DIGITAL SIGNAGE FEDERATION
Digital Signage Privacy Standards

February 2011

Introduction

Interactivity and consumer engagement are poised to be key drivers of growth for the digital signage industry. Through technologies and platforms like mobile marketing, social networking, facial recognition and radio frequency identification, digital signage companies can personalize message content, build customer relationships, streamline network management and provide accountability to advertising clients. However, some companies and consumers are understandably wary of the privacy implications of collecting personal information through these identification and interactivity technologies.

The Digital Signage Federation (DSF) believes the time is right for an industry-wide commitment to strong privacy and transparency standards. Such standards can help preserve public trust in digital signage and set the stage for a new era of consumer-friendly interactive marketing. Incorporating privacy into digital signage business models and data management practices is the best way to prevent privacy risks before they arise. It will likely be less expensive for digital signage 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 future systems. How digital signage companies handle the privacy issues they face today will affect the way the public, regulators and advertiser clients perceive the industry – as well as the industry's direction in the future.

The following are voluntary privacy guidelines recommended by DSF for digital signage companies, their partners and the venues that host these systems. The issues discussed in these guidelines are related to data collection and use through digital signage – these guidelines do not seek to address the many other methods of collecting consumer information. The DSF Digital Signage Privacy Standards are a living document and should be updated as technology and business practices evolve. Although DSF endorses these guidelines, DSF does not endorse specific companies, products, or services that use these guidelines. The DSF Digital Signage Privacy Standards do not replace legal obligations, and companies should always make certain that they are in compliance with the law at all times.

Types of information covered by the DSF Digital Signage Privacy Standards

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, the distinction between PII and non-PII is becoming much less meaningful in light of data analytic

capabilities.[1] DSF recommends that companies provide privacy protections that correspond to the sensitivity of the information they maintain.[2] For example, companies should obtain consumers' opt-in consent before collecting directly identifiable or pseudonymous data.

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 or voice recordings of individuals.

In addition to directly identifiable data, companies should extend privacy protection to *pseudonymous data* – 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, or any other unique identifier.[3] Although pseudonymous data do 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.
- 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.

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

---

[1] Researchers have demonstrated that individuals can still be identified from records stripped of traditional identifiers. *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.

[2] The Federal Trade Commission supports extending privacy protection to information beyond that which only directly identifies individuals. 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.

[3] *Id.*, Pgs. 28-31.

in digital signage may be facial recognition systems that compile the demographics of individuals passing by a digital sign over time, but do not save unique biometric data points and images of those individuals. Even though opt-in consent is not required for collecting aggregate data, companies should still be transparent about their data collection (through privacy policies and notice, discussed below).[4]

Digital signage companies should not knowingly collect directly identifiable, pseudonymous, or aggregate data on minors (under 13 years of age, or as defined by state law).

Drawing from Other Standards and Models

DSF recommends that digital signage companies and their affiliates familiarize themselves with existing privacy guidelines related to technologies they use and services they provide. None of these frameworks is perfect – so companies should not merely mimic them – but these guidelines may serve as additional resources for companies developing their own policies.

For example, digital signage companies that utilize mobile marketing should use the Mobile Marketing Association (MMA)'s Global Code of Conduct as a baseline on which to build their own privacy practices.[5] Similarly, digital signage companies that use RFID should integrate the standards of relevant trade associations or privacy groups.[6] Digital signage companies that target advertisements to consumers based on their activities may want to consider the online behavioral advertising guidelines issued by the Network Advertising Initiative and by the Interactive Advertising Bureau.[7] Finally, digital signage companies should be aware of other digital signage privacy guidelines, including the very well done Code of Conduct issued by Point of Purchase Association International.[8]

---

[4] Many consumers object to covert behavioral targeting even if it is done on an "anonymous" or aggregate basis. *See* 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.

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

[6] 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.

[7] Network Advertising Initiative, *NAI Principles* (2008), http://www.networkadvertising.org/networks/principles_comments.asp. Interactive Advertising Bureau, *Privacy Principles* (Feb. 2008), http://www.iab.net/iab_products_and_industry_services/1421/1443/1464.

[8] Point of Purchase Association International, *Best Practices: Recommended Code of Conduct for Consumer Tracking Research* (Feb. 2010), http://www.popai.com/docs/DS/2010dscc.pdf.

Fair Information Practices for Digital Signage

The DSF Digital Signage Privacy Standards are based on the widely accepted Fair Information Practices (FIPs). These internationally recognized principles are incorporated in many privacy laws in the U.S., as well as the European Union's Data Protection Directive. In 2008, the U.S. Department of Homeland Security (DHS) adopted a modern formulation of these principles.[9] These are the FIPs as set forth by DHS:

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

1) Transparency

Digital signage data collection and use should be transparent. Generally, there are two important ways for companies to do this. First, companies should develop privacy policies and publish them on their websites. Second, digital signage companies should give consumers notice at the location in which the signage 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 Policies

Companies should publish privacy policies to their websites, even if they collect nothing but aggregate data. 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,
- With what information the collected data is combined (such as credit receipts, purchases, or third party marketing data),
- How the data is protected,
- How long the data is retained,
- The choices consumers have with respect to their data, including how they may opt-in or -out of the information collection, and
- The company's point of contact for consumer feedback.

[9] 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.

Once the policy is in place, companies should not collect, share, or use data in any way contrary to the published privacy policy.[10] In some cases, the data management practices of the digital signage company may overlap with the practices of another company, such as when digital signage integrates with mobile marketing or social networking applications. The company's privacy policy should underscore how these services interact and, if applicable, explain the point at which the consumer's data becomes subject to a different company's privacy policy.

b) Notice

Companies should provide consumers with clear, meaningful notice of digital signage units collecting consumer data at the physical location in which the unit operates, even if the company collects nothing but aggregate data.[11] Notice should be provided prior to collecting consumer data. Such notice is fundamental to transparency and consumer awareness. The precise manner in which companies provide notice may differ based on physical environment, equipment and other factors, but DSF envisions two layers of notice: a notice at the entrance of the data collection area and a notice on digital signs that collect consumer data.

First, companies should provide a notice near the entrance of a data collection area (i.e., in the breezeway of a supermarket using digital signs that record age and gender). This is to alert the consumer that data collection is occurring prior to the consumer entering the area.[12] The notice need not be large, but it should be easily readable to consumers.

Second, DSF recommends displaying a notice on or near each digital signage screen associated with consumer data collection. This notice can be a static physical sign, such as a small placard. Alternatively or in addition, the notice can also be mixed in intermittently with the media content. If the notice appears intermittently, it should remain on screen long enough for consumers to read it.

- For standalone signage units, an intermittent notice message should preferably be displayed an equal number of times to the network ID interstitial – the message that identifies the digital signage network or operator. However, if the network ID occurs less than four times an hour (or not at all), a physical sign should be used. Alternatively, the notice could be displayed once per average consumer dwell time – the time the consumer spends near the unit.

- If multiple screens are networked together in one location, another option would be to display the notice once per average consumer trip. Here the goal would be to display

[10] 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).

[11] If the digital signage system in a given location is not used to collect consumer information, this notice may not be necessary.

[12] This alone would be insufficient because consumers often do not observe signs like these (i.e., the max capacity sign in a supermarket), which can defeat the point of the notice. If consumers don't observe the notice, they don't perceive the data collection as transparent and there is no positive effect on consumer trust. Hence, DSF recommends the second layer of notice – on the digital signs themselves – to give consumers an additional opportunity to become aware of the data collection.

the notice on multiple screens simultaneously at least once during the average time a consumer spends in the data collection area.

In addition, the operators of the establishment in which the unit is located should maintain an on-site hard copy of the digital signage company's full privacy policy.[13]

The notice message should – at minimum – describe

- What information the location's digital signage system collects,
- For what purpose the information is used,
- Whether any directly identifiable or pseudonymous information is combined with other data, such as purchases or third party marketing data, and
- How the consumer may access the privacy policy of the digital signage unit operator (such as the company's website).

Therefore, a typical notice message might read: *This Company Name digital sign uses a camera to estimate your age and gender in order to make advertisements more relevant to you. No images or identifying information about you is collected or stored. For more information, please visit www.companyname.com/privacy or see the store manager.*

Generic notices like "These premises are under video monitoring" are not sufficient. Such notices do not provide accurate notification to consumers that the data is collected, used and disclosed for marketing. The notice (and privacy policy) should clearly disclose whether any security video footage is used for marketing.

In cases where signage units interact with consumers' devices, such as with smart phones via Bluetooth, DSF recommends that a notice be delivered to or displayed on the consumers' devices. This should be the norm when the digital signage unit or the consumer initiates the interaction.

Digital signage companies should ensure their notices meet Americans with Disabilities Act (ADA) requirements.

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.

DSF conceptualizes digital signage audience measurement and interactive marketing as occurring on three general levels:

[13] Since most companies' privacy policies are online, most consumers are likely unable to access them in the store. Also, consumers without an Internet connection should have the opportunity to read the privacy policy elsewhere. Keeping a hard copy in the establishment in which the sign is located is the most practical way for consumers to easily access the privacy policy offline.

- Level I: *Audience counting*. Information related to consumers is gathered on an aggregate basis, but are not used for tailoring advertisements in real time (i.e., as the consumer walks by the sign). No retained information, including images, links to individuals or their property.
    - Example: facial recognition systems that only track gazes or record passerby demographics, but do not tore facial images or unique biometric data points. The advertisements are not tailored to demographics in real time.

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

- Level III: *Audience identification and/or profiling*. Information related to consumers is collected on an individual basis, regardless of whether or when the information is used to tailor advertisements. Information is retained that links to individual identity, unique travel or purchase patterns, or an individual's property (such as a mobile phone).
    - Example: combining a digital signage system with social networking, RFID tracking, mobile marketing.
    - Example: combining a digital signage system with credit card receipts, online browsing habits, purchases, or third party marketing data.

a) Consent

Consumers should have a ready means to choose whether their data is collected for advertising purposes. The precise means will differ between signage systems and services, but the consent should be persistently honored until the consumer alters his or her choice. The consent should be revocable at any time and consumers should have a readily accessible, inexpensive means of revoking consent.

- Levels I and II should implement opt out consent. At minimum, opt-out consent can be accomplished via notice. Notifying consumers that a particular signage unit collects information gives consumers the opportunity to avoid that signage unit.

- Level III requires opt-in consent, which should be issued after the consumer has the opportunity to examine the applicable privacy policy.
    - A consumer's opt-in consent should not be treated as opting into a distributed digital signage network. Rather, the consumer's opt-in consent should apply only to the physical location for which the consumer provides that consent. Digital signage systems that identify or profile consumers should therefore obtain opt-in consent from the consumer at each new location before collecting data from those consumers.

    - When digital signage companies have ongoing marketing relationships with consumers, the companies should allow consumers to exercise control over

what information is collected, which marketing messages they receive and which other companies and parties may see the data.

b) Access

Digital signage companies should designate an internal point person to receive and process consumer complaints and respond to questions. Companies should specify, in their privacy policies, a ready and inexpensive means for consumers to submit questions, complaints and requests to access their data. Ideally, consumers should have the ability to view and/or correct any directly identifiable data collected about them for digital signage marketing.

3) Purpose Specification

In their privacy policies, companies should specify how they intend to use the consumer data they collect. The purposes to which the data will be put should be 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

Companies should limit their data collection and retention to only the minimum amount they need to achieve specified ends. 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 does not seek an ongoing relationship with the individuals associated with that data.

When a digital signage 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. As a default, companies should not retain the data they collect longer than 30 days. If a consumer opts-out or cancels a service, the directly identifiable and pseudonymous information associated with that consumer 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 should generally be done only if the consumer has provided opt-in consent.

DSF strongly recommends against using the same data collection or storage system for both in-store security and marketing.

6) Data Quality & Integrity

Companies should, to the extent practicable, ensure consumer data they collect is accurate, relevant, timely and complete. Allowing consumers to access and edit identifiable data about them is one of the best mechanisms for ensuring data quality and integrity. Companies should establish a consumer complaint process that enables consumers to dispute inconsistencies in collected information and to notify the company if the consumers' consent choices are not being honored.

7) Security

Digital signage 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.[14] 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. Collected consumer data should be accessible only to those company employees who must use the data to perform their job functions.

The nature and extent of security required will largely depend on what kind of collection technology is employed and what consumer data is retained. However, no collected data, including aggregate data, should be unprotected. 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

Digital signage 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 maintain a written procedure for processing and responding to consumer complaints. Companies should provide privacy and security training to all employees, clients, contractors and affiliates who collect, access and use consumers' information. There should be meaningful penalties for violations, especially willful or chronic noncompliance.

Please direct any questions regarding these standards to the Digital Signage Federation: www.digitalsignagefederation.org.

[14] See, i.e., Payment Card Industry Security Standards Council, https://www.pcisecuritystandards.org.