KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 Eye Street, NW
Suite 1100
Washington, DC 20006

Building the Digital Out-Of-Home Privacy Infrastructure

March 1, 2010

Introduction

Digital Out-Of-Home (DOOH), also known as digital signage or "smart signs," is a communications medium characterized by a dynamic display presenting messages in a public environment.[1] One of the most common examples of DOOH media is a flat screen television displaying a loop of advertisements in retail stores. Other DOOH units take the form of kiosks, projectors or digital billboards. The units appear in a broad range of settings, including in shopping malls, hospitals and doctors' offices, public transportation, gas stations, restaurants, government facilities and public schools. The messaging content is often controlled via computer, enabling one master location to control many networked units.

The medium is a prominent part of the shift in communications and advertising away from traditional offline media.[2] DOOH has rapidly grown into a multibillion-dollar industry over the past decade. Despite the economic downturn, industry forecasts predict growth at double-digit rates for the next 3-5 years.[3] There were an estimated 630,000 displays in the United States in 2007, though there are many more worldwide, particularly in China.[4]

---

[1] Digital Signage Resource, Digital Signage Terms Glossary, http://www.digitalsignageresource.com/digital-signage-glossary-of-terms.asp?modes=3&col=term&term=digital_signage (last visited Jan. 3, 2010).

[2] *VSS Forecast Shows Major Shifts in Communications Industry Growth Patterns*, Digital Signage Expo, Sep. 14, 2009, http://www.digitalsignageexpo.net/DNNArticleMaster/DNNArticleView/tabid/78/smid/1041/ArticleID/1854/reftab/67/t/VSS-Forecast-Shows-Major-Shifts-in-Communications-Industry-Growth-Patterns/Default.aspx.

[3] *Forecasts Show Digital Out-of-Home Still on Track for Growth*, Digital Signage Expo, Nov. 18, 2009, http://www.digitalsignageexpo.net/DNNArticleMaster/DNNArticleView/tabid/78/smid/1041/ArticleID/2249/reftab/67/t/Forecasts-Show-Digital-Out-of-Home-Still-on-Track-for-Growth/Default.aspx.

[4] *InfoTrends Study Shows Strong Growth Up Ahead for Digital Signage*, InfoTrends, Jun. 6, 2007, http://www.capv.com/public/Content/Press/2007/06.06.2007.html.

Until recently, a shortcoming of digital signage as an advertising medium was the challenge in determining how many and what kind of individuals see a given display unit. This made it difficult for advertisers to measure the size of their audience and price ad time on DOOH networks accordingly. This problem also makes it relatively difficult to target ads to specific audience demographics or psychographics, which is a cornerstone of modern advertising.

To overcome these obstacles, the DOOH industry is exploring several technologies that will improve audience measurement and interactivity. Depending on the system, these enhancements often obtain a range of information about consumers. Some of the technologies have the ability to identify individual consumers, track them as they move from place to place and store detailed information about their preferences and activities. These emerging technologies include

- Facial recognition: Increasingly, DOOH units use facial measurement technology to discern certain characteristics about a person looking at the display. This is perhaps the most common method, with one company claiming to have scanned 120 million people to date.[5] Some systems, while not yet configured to identify individuals, can calculate a passerby's age, gender, and race, and determine how long an individual watches the display. The advertisement on the screen can then change to match the consumer's profile. Other systems note only gender, and still others merely count the number of faces that see the screen (gaze-tracking).

- Mobile marketing: A rising number of DOOH units interact in various ways with portable devices, particularly mobile phones. Some units communicate with phones via SMS messaging and Bluetooth to send rich content (like ringtones or movie trailers) to consumers. Other units enable consumers to download a coupon, play games, or enter contests through their mobile phones. Given the broad range of potential applications for mobile marketing and DOOH, industry analysts predict the two media will grow together.

- Social networking: Some DOOH units provide access to social networks like Facebook, Twitter and Flickr through the Web or apps on consumers' mobile devices. In some applications, consumers can send user-generated messages, photos and other content to specific DOOH screen locations in real time. Some long-view predictions see consumers consulting friends about clothing purchases through retail-based DOOH screens over social networks.

- Radio Frequency Identification (RFID): The most common use of RFID in DOOH features RFID-enabled shelves that prompt nearby digital signage units to display advertisements related to the products

[5] Quividi, Automated Audience Measurement, http://www.quividi.com/ (last visited Jan. 3, 2010).

on the shelves. Other DOOH systems air ads triggered by shopper loyalty cards equipped with RFID.[6]

- License plate scanners: In a 2009 advertising pilot, digital billboards along a UK highway displayed personalized advertisements to passing cars. Roadside cameras scanned license plates and ran the numbers through the Driver and Vehicle Licensing Agency. The billboard then displayed the license number and the best type of motor oil for that make and model of car. Public outrage and questions about whether the pilot's use of motor vehicle registration data for marketing violated UK privacy laws led to the pilot's abrupt shutdown.[7]

DOOH uses other technologies, such as GPS, to a lesser extent, and more have potential to combine with DOOH to create interactive experiences for consumers. Clearly DOOH can integrate many technologies to collect a broad range of consumer data in various contexts. Although the privacy recommendations in this document is intended to offer suggestions for present and future DOOH data collection practices, the significant innovation DOOH has shown in the past will likely lead to hitherto unforeseen business models.

The long view: Behavioral advertising on the Internet of Things

The Internet of Things has profound implications for out-of-home targeted marketing. Several sectors are converging to encourage the growth of pervasive computing, including DOOH, location-based services, mobile payment systems, supply chain management, intelligent buildings and security. An extensive digital signage network combined with ubiquitous object tagging would enable advertisers to target personalized, location-based messages to individuals wherever they are.

The "Internet of Things" is a term used to describe a computerized network of physical objects.[8] The network would be supported by an array of sensors and data storage devices embedded in objects, interacting with web services.[9] The

---

[6] Clair Swedberg, *French Jean Boutique Adopts RFID to Boost Loyalty*, RFID Journal, Jul. 11, 2007, http://www.rfidjournal.com/article/articleview/3472/1/1.

[7] Christopher Leake, *Drivers' details sold by DVLA are used in bizarre roadside adverts for Castrol*, Daily Mail, Sep. 27, 2009, http://www.dailymail.co.uk/news/article-1216414/Now-drivers-details-sold-DVLA-used-bizarre-roadside-adverts-Castrol.html.

[8] For a detailed discussion, *see* Int'l Telecomm. Union, *ITU Internet Reports 2005: The Internet of Things* (7th ed. 2005).

[9] One commonly referenced Internet of Things scenario envisions a refrigerator that can monitor the food it stores.[9] The refrigerator could notify the owner when food spoils, download recipes from websites that make use of the food in the fridge, notify the owner of recalls from the manufacturer, or notify the owner of sales of food he or she prefers. Several early versions of this appliance are out on the market. *See* Richard MacManus, *Internet Fridges: State of the Market*, ReadWriteWeb, Jul. 28, 2009 http://www.readwriteweb.com/archives/internet_fridges.php.

first generation Internet of Things is being built on RFID tags and readers, and the related Near Field Communication, but may also use Bluetooth and other technologies that enable communication at a distance. Because these technologies reveal unique numbers or addresses to readers, they are easily associated with the owners of the tagged objects.

Widely deployed, this system would reveal vast amounts of data related to the tagged objects, including location information, environmental conditions and proximity to other objects. Marketers, government or researchers could gather highly detailed data regarding an individual's activities, preferences and habits anywhere the individual goes, not just when an individual is in front of a digital sign.[10] Data aggregators would be able to accumulate the various pieces of data to create a unique profile to serve targeted advertising as individuals passed a digital sign.

An environment in which digital tags and readers are ubiquitous raises difficult issues of transparency, user control over data collection, long-term profiling and location tracking. This dynamic is likely to blur the traditional distinction between privacy in the home and outside the home, particularly if household objects relay data to third parties, which may necessitate a new theory of privacy that encompasses both the home and public places. Even so, as a practical matter, privacy safeguards may be significantly more difficult to implement on the massive scale that a pervasive system of tags, readers and advertising screens would require. The Internet of Things can bring numerous benefits, but unless careful attention is paid to privacy as the system is being built, the Internet of Things can also create a society in which constant targeted advertising and government surveillance diminish quality of life. This will take a commitment to privacy on the part of all the stakeholders in the Internet of Things, including the DOOH industry.

The time is right for a DOOH privacy framework

Using identification and interactivity technologies, the DOOH and mobile industries are taking the Internet experience into the physical world. In doing so, DOOH has established a burgeoning offline version of the behavioral advertising that currently occurs online – the practice of tracking consumers' activities in order to deliver advertising targeted to the individual interests.[11] Deployed to enough locations in digital signage units, such a practice may well be profitable to the industry, just as behavioral advertising has proven profitable on the Internet.

---

[10] As example of an early pervasive tracking system, see the 2008 Cityware research project. Researchers monitored the Bluetooth signals of hundreds of thousands of people without their knowledge in the UK town of Bath. The researchers installed Bluetooth signal receivers in pubs, offices and other public spaces and recorded the collected information in a central database to study how people move in the city. *See* Paul Lewis, *Bluetooth is watching: secret study gives Bath a flavour of Big Brother*, The Guardian, Jul. 21, 2008, http://www.guardian.co.uk/uk/2008/jul/21/civilliberties.privacy.

[11] Federal Trade Commission, FTC Staff Report: *Self-Regulatory Principles for Online Behavioral Advertising*, Pg. 2 (Feb. 2009), http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.

Privacy invasion associated with DOOH is not rampant because only a small percentage of digital signage units have audience measurement, identification or interactive capabilities. However, the industry trend is clearly toward greater adoption of measurement, identification and surveillance capabilities, not less.

The usefulness of audience data to marketers and the increasing cost effectiveness of sophisticated equipment will encourage the DOOH industry to collect detailed consumer data. Interactivity has been named a key driver of digital signage growth in 2010.[12] In January 2010, Intel and Microsoft announced a joint effort to develop DOOH that can emulate the ability of online retailers to identify returning customers and tailor advertisements to them based on their shopping histories.[13] Coordinating online and offline behavioral advertising will be especially natural to companies like Focus Media Holding. Focus Media owns an extensive Internet advertising network and also operates the largest DOOH network in China, with more than 190,000 screens.[14]

Consumers and companies are already wary of the privacy implications of identification and consumer profiling technologies in DOOH. Comments to blog posts and news articles on facial recognition in digital signage indicate many consumers have little faith that DOOH companies will protect consumer data.[15] Some industry figures have said that companies must guarantee consumer privacy,[16] while others have cited privacy issues as an obstacle to using facial recognition technology for advertising purposes.[17] A New York Times article on billboards with facial recognition prompted a major DOOH company to publicly defend its privacy practices.[18] Public backlash and possible violations of existing

---

[12] *Capital Network's Research Identifies Customer Interaction as Key Digital Signage Trend for 2010*, Digital Signage Expo, Dec. 3, 2009, http://www.digitalsignageexpo.net/DNNArticleMaster/DNNArticleView/tabid/78/smid/400/ArticleID/2312/reftab/66/Default.aspx.

[13] Don Clark and Nick Wingfield, *Intel, Microsoft Offer Smart-Sign Technology*, Wall Street Journal, Jan. 12, 2010, http://online.wsj.com/article/SB10001424052748704055104574652742982646768.html.

[14] Focus Media, Company Overview, http://www.focusmedia.cn/en/aboutus/companyoverview.htm (last visited Jan. 3, 2010).

[15] Nilay Patel, *TruMedia says its facial-recognition bilboards will never record video, it won't share with cops* – User Comments, Engadget, Jun. 10, 2008, http://engadget.com/2008/06/10/trumedia-says-its-facial-recognition-billboards-will-never-recor/#comments.

[16] Bill Gerpa, *Digital signage networks must guarantee viewer privacy*, The Digital Signage Insider, Aug. 1, 2008, http://www.wirespring.com/dynamic_digital_signage_and_interactive_kiosks_journal/articles/Digital_signage_networks_must_guarantee_viewer_privacy-569.html.

[17] Digital Signage Expo, Question of the month, Sep., 2009, http://www.digitalsignageexpo.net/Resources/QuestionoftheMonth/September09.aspx.

[18] *TruMedia: Facial Recognition Boards Will Never Record, Share Data*, MediaBuyerPlanner, Jun. 11, 2008,

privacy laws have already led to the discontinuation of some DOOH advertising projects, as with the billboard which scanned UK license plates.

The reaction to smart signs parallels the controversy associated with online behavioral advertising. A 2009 study of consumer attitudes towards behavioral advertising found two-thirds of Americans "definitely would not" allow marketers to track them online, even if the tracking is anonymous.[19] The study also found 90% of young adults reject advertising tailored to them based on offline activities. Consumers repeatedly voice opposition to behavioral tracking for online advertising. Facebook users have revolted several times over uses of their information on Facebook, persuading the social networking site to repeatedly revise its privacy policies and the information management tools it provides to its users.[20]

In 2009, the Federal Trade Commission (FTC) issued self-regulatory guidelines for online behavioral advertising.[21] The soon-to-be Chairman stated the guidelines may be the last clear chance the industry had to show it would effectively protect consumer privacy in the absence of stricter legislation.[22] Congress has held multiple hearings on the issue,[23] and members of Congress

---

http://www.mediabuyerplanner.com/entry/34111/trumedia-facial-recognition-boards-will-never-record-share-data.

[19] Joseph Turow, Jennifer King, Chris Hoofnagle, Amy Bleakly & Michael Hennessy, *Contrary to What Marketers Say, Americans Reject Tailored Advertising and Three Activities that Enable It*, Pg. 3 (Sep. 29, 2009), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214.

[20] David Coursey, *After Criticism, Facebook Tweaks Friends List Privacy Options*, PC World, Dec. 10, 2009, http://www.pcworld.com/businesscenter/article/184418/after_criticism_facebook_tweaks_friends_list_privacy_options.html?loomia_ow=t0:s0:a41:g26:r32:c0.000691:b23490248:z0. *See also* Jessica Vascellaro, *Facebook's About-Face on Data*, The Wall Street Journal, Feb. 19, 2009, http://online.wsj.com/article/SB123494484088908625.html. *See also*, Juan Perez, *Facebook's Beacon More Intrusive Than Previously Thought*, PC World, Nov. 30, 2007, http://www.pcworld.com/article/140182/facebooks_beacon_more_intrusive_than_previously_thought.html.

[21] Federal Trade Commission, FTC Staff Report: *Self-Regulatory Principles for Online Behavioral Advertising*, (Feb. 2009), http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.

[22] *Id.*, Concurring Statement of Jon Leibowitz, Chairman of the FTC, http://www.ftc.gov/os/2009/02/P085400behavadleibowitz.pdf.

[23] *Behavioral Advertising: Industry Practices and Consumers' Expectations: Hearing before the United States House of Representatives Committee On Energy And Commerce Subcomm. On Communications, Technology and the Internet and the Subcomm. On Commerce, Trade and Consumer Protection*, 111th Cong., (Jun. 2009), http://energycommerce.house.gov/index.php?option=com_content&view=article&id=1674:energy-and-commerce-subcommittee-hearing-on-behavioral-advertising-industry-practices-and-consumers-expectations&catid=122:media-advisories&Itemid=55.

have repeatedly called for privacy legislation to regulate how consumer information is collected, used and shared for online marketing.[24]

Given this environment, DOOH companies should proactively adapt their practices to be transparent and minimally intrusive, and to afford consumers control over how their information is collected and used. Incorporating privacy into the fabric of DOOH business models and data management practices is the best way to prevent privacy risks before they arise.[25] It will be less expensive for DOOH companies to integrate privacy controls now, while identification technologies are still relatively new to the industry, than it will be to retrofit privacy protections onto existing systems. How DOOH companies handle the privacy issues they face today will affect the way the public, regulators and advertisers perceive the industry, as well as the industry's direction in the future. The industry should prove its dedication to privacy protection to reduce the risk that the public will consider interactive DOOH a disrespectful intrusion.

POPAI, a trade association, recently released a first generation set of privacy guidelines for the industry.[26] POPAI's Code of Conduct is an excellent start for industry self-regulation. In particular, the Code's section on cross-channel and cross-domain marketing contains several good privacy protections, such as the requirement that a consumer re-opt in each time he or she enters a new venue where cross-domain marketing takes place.[27] However, the Code does not articulate a full set of Fair Information Practices, nor does it suggest DOOH companies establish a comprehensive privacy framework. The POPAI Code is a sound foundation for the DOOH industry, but the industry should not limit itself to the Code's recommendations.

Protection should go beyond directly identifiable information

Some privacy protection frameworks, including many industry guidelines, typically extend only what was traditionally considered "personally identifiable information" (PII). PII was thought to include only information that can be directly linked to an individual's identity. However, it is increasingly being realized that the distinction between PII and non-PII is becoming much less meaningful in light of data analytic capabilities. Researchers have demonstrated that individuals can

[24] Rep. Rick Boucher, *Behavioral ads: The need for privacy protection*, The Hill, (Sep. 24, 2009, http://thehill.com/special-reports/technology-september-2009/60253-behavioral-ads-the-need-for-privacy-protection.

[25] For more detailed discussion of the "Privacy By Design" concept, see Center for Democracy & Technology, *The Role of Privacy by Design in Protecting Consumer Privacy*, Dec. 21, 2009, http://www.cdt.org/content/role-privacy-design-protecting-consumer-privacy.

[26] POPAI Digital Signage Group, *Best Practices: Recommended Code of Conduct for Consumer Tracking Research*, http://www.popai.com/pdf/2010dscc.pdf (last visited Feb. 7, 2010).

