations of Internet marketing and information practices aimed at children. It was quite an effective shaming of companies and brought privacy problems to full light.

The study documented how children were offered free gifts such as T-shirts or chances to win a portable CD player by filling out an online survey or by signing up for an online raffle. Children as young as age 8 were being asked to fill out information forms in order to win prizes and were often urged to do so by one of their favorite television superheroes. The report also found that children's online activities were monitored in a more detailed manner than ever before due to the unique features of the Internet that I have already mentioned.

Moreover, because of this information collection, a lot of advertising was becoming much more personalized. While adults have a better chance of making a fair and unbiased determination of whether or not to follow up on a personalized offer, some children may not.

Later, the FTC presented their own report on children's online privacy to Congress.[11] This was their first such report and it found that many websites targeted at children weren't making the grade. The FTC found that 89% of the children's sites surveyed collected personally identifiable information and only half of those sites disclosed what they were doing with that data. Only half of them had any sort of privacy policy. And less than 10 % of websites examined provided for some parental control over the collection of information from children. The idea that parents should play a part in how information is being collected later became an important part of COPPA.[12]

[10] Kathyrn Montgomery & Shelley Pasnik, *Web of Deception: Threats to Children from Online Marketing*, (1996), *at* http://www.cme.org/children/marketing/deception.pdf. *See* Jeffrey D. Stanger & Natalia Gridina, *Media in the Home*, (1999), *at* http://www.appcpenn.org/mediainhome/survey/survey5.pdf (reporting rising concern of parents with influence and content of Internet on their children); *see also* FTC Staff Rep., *Public Workshop on Consumer Privacy on the Global Information Infrastructure*, (Dec. 1996), *at* http://www.ftc.gov/reports/privacy/privacy5.htm (noting potential ease with which information about children could be collected on Internet without parental notification or consent).

[11] FTC Rep., *Privacy Online: A Report to Congress*, (June 1998), *at* http://www.ftc.gov/reports/privacy3/ priv-23a.pdf.

[12] FTC Rep., *Privacy Online: A Report to Congress*, (June 1998), *at*

So, COPPA has demonstrated the importance of policy consensus.[13] When different interested groups examined these practices, it was obvious to almost all of them that steps needed to be taken. Business groups came together with consumer groups to urge Congress to pass this legislation.

Another important factor behind COPPA is the existence of similar prior legislation. In 1974, Congress passed the Family Education Rights and Privacy Act or FERPA.[14] This law addressed education records – so-called "permanent records." FERPA addressed to whom educational information could be disclosed and required parental consent for their disclosure. It also required that parents have access to their children's educational records – similar to COPPA.[15] This is something you often see in the privacy law arena – the same sort of legal standards being used over and over in different sectors.

I have a last couple of thoughts I wish to leave you with. The prospects for future privacy law are dimmer than for COPPA due to the lack of similar policy consensus. Business groups do not

http://www.ftc.gov/reports/privacy3/ priv-23a.pdf. (deeming parents' involvement "fundamental"); *see also* H.R. REP. NO. 105-775 (1998) (noting need for parents to take an active role to protect children from Internet dangers); R. Ken Pippin, *Consumer Privacy on the Internet: It's "Surfer Beware"*, 47 A.F. L. REV. 125, 136 (1999) (stating one goal of COPPA was to insure parents were involved and consented to information being collected from their children online).

[13] This policy consensus can be shown by the variety of organizations that submitted reports recognizing the need for childrens' privacy legislation regarding the Internet, testified before congressional committees prior to the passage of COPPA and continue to monitor the progress that COPPA had made since its enactment towards improving the protection of children on their travels around the Internet. The participation of government organizations, nonprofit groups and business groups, each with distinct and not always similar interests, all contributed commentary and ideas about how to bring about legislation aimed at improving Internet privacy for children. For example, the Center for Media Education (CME) (www.cme.org), a national nonprofit organization, published an early report about childrens' privacy and continues to perform studies on the effectiveness of COPPA. The Federal Trade Commission (FTC) (www.ftc.gov) also played an important role as a consumer advocate in focusing on childrens' issues and pressing for the passage of COPPA. In addition, AOL Time Warner (www.aoltimewarner.com) was involved in advocating for greater protection of children on the Internet and continues to implement controls and policies that make childrens' safety and privacy on the Internet of paramount importance.

[14] 20 U.S.C.S. § 1232g (Lexis 2002). *See* Anita L. Allen, *Minor Distractions: Children, Privacy and E-Commerce*, 38 HOUS. L. REV. 751, 755 (2001) (comparing parental disclosure aspects of FERPA and COPPA); *see also* Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV 1393, 1441 (2001) (noting FERPA and COPPA as examples of legislation dealing with privacy).

[15] *Compare* Family Education Rights and Privacy Act, 20 U.S.C.S. § 1232g(b) (Lexis 2002) (stating parental consent requirement for release of educational records) *with* Children's Online Privacy Protection Act, 47 U.S.C.S. § 231(d)(1)(A)(ii) (Lexis 2002) (outlining parent or guardian consent requirement for disclosure of information concerning individual under 17 years of age).

see eye to eye with consumer groups on how the privacy of adults should be protected on the Internet. I think this is changing for the better but right now there is a lack of similar consensus. The strong public support for such protections give us reason to believe that such consensus will eventually emerge.

Lastly, I think that when we talk about any Internet law or any Internet issues we must keep in mind the international context for any potential strategy. That is, how does our approach mix with laws in the European Union, South America, or Asia? This factor has not really entered the COPPA debate. I believe that no other country in the world, maybe other than Korea, has a privacy law similar to COPPA. Hopefully, more will follow in the future because I think that if you want anything on the Internet to be effective, there needs to be an international consensus and a unified approach. That is the last I have to say and I hope to field some questions from the audience. I'm also very interested to hear from any practitioners in attendance on how they view COPPA and its implementation. Now I'll turn it over to the experts.