WORLD **PRIVACY** FORUM

Comments of the World Privacy Forum

To the Federal Trade Commission

Regarding Face Facts: A Forum on Facial Recognition, Project No. P115406

Via ***ftcpublic.commentworks.com/ftc/facialrecognition***

Federal Trade Commission
Office of the Secretary
Room H–113 (Annex P)
600 Pennsylvania Avenue, NW.
Washington, DC 20580

January 31, 2012

The World Privacy Forum appreciates the opportunity to comment on the issue of facial recognition pursuant to the FTC Face Facts Workshop held on December 8, 2011.[1] The World Privacy Forum spoke on Panel 4 of the workshop, and those comments are already on the record. In these written comments, we would like to submit several key documents for the record and reaffirm several ideas from the workshop. The documents we are including as part of these comments include the World Privacy Forum's groundbreaking report on digital signage, *The One Way Mirror Society*. Also included as part of these comments are the consensus privacy principles for digital signage installations that were signed by the leading US consumer and privacy groups.

The World Privacy Forum is a non-profit, non-partisan public interest research and consumer education group. We are based in San Diego, California, and we focus our attention on a range of privacy topics, including technology, health care, finance, and workplace issues as well as emerging issues regarding big data and consumers. For more information see: www.worldprivacyforum.org.

I. Consent and Facial Recognition

In the workshop, one of the important issues that was highlighted in various respects was the issue of consumer consent. How is it best acquired? When should consent be required? We reiterate here what we stated at the time: the concept of a "**walk-out opt-out**" is not a viable way of managing consumer consent in the area of facial recognition or detection technologies.

[1] <http://www.ftc.gov/bcp/workshops/facefacts/>.

We note that the digital signage industry self-regulatory principles include the idea of a walk-out opt-out, we believe this is not workable for a number of reasons.

First, facial recognition technologies are not always readily visible to the human eye. Cameras are getting smaller, and deployments can be quite stealthy. Consumers cannot opt out of what they do not know exists.

Second, facial recognition (and detection) technologies are already being deployed widely in retail and other spaces. (See our report on digital signage, *The One-Way Mirror Society*, which is included in this document.) In five to ten years we expect that these technologies will be ubiquitous in certain public areas, thus making the "walk-out opt-out" point essentially moot. Instead of walking out or away from a single facial recognition or detection installation, consumers will be faced in some circumstances with multiple instances of these technologies within short distances, and walking out or physically leaving a space will not be possible. Retail and public spaces already exist that fit this scenario.

Third, the walk-out opt-out model burdens consumers with having to control data collection. The onus for privacy protection should not fall entirely on the consumer. It is difficult to envision a consumer education campaign surrounding this issue that does not verge on parody. "Consumers: if you don't want to have your face print taken, please leave the store." Consumers should not have to be wondering if and when their face print is being taken; it should not be a guessing game, and they should not have to edit their patronage of services based on fear of a camera or collection of facial biometrics.

In order to address this problem, some form of collection limitation or rules of the road will need to be imposed on the technology.

II. Face Prints and Consumer Rights

A striking development in the FTC hearings occurred on Panel 4, when Dr. Joseph Atick, a world-class biometrics expert, stated that consumers need to have the rights to their own face prints.

He said:

> "The face print is ultimately the element to that allows a system to perform the identification of a person or even to temporarily know that this person is the same person that was in aisle three versus aisle seven. So if we begin to elevate the face print to the status of a PII and acknowledge its ownership to say that while my image may not be owned by me and can be taken by anybody in public, because my reasonable expectation of privacy doesn't exist, my face print is supposedly an element, a unique code, that belongs to me. And therefore, if you are to exploit it in any way, by storing it in a database, you need my consent. By temporarily generating it and matching it against another instance in the last several hours, you need my consent. Therefore, in all of the analyses that we've heard today and the parting point for the International Biometric

> Industry Association has always been recognition of this code as the most critical element that needs to be protected."
>
> And:
>
> "Again, we strongly believe that face recognition is a viable technology, is an important technology in society, and should have a role to play, but it should be part of responsible use. All of the problems that we have heard about today result from the treatment or mistreatment of a face print. I'll drill this back home again. Face print is a biometric. Just like all biometrics, it should be considered as a PII, owned by the identity from which it was generated from, and it should enjoy the protection, one, vested upon it by the status of PII, second, the ownership rights from which it was derived. Everything else could legitimately be derived subject to these principles."[2]

Dr. Atick's approach provides an important avenue of thinking that we urge the FTC to explore further. We believe it holds significant promise and has the most potential for a positive and fair outcome. The policy dialogue around facial recognition and detection technologies has been overlaid by approaches with roots in past technologies from past eras. Much of the policy discussions to date have not been informed by Dr. Atick's level of knowledge, and as such have not taken into sufficient account the uniqueness of the face print, the nature of the technology, and the manner in which it is being deployed.

Just because a face print may be collected more readily and remotely than a fingerprint does not change the fact that a face print is a fundamental human biometric. Certainly, the ease of collecting the face print biometric has lent this particular metric to rapid commercial exploitation; but just because it can be used and is being used does not mean these uses should continue.

III. Digital Signage Privacy Principles for Consumers

The World Privacy Forum crafted a set of consensus principles around the issue of facial detection and recognition technologies used in digital signage in 2010. Seven leading consumer and privacy groups worked on these principles and signed on to them. We believe these principles provide a reasonable and balanced first step. These principles explicitly include language about children, which we believe is a key component of the principles. The issue of children and digital signage was not discussed at length in the FTC workshop. We also want to highlight that sensitive contexts remain an important consideration, for example, the non-treatment use of these technologies in health care settings.

Below are the Digital Signage Privacy Principles.

---

[2] FTC Face Facts Transcript, <http://htc-01.media.globix.net/COMP008760MOD1/ftc_web/transcripts/120811_FTC_sess4.pdf>.

Digital Signage Privacy Principles (Originally published 2/25/2010)

New forms of sophisticated digital signage networks are being deployed widely by retailers and others in both public and private spaces. Capabilities range from simple people-counting sensors mounted on doorways to sophisticated, largely invisible facial recognition cameras mounted in flat video screens and end-cap displays. These digital signage technologies can gather large amounts of detailed information about consumers, their behaviors, and their characteristics.

Even though these technologies are quickly becoming ubiquitous in the offline world, few consumers, legislators, regulators, or policy makers are aware of the capabilities of digital signs or of the extent of their use. Currently there is little if any disclosure to consumers that information about behavioral and personal characteristics is being collected and analyzed to create highly targeted advertisements, among other things. The technology presents new problems and highlights old conflicts about privacy, public spaces, and the need for a meaningful debate. The privacy problems inherent with digital signage are profound, and to date these issues have not been adequately addressed by anyone.

Digital signage networks, if left unaddressed, have the potential to create a new form of secret and highly sophisticated marketing surveillance, with the prospect of unfairness, discrimination, and abuses of personal information. Industry has taken a small step with its draft code of conduct, but the concerns are too important to be left to industry control alone.

The consumer privacy principles below represent a starting point for discussion of what consumer protections need to be included in digital signage networks.

Scope: These principles apply to digital signage. Digital signage is a digital display, camera (including an endcap and a pinhole camera), sensor, network, or similar facility that collects data or images of an individual or of identifiable property owned by an individual and that is used by a commercial entity for targeting, information, entertainment, merchandising, or advertising purposes. A security camera used exclusively for security purposes is not digital signage.

Notice: All digital signage must have a readable label that clearly discloses its purpose to individuals in its vicinity.

Deletion: Any identifiable data about an individual collected from digital signage or linked to identifiable digital signage data by a digital signage operator or affiliate must be erased within 14 days of collection.

Privacy: The data must be subject to a privacy policy that addresses all eight fair information practice principles, and the privacy policy must be available at the time the images are collected.

Children: Any digital signage operator collecting images of or data about a child who appears to be under 13 must immediately erase all images of the child as well as any identifiable data about the child.

Prohibitions: No digital signage may be used in sensitive areas, including but not limited to bathrooms; areas where children congregate; changing rooms; locker rooms; or in health care facilities, including gyms, health food stores, and areas over-the-counter drugs are sold.

Display: No image or data of an individual from digital signage may be publicly displayed in a manner that would make the image or data visible to any person other than the subject of the image or data.

Accountability: A digital signage operator must be accountable for complying with these principles.

Pam Dixon,
World Privacy Forum

Jeff Chester,
Center for Digital Democracy

Michelle De Mooy,
Consumer Action

Susan Grant,
Consumer Federation of America

Deborah Pierce,
Privacy Activism

Ashley Katz,
Patient Privacy Rights

Beth Givens,
Privacy Rights Clearinghouse

IV. One Way Mirror Society Report

In January, 2010 the World Privacy Forum published the first report on the privacy of digital signage networks. We are attaching the report in its entirety here as part of these comments.

World Privacy Forum

The One-Way-Mirror Society

Privacy Implications of the new Digital Signage Networks

by Pam Dixon

Brief Summary of Report

New forms of sophisticated digital signage networks are being deployed widely by retailers and others in both public and private spaces. From simple people-counting sensors mounted on doorways to sophisticated facial recognition cameras mounted in flat video screens and end-cap displays, digital signage technologies are gathering increasing amounts of detailed information about consumers, their behaviors, and their characteristics.

These technologies are quickly becoming ubiquitous in the offline world, and there is little if any disclosure to consumers that information about behavioral and personal characteristics is being collected and analyzed to create highly targeted advertisements, among other things. In the most sophisticated digital sign networks, for example, individuals watching a video screen will be shown different information based on their age bracket, gender, or ethnicity.

While most consumers understand a need for security cameras, few expect that the video screen they are watching, the kiosk they are typing on, or the game billboard they are interacting with is watching them while gathering copious images and behavioral and demographic information. This is creating a one-way-mirror society with no notice or opportunity for consumers to consent to being monitored in retail, public, and other spaces or to consent to having their behavior analyzed for marketing and profit.

The privacy problems inherent in these networks are profound, and to date these issues have not been adequately addressed by anyone. Digital signage networks, if left unaddressed, will very likely comprise a new form of sophisticated marketing surveillance leading to abuses of the collected information.

Summary of Recommendations

Principal preliminary recommendations discussed in the report include:

- Better notice and disclosure to consumers
- No one-sided industry self regulation
- No price or other unfair discrimination
- The full set of Fair Information Practices must apply for compiled information
- Notice given to consumers about subpoenas for their information
- Prohibitions on digital signage in bathrooms, health facilities, etc.
- More robust consumer choices regarding data capture and use from signage
- Special rules for collection and use of pictures and information about children

Background of Report

This report was originally prepared as background for the World Privacy Forum's testimony at the Federal Trade Commission's Privacy Roundtable at the University of California, Berkeley.

About the World Privacy Forum

The World Privacy Forum is a non-profit public interest research and consumer education group. It focuses on a range of privacy matters, including financial, medical, employment, and Internet privacy. The World Privacy Forum was founded in 2003. www.worldprivacyforum.org.

Table of Contents

Table of Figures

I. Introduction. What is digital signage and why care about its privacy implications?

The digital signage networks this report addresses are bi-directional. These networks give information to viewers while they capture information from viewers and send it back to a home base. In the digital signage industry, the new technologies are often compared to the interactive signs from the movie *Minority Report*.[3] In the movie, large-screen video billboards recognized individual consumers and delivered personalized advertisements to each person. The movie version of the digital signs and billboards relied on an iris scan to customize the ads. Today's modern digital signs rely on advanced video analytics and sophisticated cameras and sensors.

Digital signs typically output video, but that is only half of what they do. They can also be outfitted with hidden facial recognition technology, pinhole cameras, and even infrared cameras. As people walk by these signs, these signs capture consumer images, analyze them, and report the data back to their operators and tell those operators a great deal. The screens are typically networked to a central location and can be controlled remotely in real-time.

Digital signage is becoming ubiquitous while remaining secretive. The vast majority of people walking in stores, near elevators and in other public and private spaces have no idea that the innocent-looking flat screen TVs playing videos may be capturing their images and then dissecting and analyzing them for marketing purposes or personalizing and targeting ads to them.

[3] For more information, see IMDb *Minority Report* overview page <http://www.imdb.com/title/tt0181689/>.

Most people do not know that the advertisements they see may be different than those displayed to another person in the store because of their gender or age.

Digital signage raises a host of policy questions. How long will it take before the signs support differential pricing based on sex, race, and other demographic characteristics? Are the signs in stores recording children under 13? Who is able to access the footage: police, private litigants, tax enforcers? What disclosure is given to consumers that this is happening? What is the proper role of consent in data collection and use? Sadly, there are more questions than answers.

Digital signage is a privacy Chernobyl just waiting to happen, unless something is done quickly, and proactively. When customers realize how pervasive and how invasive this digital sign surveillance is, they will not like what they learn. Controls need to be put in place now, before this technology runs amok and becomes an entrenched problem that is too systemic to root out.

Society has not adequately confronted the conflicts that arise over privacy in public spaces. Individuals give up some privacy when in public, but that does not automatically mean that tracking everyone everywhere is unobjectionable. The ability of modern technology to watch and record people constantly while in public places enormous pressure on the old notion that there is no privacy in public. Unrestrained surveillance and collection of personal data through digital signage force us to confront the conflicts sooner than later.[4]

Defining digital signage

POPAI (Point of Purchase Advertising International),[5] a large, well-established global organization for marketing at retail and the digital signage industry, defines digital signage as:

> "A network of digital displays that are centrally managed and addressable for targeted information, entertainment, merchandising and advertising. Synonyms: dynamic signage, digital signs, electronic signage, digital media advertising, digital signage network, in-store TV network, captive audience network, narrowcasting network, out-of-home media network, digital media network, advertising network."[6]

Bill Gerba, a respected digital signage expert and CEO of WireSpring, a digital signage company, has offered this definition of digital signage:

---

[4] See, e.g., Christopher Slobogin, *Camera Surveillance of Public Places and the Right to Anonymity*, 72 Mississippi Law Journal 213, 233 (2002).

[5] Point of Purchase Advertising International (POPAI) <http://popai.com/>. "POPAI is the only global, non-profit trade association dedicated to the advancement of the marketing at retail advertising medium. Founded in 1936, POPAI is the oldest association representing marketing at retail with 20 chapters worldwide, with headquarters in Metropolitan Washington DC, and representing over 1,700 member companies internationally."

[6] Point of Purchase Advertising International (POPAI) <http://popai.com/>.

> "Any kind of electronic display (such as a TV, computer monitor, or flat screen) that can be remotely controlled over a computer network (like the Internet) and is placed into a venue to show targeted information, content and advertisements."[7]

Although digital signage is not new by any means, in 2006 it reached a new maturity due to the introduction of surveillance technologies that could capture, measure, and analyze how people were responding to the signs, and even the demographic profile those responding to the signs. By 2008, start-up companies had introduced competing analytical products based on these ideas for retailers, hotels, colleges, and others interested in signs that both deliver and capture video. Digital sign networks currently boast a high level of sophistication, and the technology is continuing to mature fairly rapidly.[8]

An Intel Solution Brief about digital signage stated:

> Consumers watching advertisements in stores, airports or just about anywhere probably don't realize that some digital signage systems are helping advertisers gauge their interest. Equipped with cameras and anonymous facial recognition software, these systems detect personal features and determine whether consumers are paying attention to the display, just glancing at it or ignoring it completely.

The brief also stated:

> With this capability, called "anonymous video analytics," advertisers can also target specific demographic groups by displaying ads that are compelling to the viewing audience. For example, the systems can dynamically change their content if the audience is male, female, a senior, or a family.[9]

The possibilities of the technology are mesmerizing, and it is already in use today. Companies have already been running campaigns using the capacities of the advanced surveillance analytics of digital signage to gather information about those interacting or passing by the signage and to tightly tailor ads to individuals.

Modern digital signage in action: the Castrol digital billboards

---

[7] Bill Gerba, *POPAI introduces Digital Signage Standards*, October 28, 2005. <http://www.wirespring.com/dynamic_digital_signage_and_interactive_kiosks_journal/articles/POPAI_introduces_Digital_Signage_Standards-250.html >.

[8] In addition to the current use of cameras in screens, new technology is emerging that will further mature the industry. See for example, Siggraph Asia 2009 e-Tech Prototype, the BiDi Screen. This LCD screen is bi-directional and allows for 3-D interaction using hand gestures. Photo-diodes are used as sensors. See <http://web.media.met.edu/~mhirsch/bidi/index.html>.

[9] *Reaching the Right Audience: Intel technologies in digital signage systems help maximize advertising messaging and return on investment*. Intel Digital Signage Solution Brief, <http://www.intel.com/design/intarch/platforms/digitalsignage/322038.pdf>.

On September 21, 2009, Castrol, a large oil company headquartered in the UK,[10] launched a highly personalized digital signage campaign in London. The campaign was "Right oil, right car." The idea was that Castrol would use advanced digital signage technologies to capture car information and them make custom oil recommendations to each passing car via a roadside digital billboard. To do this, cameras were positioned just before the billboards to capture the license plates of approaching cars. The cars' license plates were then matched in real time to the make and model of the car via the company's access to the UK Government's Driver and Vehicle Licensing Agency database.[11] (The DVLA database is the database of car registrant information in the similar to the state-level Division of Motor Vehicles and its databases in the U.S.)

Within 2 seconds, as the drivers passed by the billboard, the billboard displayed the car's registration and a personalized oil recommendation. Each personalized ad was displayed for 7.5 seconds. (Figure 1).

Figure 1

The Castrol personalized digital sign campaign in London. As cars approached the digital billboard, images of motorists' license plates were captured, matched to a database, then the billboard displayed an ad tailored to that make and model of car.

[10] Castrol, <http://www.castrol.com/castrol/castrolglobalhomeflash.do>.

[11] UK Department for Transport, Driver Vehicle and Licensing Agency. <http://www.dft.gov.uk/dvla/>. See also DVLA information regarding data release <http://www.dft.gov.uk/dvla/data.aspx>.

The Castrol campaign itself only lasted four days – the UK's DVLA launched an immediate investigation into how the car registrations of millions of drivers were sold for use by a large multinational oil firm. UK news reports on the issue revealed that Castrol used a third-party company to obtain the data from the database.[12]

The Castrol campaign is illustrative of the capabilities of the technology, and some of the privacy issues inherent in its use.

The digital signage industry is not unaware of privacy and other consequences of the technology, and industry has begun to think about some of these issues. An industry-crafted ***Recommended Code of Conduct for Consumer Tracking Methods*** (See Appendix A) describes some of the digital signage technologies that are privacy-invasive and seeks to encourage avoidance of some of the worst practices. But the industry by and large is not pressing for strong privacy protections in digital signage networks.

Digital Signage by the Numbers

Digital signage is not new, but it is considered to be the most promising newcomer in the digital advertising ecosystem. Any business or institution that can hang a high-definition screen and use it to track customers is a potential candidate for digital signage. Gas stations,[13] sports stadiums,[14] subway cars,[15] elevators,[16] bars,[17] movie theatres,[18] airports,[19] grocery stores,[20] retail stores,[21]

---

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

[13] See Gas Station TV, <http://www.gstv.com/>. See also < http://www.gstv.com/network.php>.

[14] Stephen Lawson, *Cisco plans networked screens at Yankee Stadium*, TechWorld, November 13, 2008. <http://www.techworld.com.au/article/267090/cisco_plans_networked_screens_yankee_stadium>.

[15] See TransitTV < http://www.transitv.com/>. See also <http://www.transitv.com/audience_markets_demographics_impressions_young_hispanic_african_american_transit_tv.html>.

[16] See The Elevator Channel, <http://www.digitalview.com/casestudies/cs_elevate.php>.

[17] See TapTV <http://www.tap.tv/bars_overview.php>.

[18] See < http://www.norvision.com/cs_harkins.asp>.

[19] See AirMedia < http://www.airmedia.net.cn/e/about.html>. See also: *For The World's Largest Digital Signage Networks— Look at China*, <http://www.digitalsignageuniverse.com/marketing7.html>.

[20] *The Marketplace Station Introduces In-Store Digital Stations at Whole Foods Market to help Marketers and Consumers*, November 17th, 2008. <http://www.themarketplacestation.com/files/news/51.pdf>.

restaurants,[22] college campuses,[23] museums,[24] casinos,[25] malls,[26] hotels,[27] and hospitals[28] are among commonly seen venues for digital signs and digital sign networks.[29]

The full maturation of digital signage as a viable and growing medium for marketing began in earnest around 2005-06. A Forrester Research report captured the beginning of the cycle when it reported in 2006 that by 2011, 90 percent of U.S. retailers would have implemented some form of "customer-facing, in-store digital media network."[30] In 2008, POPAI blogger Jeff Dickey wrote

> Digital signage is on the verge of becoming a truly mass media that, within a decade, should reach more people on a daily basis than traditional television, radio or

---

[21] See discussions of WalMart's digital signage network; ex.: Bill Gerba, *Walmart's Cost-Supplement Initiative: Retailer Becomes Ad Agency*, July 22, 2009. <http://www.wirespring.com/dynamic_digital_signage_and_interactive_kiosks_journal/articles/Walmart_s_Cost_Supplement_Initiative__Retailer_Becomes_Ad_Agency-731.html >. See also Jane Goodwin, *WalMart Digital Signage Celebrated Earth Month Last Year*, March 20, 2009. <http://www.wirelessdigitalsigns.com/2009/03/20/walmart-digital-signage-celebrated-earth-month-last-year/>.

[22] *First All digital restaurant sets new standards for QSR*, POPAI, Sept. 25, 2009. <http://www.popai.com/>.

[23] *Digital Signage to Make Campus Safer, Greener*. Univeristy of California Press Release, October 22,2009. <http://www.universityofcalifornia.edu/news/article/22181>.

[24] *OpenEye Develops Digital Wayfinding System for the National Museum of Natural History at the Smithsonian Institution in Washington D.C.* < http://www.digitalsignageuniverse.com/marketing21.html>.

[25] *Cisco Announces Interactive Digital Signage Pilot with Harrah's*, Jan. 11, 2009. <http://newsroom.cisco.com/dlls/2010/prod_011110b.html?sid=BAC-JsSynd>. See also Cisco Digital Signage, <http://www.cisco.com/web/solutions/dms/digital_signage.html>. Harrah's Casinos is piloting a large digital sign project. The Harrah's signs could be integrated with back-end business analytics systems and databases, which would allow the casino to offer deals based on individual consumers'interests

[26] *Southcentre Mall Deploys Digital Signage Powered By Omnivex Software*, Dec. 17, 2009. <http://www.digitalsignageexpo.net/DNNArticleMaster/DNNArticleView/tabid/78/smid/400/ArticleID/2379/reftab/66/t/Southcentre-Mall-Deploys-Digital-Signage-Powered-By-Omnivex-Software/Default.aspx>.

[27] Bill Yackey, *Four Winds outfits Royal Caribbean's Oasis of the Seas with digital signage*, Dec. 21 2009. <http://digitalsignagetoday.com/article.php?id=23433&prc=383&page=150>.

[28] See Catholic Healthcare West, <http://www.norvision.com/cs_chw.asp>.

[29] Joab Jackson, *IT Firms Promote Interactive Digital Signs at Retail Show*, PC World, Jan. 14, 2010. <http://www.pcworld.com/printable/article/id,186959/printable.html>.

[30] How Digital Media Transform In-Store Marketing, Forrester Research, 26 April 2006. Nikki Baird, with Carrie Johnson, Sean Meye and Brian Tesch. See also In-Store Digital Media: How to Reestablish Retail's Role as a Mass Consumer Medium. Bill Collins, Dorothy Allan, Decision Point Media Insight.

> newspapers. It is not television and it is not the Internet. It is a little of both and a lot of neither.[31]

While the 90 percent figure from 2006 was likely too optimistic,[32] the overall trajectory was correct. In-store and out of home digital networks have indeed taken hold, and the upward trend is strong worldwide. While there is no available study showing the degree of market penetration, by looking at individual businesses and vendors it is possible to get a sense for the overall size and scope of the industry.

In the U.S., Arbitron research indicates that about 155 million people have seen digital "out of home" displays.[33] (Digital out of home, or DOOH, is a term of art in the digital signage industry that generally refers to signage in places other than a home). A UK-based media company, SymonDacon, has placed 20,000 digital signage installations worldwide.[34] Scala, a company headquartered in near Philadelphia in the U.S., states that its global digital signage reach is in excessive of 300,000 screens worldwide.[35] In 100 U.S. malls, a company called Adspace creates campaigns on a network of 1,400 digital screens.[36] TransitTV operates more than 8,400 screens in buses and trains worldwide.[37] Quividi, a company that measures audience response to digital signs, states that the number of consumers that have looked at digital signs that contain its proprietary technology is 120 million people.[38]

---

[31] Jeff Dickey, *The Evolution of a New Media*, July 10, 2008. POPAI <http://www.popaidigitalblog.com/blog/index.html>.

[32] It is difficult to accurately determine exact percentages of penetration. But, for example, In 2008, about 25 percent of retailers were using camera-enabled traffic counting technology, one component part of some digital signage systems. See Deena M. Amato-McCoy, *Stepping it Up: Traffic-Counting Technology Improves Marketing, Sales*, Chain Store Age, Vol. 84, No. 5, May 2008.

[33] Joab Jackson, *IT Firms Promote Interactive Digital Signs at Retail Show*, PC World, Jan. 14, 2010. <http://www.pcworld.com/printable/article/id,186959/printable.html>.

[34] *Symon Dacon launch AV partner program to promote intelligent digital signage*, AV Magazine, January 14, 2010 <http://www.avinteractive.co.uk/news/search/977526/Symon-Dacon-launch-AV-partner-program-promote-intelligent-digital-signage/>. See also Symon Dacon <http://www.symon.com/solutions.shtml> and <http://www.symon.com/>.

[35] See Scala, About Us, <http://www.scala.com/about>.

[36] *Adspace launches Trend Alert messages on mall DOOH screens*, Oct. 7, 2009. Digital Signage Today, <http://www.digitalsignagetoday.com/article.php?id=23082 >.

[37] David Barbara, *Digital out-of-home advertising on the rise in '10*, Digital Marketing Observations, November 13, 2009.

[38] "120 million people counted in the VidiCenter: the foundation of our expertise." Quvidi home page, http://www.quividi.com.

Digital signage revenue is forecast to grow at a compound rate of about 20 percent to 2016.[39] The basis for the forecast rests in a combination of research showing that a preponderance of consumers' purchasing decisions – especially brand decisions – are made after they are physically in a store or retail location. "[C]onsumers make about 70 percent of their brand decisions once they are in-store, opening a window for grocers and manufacturers to target shoppers and they make their way through the aisles."[40]

II. Overview of key digital signage capabilities in place today

The best way to understand the capabilities of digital signage today and how it is being used is to see the digital signage industry's newly minted ***Recommended Code of Conduct for Consumer Tracking Methods*** (See Appendix A for complete document). This document on consumer tracking methods in digital signage was written and agreed upon entirely by industry members, without any participation by consumer representatives. The document reflects the advances in technology in this area and where the possibilities for abuse lay. The opening of the document reads:

> "Technological advances have made it **effortless and inexpensive** to track consumers in stores, through surveillance or other types of camera or recording media. On the one hand, there is huge demand to **gather shopper insights** in order to profitably market the right products to the investing consumer and provide a hassle-free shopping experience. On the other hand, the ability to record and track a customer's every move through the store, identify customers facially and demographically, and pinpoint where ad what customers are looking at, picking up, and putting into their shopping carts through Observed Tracking Data (OTD) raises privacy issues and sends shivers down the spine of even the boldest marketer."[41] (*emphasis added*)

In the best practices document, a set of digital signage technologies that raise privacy issues are discussed and categorized. It is not just digital signs themselves that are noted, but the entire technical "ecosystem" of digital signage: the tracking systems, cameras, and other surveillance

---

[39] *Digital Signage Display Revenue to Grow at 20 Percent CAGR to 2016*, Digital Signage Expo, July 11, 2009. <http://www.digitalsignageexpo.net/DNNArticleMaster/DNNArticleView/tabid/78/smid/400/ArticleID/1430/reftab/71/t/Digital-Signage-Display-Revenue-to-Grow-at-20-Percent-CAGR-to-2016/Default.aspx >.

[40] *CMM's retail TV Network Targets Southern California's Hispanic Consumers...Digital Signs Deliver In-Store Communications to Supermarket Shoppers*. April 9, 2009, <http://www.popai.com/index.php?option=com_content&view=article&id=78:cmms-retail-tv-network-targets-southern-californias-hispanic-consumers-digital-signs-deliver-in-store-communications-to-supermarket-shoppers&catid=29:popai-member-news&Itemid=76>.

[41] *Best Practices: Recommended Code of Conduct for Consumer Tracking Methods*, POPAI. This document is contained in full in Appendix A of this report.

mechanisms that go along with the digital signage network. The systems are those that are in place and in use today.[42]

Digital signage and media expert Laura Davis-Taylor discusses three primary ways that retailers use to track customers:

- Simple traffic counters, such as laser beams.
- Video-based recognition systems that count the number of people who have walked by a space, and measure how long they pause in a space (dwell time).
- Pathway tracking technologies that attach a unique ID number to each customer entering a store and then track that customer. The visit log of that individual can then be used to create a "heat map" or pathway map of their activities in the store.
- A fourth method has been developed recently, dubbed "automated tracking and reporting." This technique uses cameras and facial recognition software to capture and determine a customer's age, ethnicity, and gender.[43]

It is the last two capabilities that raise the most concerns: tracking individual customers can capturing age, gender, and ethnicity. Additionally, video signage technologies are being increasingly tied to identifiable mobile devices and loyalty card programs, which adds to the capabilities to track and identify individual customers.

The Code of Conduct for Consumer Tracking ranks the universe of consumer tracking methods in a hierarchy of low risk to high-risk methods. (OTD stands for *Observed Tracking Data*.)

Here is the most current version of the hierarchy (January, 2010.)

2.1 - Low Risk OTD Collection Methods

- Infrared or laser beam motion detectors
- Sonar and other non-recording, sound-based motion detectors
- Overhead path tracking systems that are capable of generating on-premise, aggregate "heat maps" of consumer presence, but are not able to track or record individual consumer paths.

2.2 - Medium Risk OTD Collection Methods

---

[42] A good early discussion of digital signage network tracking is: Bill Gerba, *Proven Methods for Tracking Your At-retail Media Network*, June 3, 2006. <http://www.wirespring.com/dynamic_digital_signage_and_interactive_kiosks_journal/articles/Proven_methods_for_tracking_your_at_retail_media_network-277.html >. This article mentions privacy as a consideration in its closing paragraphs and accurately anticipated the privacy issues that were to emerge.

[43] *Measurement and Analysis for Digital Signage, A Guide for Digital Signage Today and Retail Customer Experience*, p. 5. <http://leadgen.networldalliance.com/downloads/white_papers/BroadSignMeasurementandAnalysisGuideFinal.pdf> .

- Overhead camera-based path tracking systems or "gaze tracking" systems that are able to track and/or record individual consumer paths, but do not uniquely or individually identify consumers.
- Sensor-laden shopping carts that track and/or record individual consumer paths, but are not able to uniquely or individually identify consumers.
- RFID or other wired or wireless tracking devices knowingly worn or carried by consumer, or used on shopping carts and baskets to track consumer behavior, but are not able to personally or uniquely identify consumers.
- Any method where information can be used to collect demographic or psychographic information, but cannot be used to individually or uniquely identify consumers.

2.3 High Risk OTD Collection Methods

- Personally identifiable OTD collection via mobile phone or mobile computing device via wireless (cellular, Bluetooth, etc.) connection.
- Any method capable of identifying consumers based on past purchases, loyalty card programs, or other behavioral patterns collected by OTD collection methods.
- Any camera-based OTD system that collects and stores visual data.
- Any method used to personally or uniquely identify consumers, when combined with loyalty program data, or 3rd party marketing data.

The next sections of this report offer a more detailed discussion of these technologies and examples of the technologies in active use.[44]

III. Lower and Medium Privacy Risk Consumer Tracking Technologies

Heat maps and path tracking

Heat maps and path tracking technologies essentially generate maps of where consumers spend the most time standing and walking in stores. (Figure 2). One product, PathTracker, uses RFID chips for large store tracking, and video tracking technology for smaller stores or sub-areas within stores.

> "PathTracker is an electronic tracking system that records the coordinates of shoppers from the time the enter the store until checkout.....to protect the privacy of shoppers, the identities of the shoppers remain anonymous."[45]

---

[44] For an excellent industry discussion of aspects of privacy in digital signage, see Bill Gerba, *Digital Signage Networks Must Guarantee Viewer Privacy*, August 1, 2008. <http://www.wirespring.com/dynamic_digital_signage_and_interactive_kiosks_journal/articles/Digital_signage_networks_must_guarantee_viewer_privacy-569.html >.

[45] *Track Shoppers to Greater Profits, PathTracker for Retailers*. <http://www.sorensen-associates.com>.

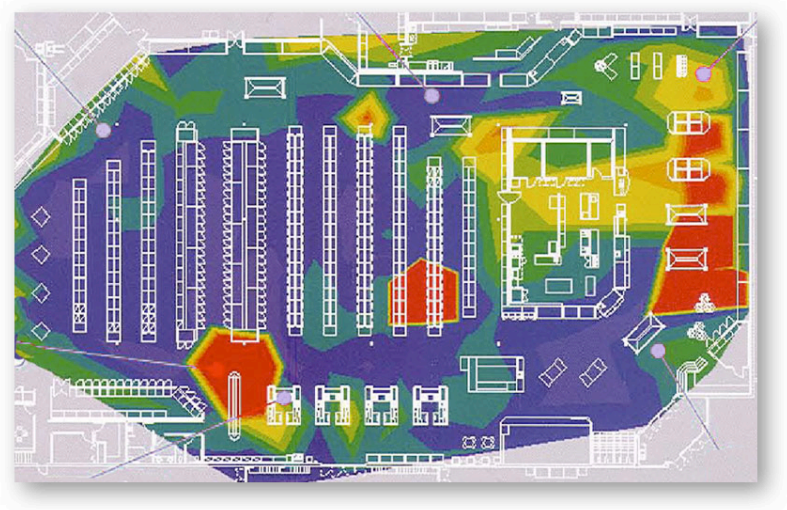

Figure 2

A heat map of customers' movements in a retail store; the red areas show the sites where consumers spent the most time.

A growing body of research exists about supermarket shopping tracking and shopper's pathways through stores.[46] The technology has a number of variations, but the theme is generally the same.

Gaze tracking

Gaze tracking in the context of digital signage is typically used in package and shelf testing.[47] One market research company noted that sample marketing questions gaze tracking can answer can include:

- Do shoppers see the product on the shelf?
- How many of the products on the shelf are noticed?
- How much attention does the product get compared to competing products?
- How quickly is the product able to attract attention?
- How long time does it take for shoppers to find a product that they are actively looking for?
- For how long is the product considered?
- How many times do shoppers look at the product?[48]

---

[46] Larson, Bradlow, Fader. *An Exploratory Look at Supermarket Shopping Paths*, April 2005. Wharton School, University of Pennsylvania.

[47] Tobii, <http://www.tobii.com/market_research_usability/research_fields/retail_shopping/white_papers.aspx >.

[48]<http://www.tobii.com/market_research_usability/research_fields/retail_shopping/example_research.aspx>.

Gaze tracking technology may be based on a single gaze tracking camera,[49] or it may be used in conjunction with other cameras and technologies.

IV. High Privacy Risk Consumer Tracking Technologies

Facial Recognition

Facial recognition technology was initially developed for security purposes, but it has found a new use in digital signage for marketing and ad targeting purposes. Essentially, the process is that a camera captures an individual's image, then checks it against algorithms that analyze at least 80 facial characteristics, such as distance between eyes, length of the face, width of the face, depth of eye sockets, and so forth. [50] Layers of algorithms are used to crunch the facial information into determinations about a person's age bracket, gender, and ethnicity. The next efforts are going toward coding the facial expressions of shoppers to "capture their emotional reactions to in-store environments."[51]

The video stream from the camera capturing the facial data is sent to a computer with a face-tracking engine that registers the number of viewers in front of the screen and can even determine whose eyes actually looked at the screen. Some software packages can also determine the gender, age, and ethnicity of the viewers. [52]

Audience Surveillance and Measurement for Marketing

One of the primary selling points for those wanting to deploy digital signage is that the screens are not just a one-way technology going from screen to consumer. The most advanced digital signage installations have screens concealing a host of technologies that gather information from the rooms they are placed in and the people who come within view of the screens, and then respond accordingly, often instantly. Digital signs can record the customers near them, monitor room temperature, check carbon dioxide levels, and more. For example, it is now an unremarkable feature for a digital signage installation to show ads targeted to the specific gender or age of a person looking at the screen as the person is standing in front of it.

---

[49] <http://www.irc.atr.jp/en/research_project/human_beh_ana/gaze_det/>.

[50] Manolo Almagro, *Quividi's Digital Sex Change Feature*, DailyDOOH , March 2, 2009 <http://www.dailydooh.com/archives/8887/print/>.

[51] Raymond R. Burke, Retail Shoppability: A Measure of the Worlds Best Stores, 2005. p. 13. Originally published in Future Retail Now: 40 of the World's Best Stores, Retail Industry Leaders Association. <http://kelley.iu.edu/features/archive/fall_2007/shoppability2.html>.

[52] Bill Yackey, *The Push for Digital Signage Metrics*, June 9, 2008, Digital Signage Today, <http://www.digitalsigngaetoday.com/article.php?id=20004>.

To accomplish this, digital signs are equipped with sensors and/or cameras or webcams built directly into the screen,[53] that can capture and record large amounts of information about who is looking at the sign, for how long, and at what time of the day. Then sophisticated video analytics create a demographic profile of the gender, age, and ethnicity among other characteristics. In some cases, multiple cameras are used, including cameras outside the screens. As seen in Figure 3, cameras can be tucked inconspicuously into end cap displays, on ceilings, and elsewhere.

Figure 3

Video analysis technologies exist in many retail and other environments. People looking at digital screens can have their images captured by a sensor or camera in or near the screen, then be analyzed by facial recognition technology. The cameras may be miniature and difficult to detect.

[53] Vendco Introduces Screens with Integrated Audience Measurement, July 30, 2008, <http://www.digitalsignagetoday.com/article.php?id=20284>.