[27] See POPAI Code, Pgs. 8-9.

still be identified from records stripped of traditional identifiers.[28] The FTC supports extending privacy protection to information beyond that which only directly identifies individuals.[29]

Therefore, the best approach for companies is to evaluate all the data they collect on a spectrum ranging from directly identifiable to "pseudonymous" to aggregated, providing different levels of privacy protection corresponding to the sensitivity of the information involved.[30]

Directly identifiable data includes what was once referred to as PII:

- Name
- Address
- Telephone number
- Date of birth
- Social Security Number
- Driver's license number
- License plate number
- Email address
- Bank, credit card, or other account number
- Biometric data, such as unique data points captured via facial recognition systems
- Images of individuals.

In addition to directly identifiable data, companies should extend protection to any data that could reasonably be associated with a particular consumer or a particular consumer's property, such as a smart phone or other device.[31]

The term "*pseudonymous data*" refers to information associated with a unique identifier. Although pseudonymous data does not directly identify an individual, pseudonymous data can be traced to an individual's identity with relative ease. This type of data includes, but is not limited to

- RFID codes: RFID chips frequently come with a uniquely identifiable number, which can individualize any property to which the chip is attached.
- Device identification numbers, such as IP address, Mac address, Bluetooth number, Near Field Communication number, International Mobile Equipment Identity number.

---

[28] *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization* (August 2009), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006.

[29] Federal Trade Commission, FTC Staff Report: *Self-Regulatory Principles for Online Behavioral Advertising*, Pgs. iii, 21-22 (Feb. 2009), http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.

[30] See Center for Democracy & Technology, *Threshold Analysis for Online Advertising Practices*, Pg. 17 (Jan. 2009), http://www.cdt.org/privacy/20090128threshold.pdf.

[31] Federal Trade Commission, FTC Staff Report: *Self-Regulatory Principles for Online Behavioral Advertising*, Pgs. 28-31 (Feb. 2009), http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.

- Internet username, such as the name with which one uses to posts to a discussion forum.
- Social networking data, including login information and friend lists.
- User-generated data: data generated knowingly by an individual, such as search terms, posts in discussion forums and data input into social networking profiles.

Whether a data element will reasonably identify an individual will depend on the context in which the data was collected. When determining the privacy practices necessary for handling pseudonymous data, companies should consider the availability of other data sets.[32] An individual's identity may be reasonably inferred by combining pseudonymous data with, for example, records of purchases from credit or loyalty cards, security surveillance systems, or aggregated location data which reveals unique habits or travel patterns.

Aggregate data includes information about multiple individuals that cannot reasonably be used to directly identify or infer the identity of a single individual. The most prominent example of this in DOOH may be facial qualification, where the demographics of individuals passing by a digital sign are compiled over time, but unique biometric data points and images of individuals are not saved. Even though aggregate data may not be directly identifiable or re-identifiable, companies should incorporate privacy practices – particularly transparency – into their collection of such data. Many consumers object to covert behavioral targeting even if it is done on an "anonymous" or aggregate basis.[33]

Policy Framework and Models

Privacy standards for DOOH should be based on the widely accepted Fair Information Practices (FIPs). These internationally recognized principles are reflected (although often incompletely) in many privacy laws in the U.S. and are also the basis of more comprehensive privacy laws internationally, such as the European Union's Data Protection Directive. Recently, the U.S. Department of Homeland Security adopted a modern and comprehensive formulation of these principles.[34] CDT has recommended DHS' formulation of the FIPs to the FTC as the basis for addressing online behavioral advertising, and we believe it is equally well-suited as the basis for privacy guidelines for the DOOH industry. These are the FIPs as set forth by DHS:

- Transparency

---

[32] *See, e.g.,* Bradley Malin and Latanya Sweeney, *How (Not) to Protect Genomic Data Privacy in a Distributed Network: Using Trail Re-identification to Evaluate and Design Anonymity Protection Systems*, Journal of Biomedical Informatics 37 (2004), 179-192.

[33] Joseph Turow, Jennifer King, Chris Hoofnagle, Amy Bleakly & Michael Hennessy, *Contrary to What Marketers Say, Americans Reject Tailored Advertising and Three Activities that Enable It*, Pg. 3 (Sep. 29, 2009), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214.

[34] Department of Homeland Security, *The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security* (Dec. 2008), http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

- Individual Participation
- Purpose Specification
- Data Minimization
- Use Limitation
- Data Quality and Integrity
- Security
- Accountability

The online behavioral advertising industry has partially incorporated the FIPS into various self-regulatory guidelines. These include the guidelines issued by the Network Advertising Initiative and by the Interactive Advertising Bureau. However, as CDT has pointed out, the guidelines of the online advertising industry fall short in key areas, so the DOOH industry should not merely mimic them.[35] Nevertheless, the industries share the practice of targeting advertisements to consumers based on their activities. This makes it worthwhile for DOOH companies to familiarize themselves with the privacy frameworks of their online counterparts.

DOOH companies and their affiliates may also find relevance in existing frameworks for the technologies they use. For example, DOOH companies that utilize mobile marketing should use the Mobile Marketing Association (MMA)'s Global Code of Conduct as a baseline on which to build.[36] Similarly, DOOH companies that use RFID should integrate the standards of relevant trade associations or privacy groups.[37] None of these frameworks is perfect, and some are deficient in certain areas, but they may serve as a starting point for companies to develop their own policies.

With reference to existing models, and drawing on the comprehensive DHS framework, CDT recommends that the DOOH industry develop a privacy framework along the following lines:

1) Transparency

DOOH data collection and use should be transparent. Generally, there are two important ways for DOOH companies to do this. First, DOOH companies should develop privacy policies and publish them on their websites. Second, DOOH companies should give consumers notice at the location in which the DOOH unit is placed. Transparency through notice and a public privacy policy is the

---

[35] Center for Democracy & Technology, *Online Behavioral Advertising: Industry's Current Self-regulatory Framework is Necessary, But Still Insufficient On Its Own to Protect Consumers*, Dec. 7, 2009, http://www.cdt.org/report/online-behavioral-advertising-industrys-current-self-regulatory-framework-necessary-still-ins.

[36] Mobile Marketing Association, *Global Code of Conduct* (Jul. 2008), http://www.mmaglobal.com/codeofconduct.pdf.

[37] Center for Democracy & Technology Working Group on RFID, *Privacy Best Practices for Deployment of RFID Technology*, May 1, 2006, http://old.cdt.org/privacy/20060501rfid-best-practices.php. *See also* Electronic Privacy Information Center, *Guidelines on Commercial Use of RFID Technology*, Jul. 9, 2004, http://www.epic.org/privacy/rfid/rfid_gdlnes-070904.pdf.

responsibility of not just the technology vendors, which are unfamiliar to consumers, but also the digital signage network operators and the owners of the establishments at which the signage is located.

a) Privacy Policies

Privacy policies serve an important role. Internally, the process of developing a privacy policy forces a company to assess its data collection practices and develop rules for the custodianship of the data it collects. A privacy policy should describe in concise, specific terms

- What consumer data is collected,
- How the data is collected,
- The purposes for which the data is used,
- With whom the data is shared,
- How the data is protected,
- How long the data is retained, and
- The choices that consumers have with respect to their data.

Once the policy is set, data should not be collected, shared or used in any way contrary to the published privacy policy.[38] In some cases, the data management practices of the DOOH company may overlap with the practices of another company, such as when DOOH integrates with mobile marketing or social networking applications. The DOOH privacy policy should underscore how these services interact.

Numerous DOOH companies already publish privacy policies. For example, some of the policies of companies using facial recognition state they do not retain images or identify individuals.[39] Similarly, some companies that integrate digital signage and social networking publish privacy policies.[40] However, existing policies vary greatly in detail, and not all DOOH services specify what they do with personal information.[41] A privacy policy alone is not enough, however, and

[38] The FTC considers a material violation of a published privacy policy to constitute an unfair and deceptive trade practice prohibited under the Federal Trade Commission Act. 15 U.S.C. 45(a)(2). See also Mark Foley, *The FTC's Web Site Privacy and Security Rules for Every Business*, Wisconsin Lawyer, (Mar. 2008), http://www.wisbar.org/AM/Template.cfm?Section=Wisconsin_Lawyer&template=/CM/ContentDisplay.cfm&contentid=70438.

[39] Cognovision, Privacy Policy, Sep., 2007, http://cognovision.com/privacy.php.

[40] LocaModa, Privacy Policy, http://locamoda.com/legal/privacy_policy (last visited Jan. 3, 2010).

[41] See e.g., The Marketplace Station, Privacy Policy, http://www.themarketplacestation.com/privacy.html (last visited Feb. 7, 2010). The policy makes no reference of the data collection systems integrated into some of Marketplace Station's screens. See *Cognovision integrates with BroadSign for automated digital signage campaign analytics*, Digital Signage Today, Apr. 17, 2009, http://www.digitalsignagetoday.com/article.php?id=22115.

many consumers confuse the mere existence of a policy with substantive privacy protections.[42]

b) Notice

At present, most DOOH companies are completely unknown to consumers, so consumers are unlikely to look for the privacy policies posted on the websites of DOOH companies. Even if consumers come to know the names of DOOH companies, current practices give consumers little hint as to what company is responsible for a given DOOH display. The challenge for the industry is to find a way to present meaningful notice at the point of data collection. Such notice is fundamental to transparency and individual participation.

