Safeguarding Privacy in the Digital Signage Industry

March 31, 2010
Tags: Array
Policy Posts are in-depth analyses on current tech policy issues from CDT experts. Sign up to receive the latest Policy Posts here:

---

1) CDT issues report and recommendations for digital signage privacy

CDT released a report on consumer privacy and digital signage entitled Building the Digital-Out-Of-Home Privacy Infrastructure. CDT's report includes a set of recommendations for safeguarding privacy as the digital out-of-home (DOOH) industry continues to adopt identification and interactivity technologies, such as facial recognition, mobile marketing, social networking, RFID tracking and license plate scanners.

CDT believes consumer privacy controls are essential for digital signage advertising to maintain consumer trust, which in turn is crucial if the industry is to continue growing at its current explosive pace. Unless the industry adopts robust self-regulation, it is likely to face consumer backlash and reactive government regulation that may stifle innovation. It will only take a few bad apples that flout consumer privacy expectations to spoil the image of the whole industry.

CDT's comprehensive digital signage privacy recommendations are based on the widely accepted Fair Information Practices (FIPs [1]). CDT's report marks the first time a full set of FIPs were applied to the digital signage medium. Incorporating privacy into the fabric of DOOH business models and data management practices is the best way to prevent privacy risks before they arise. Because digital signage identification technologies are still in their early stages, the DOOH industry has the opportunity to incorporate privacy by design [2]. It will be easier and less expensive to integrate privacy controls now than to bolt them 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.

POPAI, a trade association, recently released a first generation set of privacy guidelines for the industry. POPAI's Code of Conduct is an excellent start for industry self-regulation. However, the Code does not articulate a full set of FIPs, 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.

In-depth resources on privacy protection are now readily available to DOOH companies through the work of organizations like CDT, POPAI and World Privacy Forum. What remains is for the digital signage industry as a whole to apply comprehensive privacy safeguards to their business practices

CDT's report on digital signage privacy [3]

CDT blog posts on digital signage [4]
POPAI Code of Conduct [5]

Word Privacy Forum digital signage privacy principles [6]

---

2) What is digital signage?

Digital Out-Of-Home (DOOH [7]), also known as digital signage or "smart signs," is a communications

medium characterized by a dynamic display presenting messages in a public environment. 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.

DOOH has rapidly grown into a multibillion-dollar industry over the past decade. Despite the economic downturn, industry forecasts [8] predict growth at double-digit rates for the next 3-5 years. There were an estimated [9] 630,000 displays in the United States in 2007, though there are many more worldwide, particularly in China.

The DOOH industry is exploring several technologies to 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: 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.

Social networking: Some DOOH units provide access to social networks like Facebook, Twitter and Flickr through the Web or apps on consumers' mobile devices.

Radio Frequency Identification (RFID): Some systems use RFID-enabled shelves to prompt nearby digital signage units to display advertisements related to the products on the shelves, while other DOOH systems [10] air ads triggered by shopper loyalty cards equipped with RFID.

Using identification and interactivity technologies, DOOH has established a burgeoning offline version of the behavioral advertising [11] that currently occurs online – the practice of tracking consumers' activities in order to deliver advertising targeted to the individual interests. Privacy invasion associated with DOOH is not rampant at present 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. It is reasonable to presume that one day the DOOH industry will routinely identify individuals for the simple reason that it will be profitable to do so.

---

3) Privacy Standards

Privacy standards for DOOH should be based on the widely accepted Fair Information Practices (FIPs). CDT recommends the modern formulation of the FIPs issued [1] by the Department of Homeland Security.

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 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 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.

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. 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.

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.

At minimum, opt-out consent can be accomplished via notice by giving consumers an opportunity to avoid a particular DOOH unit. However, explicit opt-in consent should be required when DOOH units collect information linked to individual identity or an individual’s property (such as a mobile phone). Affirmative consent should be issued only after the consumer has the opportunity to examine the applicable privacy policy.

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.

Purpose Specification
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.

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 the minimum amount of consumer data necessary to fulfill their specified purposes. When a company does not seek an ongoing relationship with the individuals associated with that data, it may not be necessary to retain consumer data for future use beyond the delivery of a contextual advertising message. 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. If a consumer opts-out or cancels a service, the associated information should be destroyed.

Use Limitation
Consumer data should not be used or shared in any way incompatible with the protections and purposes specified in the company’s privacy policy.

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.

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. 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.

Accountability
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 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.

-
- digital signage

Links:
[1] http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf
[2] http://www.cdt.org/content/role-privacy-design-protecting-consumer-privacy
[3] http://www.cdt.org/report/framework-digital-signage-privacy
[4] http://www.cdt.org/search/node/%22digital%20signage%22
[5] http://www.popai.com/pdf/2010dscc.pdf
[6] http://www.worldprivacyforum.org/pdf/DigitalSignage-principlesfs.pdf
[7] http://www.digitalsignageresource.com/digital-signage-glossary-of-terms.asp?modes=3&col=term&term=digital_signage
[8] 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
[9] http://www.capv.com/public/Content/Press/2007/06.06.2007.html
[10] http://www.rfidjournal.com/article/articleview/3472/1/1
[11] http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf