A Framework for Digital Signage Privacy

Harley Lorenz Geiger
Policy Counsel, Center for Democracy & Technology (CDT)

Abstract: Privacy controls are essential for digital signage to maintain consumer trust as the medium continues to assimilate identification and interactivity technologies. Unless the industry adopts robust self-regulation, it is likely to face consumer backlash and reactive government regulation that may stifle innovation. The digital out-of-home industry as a whole should commit to comprehensive privacy standards based on the Fair Information Practices. A set of model standards is presented in this article.

1. Introduction

Digital signage, also known as “digital out-of-home” or DOOH, is a communications medium characterized by a dynamic display presenting messages in a public environment.1 A common example of digital signage media is a flat screen television displaying a loop of advertisements in retail stores. Other digital signage units take the form of kiosks, projectors or 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 (Digital Signage Expo, 2009a). Digital signage 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 (Lebovitz, 2009). There were an estimated 630,000 displays in the United States in 2007, though there are many more worldwide, particularly in China (Infotrends, 2007).

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 digital signage 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 digital signage 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, digital signage 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 more than 400 million people to date. 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 digital signage 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 digital signage, industry analysts predict the two media will grow together.

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

Radio Frequency Identification (RFID): The most common use of RFID in digital signage features RFID-enabled shelves that prompt nearby digital signage units to display advertisements related to the products on the shelves. Other digital signage systems air ads triggered by shopper loyalty cards equipped with RFID (Swedberg, 2007).

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 (Leake, 2009).

Digital signage uses other technologies, such as GPS, to a lesser extent, and more have potential to combine with digital signage to create interactive experiences for consumers. Clearly digital signage 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 digital signage data collection practices, the significant innovation digital signage has shown in the past will likely lead to hitherto unforeseen business models.

2. The Time is Right for a Digital Signage Privacy Framework

Using identification and interactivity technologies, the digital signage and mobile industries are taking the Internet experience into the physical world. In doing so, digital signage 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 (U.S. Federal Trade Commission, 2009). 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. Privacy invasion associated with digital signage 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 digital signage industry to collect detailed consumer data. Interactivity has been named a key driver of digital signage growth in 2010 (Digital Signage Expo, 2009b). In January 2010, Intel and Microsoft announced a joint effort to develop digital signage that can emulate the ability of online retailers to identify returning customers and tailor advertisements to them based on their shopping histories (Clark and Wingfield, 2010).

Consumers and companies are already wary of the privacy implications of identification and consumer profiling technologies in digital signage. Comments to blog posts and news articles on facial recognition in digital signage indicate many consumers have little faith that digital signage companies will protect consumer data (Patel, 2008). Some industry figures have said that companies must guarantee consumer privacy (Gerba, 2008), while others have cited privacy issues as an obstacle to using facial recognition technology for advertising purposes (Digital Signage Expo, 2009c). A New York Times article on billboards with facial recognition prompted a major digital signage company to publicly defend its privacy practices (MediaBuyerPlanner, 2008). Public backlash and possible violations of existing privacy laws have already led to the discontinuation of some digital signage advertising projects, as with the billboard which scanned UK license plates.

The reaction to this form of digital signage marketing 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 (Turow et al., 2009). The study also found 90% of young adults reject advertising tailored to them based on offline activities. Facebook members have revolted several times over uses of their information on the social networking site, persuading Facebook to repeatedly revise its
privacy policies and the information management tools it provides to its users (Coursey, 2009).

In 2009, the U.S. Federal Trade Commission (FTC) issued self-regulatory guidelines for online behavioral advertising (U.S. Federal Trade Commission 2009). 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 (Leibowitz, 2009). The U.S. Congress has held multiple hearings on the issue, and members of Congress have repeatedly called for privacy legislation to regulate how consumer information is collected, used and shared for marketing (Boucher, 2009).

Given this environment, digital signage 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 digital signage business models and data management practices is the best way to prevent privacy risks before they arise (Center for Democracy & Technology, 2009a). It will 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 existing systems. How digital signage companies handle the privacy issues they face today will affect the way the public, regulators and advertisers perceive the medium, 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 digital signage a disrespectful intrusion.

In 2010, the Point Of Purchase Association International (POPAI), a trade association, released a first generation set of privacy guidelines for digital signage (POPAI Digital Signage Group, 2010). 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. However, the Code does not articulate a full set of Fair Information Practices, nor does it suggest digital signage companies establish a comprehensive privacy framework. The POPAI Code is a sound foundation for the digital signage industry, but the industry should not limit itself to the Code’s recommendations.

In 2011, the Digital Signage Federation, another trade association, adopted the guidelines set forth in this paper as the Digital Signage Privacy Standards for its member companies (Digital Signage Federation, 2011). The guidelines in this paper have the advantage of applying all the Fair Information Practices, but are nonetheless voluntary and have no enforcement or oversight mechanism. It remains to be seen whether a critical mass of individual companies will integrate the Digital Signage Privacy Standards or the Code of Conduct into their business practices.

3. 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 still be identified from records stripped of traditional identifiers (Ohm, 2009). The FTC supports extending privacy protection to information beyond that which only directly identifies individuals (U.S. Federal Trade Commission, 2009).

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 (Center for Democracy & Technology, 2009c).

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 (Federal Trade Commission, 2009).

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, Blue-tooth 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.

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 (Malin and Sweeney, 2004). 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 digital signage 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 (Turow et al., 2009).

4. **Policy Framework and Models**

Privacy standards for digital signage 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. We believe the FIPs are equally well-suited as the basis for digital signage privacy guidelines. Recently, the U.S. Department of Homeland Security (DHS) adopted a modern and comprehensive formulation of these principles (U.S. Dept. of Homeland Security, 2008). These are the FIPs as set forth by DHS:

- Transparency
- 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, the guidelines of the online advertising industry fall short in key areas, so the digital signage industry should not merely mimic them (Center for Democracy & Technology, 2009b).
Nevertheless, the industries share the practice of targeting advertisements to consumers based on their activities. This makes it worthwhile for digital signage companies to familiarize themselves with the privacy frameworks of their online counterparts.

Digital signage companies and their affiliates may also find relevance in existing frameworks for the technologies they use. 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 (Mobile Marketing Association, 2008). Similarly, digital signage companies that use RFID should integrate the standards of relevant trade associations or privacy groups (Center for Democracy & Technology, 2006). 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, we recommend that the digital signage industry develop a privacy framework along the following lines:

4.1. Transparency

Digital signage data collection and use should be transparent. Generally, there are two important ways for digital signage companies to do this. First, digital signage 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 digital 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.

4.1.1 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. 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,
- 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. 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 digital signage privacy policy should underscore how these services interact.

Numerous digital signage 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 (Cognovision, 2007). Similarly, some companies that integrate digital signage and social networking publish privacy policies (LocaModa, 2010). However, existing policies vary greatly in detail, and not all digital signage services specify what they do with personal information (Market-place Station 2010). A privacy policy alone is not enough, however, and many consumers confuse the mere existence of a policy with substantive privacy protections (Turow, et al. 2006).

4.1.2 Notice

At present, many digital signage companies are completely unknown to consumers, so consumers are unlikely to look for the privacy policies posted on the web-sites of digital signage companies. Even if consumers come to know the names of digital signage companies, current practices give consumers little hint as to what company is responsible for a given digital signage 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 digital signage 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 digital signage unit that is collecting the information.² One notice should not cover, for example, an entire supermarket, but instead should be at each sensor and associated digital signage screen within the supermarket.

The precise manner in which companies provide notice may differ based on physical environment, equipment and other factors, but we conceptualize 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.⁴ The notice need not be large, but it should be easily readable to consumers.

³ The POPAI Code permits one notice to cover one establishment. See POPAI Code of Conduct, Pg. 8. However, we believe 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 digital signage network collecting data throughout the store.

⁴ 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
Second, companies should display a notice on or near each digital signage screen associated with consumer data collection. This notice can be a physical sign, such as a small placard. 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, 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 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.\(^5\)

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, visit www.companyname.com/privacy or see the store manager.*

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 digital signage unit is trusted. Hence, the second layer of notice – on the digital signs themselves – should give consumers an additional opportunity to become aware of the data collection.

\(^5\) Since companies’ privacy policies are online, most consumers are likely unable to access them in the store. Also, consumers without Internet access 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 review the privacy policy offline.
used for both security and for marketing, or if security in-formation is used for marketing, the notice (and privacy policy) should clearly disclose this.

In cases where digital signage 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 digital sign-age unit or the consumer initiates the interaction.

4.2 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, we conceptualize digital signage audience measurement and interactive marketing as occurring on three general 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 digital signage networks for social networking, RFID tracking, mo-bile marketing.

4.2.1 Consent

Consumers should have a ready means to choose whether their data is collected for advertising purposes. The means will differ between digital signage systems and services. Levels I and II (described above) should implement opt-out consent. At minimum, opt-out consent can be accomplished via notice by giving consumers an opportunity to avoid a particular digital signage 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.

4.2.2 Access

Consumers should have the ability to view and/or correct any directly identifiable data collected about them for digital signage marketing. Digital signage companies should designate an internal point person to receive and process consumer complaints and 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.

4.3 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 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.

4.4 Data Minimization

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

Digital signage 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 (Leake, 2009). 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. If a consumer opts-out or cancels a service, the associated information should be destroyed.

4.5 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 (POPAI, 2010).
4.6 Data Quality & Integrity

Digital signage 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. 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.

4.7 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. 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. 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.

4.8 Accountability

There has been substantial criticism of self-regulation of the behavioral advertising industry because of a lack of accountability for noncompliance. 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, contractors and affiliates who collect and use consumers’ information. There should be meaningful penalties for violations, especially willful or chronic noncompliance.

The digital signage 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.
5 Conclusion

Privacy can be an enabler – not an impediment – to the development of digital signage as an industry and a communications medium. If companies are willing to incorporate strong privacy protections into their business models, then the industry has the opportunity to enter a new era of responsible, consumer-friendly, interactive out-of-home marketing. By adopting strong privacy protections early on, the digital signage industry can avoid the ire of regulators and the embarrassment of advertisers. There’s also the matter of consumer trust: It’s far easier to keep than to win back.

Acknowledgements

The original version of this paper was first published by the Center for Democracy & Technology in Mar. 2010 (available at www.cdt.org). This paper formed the basis of a set of digital signage privacy standards I wrote for the Digital Signage Federation, a U.S.-based trade association, in Feb. 2011 (available at www.digitalsignagefederation.org). This paper is also a book chapter in Pervasive Advertising, 2011, Jörg Müller, Florian Alt, Daniel Michelis, Eds., Springer-Verlag GmbH Berlin Heidelberg.

References

10. Digital Signage Expo (2009b), Capital Network’s Research Identifies Customer Interaction as Key Digital Signage Trend for 2010,