Consumers should be given clear, prominent notice of DOOH media units that collect consumer data at the physical location in which the unit operates. To the extent possible, the notice should appear conspicuously on or close to each DOOH unit that is collecting the information.[43] One notice should not cover, for example, an entire supermarket, but instead should be at each sensor and associated DOOH screen within the supermarket. There should be no hidden receivers, cameras or sensors used exclusively for marketing.

Generic notices like "These premises are under video surveillance" are not sufficient. Consumers have come to assume such notices to relate to security measures, not marketing. Such notices do not provide accurate notification of the more comprehensive data collection, sharing and usage associated with marketing. If a DOOH unit is used for both security and for marketing, or if security information is used for marketing, the notice (and privacy policy) should clearly disclose this.

CDT conceptualizes three tiers of notice. At minimum, DOOH companies could adopt a symbol to place on signage units, such as on a small placard or appearing on the screen alongside content. The symbol should identify the unit as one that collects some form of consumer data. This approach works best if the symbol is adopted on an industry-wide basis and tested to ensure real consumers understand what it means. The online behavioral advertising industry is adopting this approach. Many online ads that use demographic and behavioral data will include a certain symbol and phrases like "Why did I get this ad?". An Internet user who clicks the symbol or phrase will receive an explanation of the how the ad was targeted to him or her.[44] Similarly, if DOOH units include only

[42] Joseph Turow, Chris Hoofnagle, Deirdre Mulligan, Nathaniel Good, Jens Grossklags, *The FTC and Consumer Privacy in the Coming Decade*, Pg. 2 (Nov. 8, 2006), http://www.ftc.gov/bcp/workshops/techade/pdfs/Turow-and-Hoofnagle1.pdf.

[43] The POPAI Code permits one notice to cover one establishment. See POPAI Code of Conduct, Pg. 8. However, CDT believes a notice should be provided at each screen. One discreet notice in an isolated location within a large retail store full of labels competing for consumers' attention is insufficient to provide notice for a DOOH network collecting data throughout the store.

[44] Stephanie Clifford, *A Little 'i' to Teach About Online Privacy*, New York Times, January 26, 2010, http://www.nytimes.com/2010/01/27/business/media/27adco.html.

symbols as notice, a comprehensive notice should also be placed elsewhere in the establishment.

The second tier of notice that could be placed on the DOOH unit would identify the company who owns or operates the unit, inform consumers of what information is being collected. Again, there should be a comprehensive notice elsewhere in the establishment. The third tier is a comprehensive notice that includes the above information, and also the purposes for which the information is being used, with whom the information is shared, what other consumer data will be combined with the information and, if applicable, the choices consumers have with respect to the information being collected.

In cases where DOOH units interact with consumers' devices, such as with smart phones via Bluetooth, a comprehensive notice should also be delivered directly to the consumers' devices. This should be the norm when the DOOH unit or the consumer initiates the interaction.

2) Individual Participation

The FIPs principle of "individual participation" embodies two concepts: the right to consent to the collection and use of data and the right to access to data that has been collected about oneself. The robustness of the individual participation protocol required varies depending on the sensitivity and identifiability of the information collected and the use to which it is put. Similarly to the POPAI Code, CDT conceptualizes DOOH audience measurement and interactive marketing as occurring on general three levels:

- Level I: *Audience counting*. Information related to consumers is gathered on an aggregate basis and not used for tailoring advertisements. No retained information, including images, links to individuals or their property. Example: facial recognition systems that track gazes or record passerby demographics, but do not store facial images or contextualize ads.

- Level II: *Audience targeting*. Information related to consumers is collected on an aggregate basis and is used for tailoring contextual advertisements to individuals. No retained information, including images, links to individuals or their property. Example: facial recognition systems that record passerby demographics and contextualize ads accordingly.

- Level III: *Audience identification and/or profiling*. Information related to consumers is collected on an individual and aggregate basis and is used for tailoring advertisements. Information linked to individual identity or an individual's property (such as a mobile phone) is retained. Example: using DOOH networks for social networking, RFID tracking, mobile marketing.

a) Consent

Consumers should have a ready means to choose whether their data is collected for advertising purposes. The means will differ between DOOH systems and services. Levels I and II should implement opt-out consent. At minimum, opt-out consent can be accomplished via notice by giving consumers an opportunity to avoid a particular DOOH unit. Level III requires opt-in consent, which should be issued after the consumer has the opportunity to examine the applicable privacy policy.

Consumers should be able to exercise control over what information is collected, which marketing messages they receive, and which other companies and parties may see the data. The consent should be persistently honored until the consumer alters his or her choice, and the consent should also be revocable at any time. To the extent possible, opt-in consent protocol should be granular without also being confusing to consumers. One way to strike this balance is to offer various privacy control options, but to also offer an easy means to opt-out or opt-in to all the choices at once.

b) Access

Consumers should have the ability to view and correct any directly identifiable data collected about them for DOOH marketing. Consumer confidence in an organization may be vastly improved if individuals have access to their own data, whereas consumers will perceive surveillance and data analysis behind closed doors as considerably more intrusive.

3) Purpose Specification,

The purpose specification principle requires a company to think through its data collection and use practices and to specify how the company intends to use the data it is collecting. The purposes to which consumer data will be put should be only specified not later than at the time of collection. Properly applied, the principle should lead companies to minimize the collection of unnecessary data, which is the next principle.

4) Data Minimization

Through privacy policies and guidelines, individual companies and the DOOH industry as a whole should commit to limit their data collection and retention to only the minimum necessary to achieve specified ends.

DOOH companies should collect and use the minimum amount of consumer data necessary to deliver their services. For example, there is no need to use a license plate number when a car's make and model will do.[45] In most cases, it may not be necessary to retain consumer data for future use beyond the delivery of a contextual advertising message. For example, there is no need to maintain persistent records of phone numbers or Bluetooth addresses when a company

[45] Christopher Leake, *Drivers' details sold by DVLA are used in bizarre roadside adverts for Castrol*, Daily Mail, Sep. 27, 2009, http://www.dailymail.co.uk/news/article-1216414/Now-drivers-details-sold-DVLA-used-bizarre-roadside-adverts-Castrol.html.

does not seek an ongoing relationship with the individuals associated with that data. When a DOOH company does retain consumer information, that retention should last no longer than is needed to serve the purpose for which it was collected, as specified in the privacy policy.[46] If a consumer opts-out or cancels a service, the associated information should be destroyed.

5) Use Limitation

Consumer data should not be shared for any uses that are incompatible with the purposes specified in the company's privacy policy. Transfers of consumer data to any third parties or affiliates should be transparent, specified in advance to consumers and may require opt-in consent.[47]

6) Data Quality & Integrity

DOOH companies should, to the extent practicable, ensure consumer data they collect is accurate, relevant, timely and complete. Allowing consumers to access and edit data collected about them is one of the best mechanisms for ensuring data quality and integrity.

7) Security

DOOH companies should exercise reasonable and appropriate efforts to secure information collected about consumers. In so doing, a company should maintain a standard information security program appropriate to the amount and sensitivity of the information stored on its system. Such a security program should include processes to identify and address reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of information.

The nature and extent of security required will largely depend on what kind of collection technology is employed and what consumer data is retained. Unnecessary consumer data should be destroyed via secure methodologies. The best data security is for a company not to possess consumer data in the first place.

8) Accountability

There has been substantial criticism of self-regulation of the behavioral advertising industry because of a lack of accountability for noncompliance. DOOH companies who collect and use consumers' information should establish internal accountability mechanisms. These mechanisms should ensure strict compliance with companies' privacy policies, as well as laws and other applicable privacy protection requirements. Companies should provide privacy and security training to all employees, contractors and affiliates who collect and

[46] The POPAI Code recommends that image or biometric data "should be stored for up to 3 months or the maximum period allowed by law." *See* POPAI Code of Conduct, Pg. 6. It is unclear whether POPAI means that the data should be stored *no longer than* that period, or whether POPAI recommends that the data be stored regardless of whether there is a business need for it, so long as the law allows it.

[47] See POPAI Code of Conduct, Pgs. 8-9.

use consumers' information. There should be meaningful penalties for violations, especially willful or chronic noncompliance.

The DOOH industry may also consider empowering one or more trade associations with independent oversight functions to monitor compliance and offer privacy management guidance for individual companies. The organization that takes on these functions should provide a dispute resolution forum for consumers and articulate clear benchmarks for companies to evaluate the efficacy of their privacy practices.

For more information, please contact

Harley Geiger
Staff Attorney, CDT
202-637-9800 x 316
harley@cdt.org

CDT wishes to thank Melissa Ngo of Privacy Lives (www.privacylives.com) for her consultation and contributions to this report.