It is important to remember that digital signage networks can involve an entire video architecture, one that includes existing security cameras. The audience measurement ecosystem may also use other shopper measurement systems in addition to the digital signage.[54]

Technologies that Measure Ethnicity, Age, and Gender

While it may come as a substantial surprise to consumers, it is a current business practice to use advanced video analysis technologies to determine a consumer's age, gender, and sometimes ethnicity to target ads and marketing directly to a particular customer. This technology is not new, but it did reach a maturation point in 2008/2009. Often called *advanced audience measurement* features, or *advanced video analytics,* the technology is used to determine a customer's ethnicity, gender, and age using facial recognition software and other techniques.[55] The technology has reportedly reached about a 90 percent accuracy rate.

Initially, the technology began as simple gaze tracking, but expanded into the demographic uses.[56] Cognovision, one company selling this technology, states in its materials that it measures five areas of consumer behavior and characteristics:

- Actual Impressions - The number of people who look at your displays
- Length of Impressions - How long people look for
- Potential Audience Size - The number of people who walk by
- Dwell Time - How long people stay near your displays
- Anonymous Demographics - Demographics of your audience (gender and age bracket)[57]

The point of creating demographic profiles is twofold: one, to determine how many people are watching the ad on the digital signage, and what ages, genders, and ethnicities they are; and two, to target the advertising based on that information.[58]

---

[54] See for example ShopperGauge. "ShopperGauge is an in-store monitoring system that delivers continuous reporting of REAL shopper behavior." Its website states: "24/7 digital monitoring by a strategically installed camera measures body language. Interpretive software reports traffic, dwell time, and shopper engagement with the display or shelf." The web site notes that the shopper data is live. ShopperGauge, < http://www.shoppergauge.com/how-shoppergauge-works>.

[55] See for example audience measurement products by Quividi <http://www.quividi.com/>, Cognovision <http://www.cognovision.com/solutions.php>, Tru-Media <http://www.tru-media.com/>, and Wututu <http://www.wututu.com/en/>.

[56] Laura Davis-Taylor, *The In Store Shopper Profiling Debate*, May 20, 2008, POPAI <http://www.popaidigitalblog.com/blog/articles/The_in_store_shopper_profiling_debate-439.html>.

[57] Cognovision Solutions page, <http://www.cognovision.com/solutions.php>.

[58] Steve Arel, *Video Analytics for Digital Signage Deployments*, White Paper, <http://DigitalSignageToday.com>, 2009. White Paper sponsored by Intel. "Various forms of analytics exist, breaking down consumer activity and behavior. The video version gives businesses a more detailed look at individuals who come in contact with digital signage. Through cameras installed on and integrated into monitors, software can show everything from the length of time someone watches an ad or message to exactly who watches, and correlate the effectiveness of those spots."

The ultimate goal is to have digital signs that change content based on the characteristics of the people standing right in front of the display:

> "[A]dvanced consumer demographics...will enable dynamic message selection on the digital sign and the ability to vary content based on viewer characteristics including gender, ethnicity, and banded age group."[59]

One example of this nexus can be seen in TargetScent, a kiosk-style "gender aware" fragrance dispenser. The kiosk/dispenser uses a small computer running Quividi facial recognition software. A camera in the display detects human faces in the vicinity of the display, estimates the corresponding gender of prospective customers and sends that information to the fragrance dispenser, choosing one of four fragrances based on the facial analysis. The units were introduced in 2009 in Europe.[60]

A more generalized example of this can be seen in the Whole Foods installation of the Marketplace Station digital signage network in Chicago in the U.S. and in Canada. A 2008 press release about the program, which rolled out first in Canada, described how the digital signage stations would benefit consumers with product information and food and lifestyle ideas. There is also a one-sentence description in the press release that hints at the fact the signs are equipped with advanced video analytics:

> A software application will also be in place to comprehend viewer metrics of each digital station, for hands-on tactical management of campaigns from start to finish. [61]

In May of 2009, the Marketplace Station digital signage network was deployed in the Chicago Whole Foods store. Beginning in March 2010, a press release notes that a new kiosk system will be added and consumer analytics will be captured. The new digital program is described as being capable of deriving data from actual audience viewership captured through an anonymous analytics sensor. The press release goes on to state that they will be reporting on the "gender of impressions."[62] Past analytics reports on the company's web site reveal that gender is indeed being analyzed at the Whole Foods stores through the facial recognition capabilities of its digital signage network.

---

[59] NRF: STRATACACHE debuting audience measurement tech, Jan. 13, 2009, <digitalsignagetoday.com/article.php?id=21409>.

[60] Quividi Press Release, *Presensia and Quividi Invent the First Gender-Aware Fragrance Dispenser*, January 7, 2009. <http://www.quuividi.com/news/090107/pressreleases>.

[61] *The Marketplace Station Introduces In-Store Digital Stations at Whole Foods Market to help Marketers and Consumers*, November 17th, 2008. <http://www.themarketplacestation.com/files/news/51.pdf>.

[62] *30 Retailers One Digital Network*, January 21, 2010. <http://www.themarketplacestation.com/files/news/55.pdf>.

The Whole Food's privacy policy makes no mention of its digital signage network. The Marketplace Station made no mention of its facial recognition software in its privacy policy. There is though, a YouTube video about Intel chips that highlights the Whole Foods/Marketplace Station digital signage installation, complete with an explanation of how the advanced analytics captures the gender of people looking at the signs. The video even shows a person shopping at the Whole Foods store looking up at the screens and being analyzed for demographic characteristics.[63] (Figure 3). Only the individual who looks at the video will have any real idea what is happening with Whole Foods digital signage behind the scenes.

Figure 4.

A screen shot of a YouTube video showing how the Whole Food's Marketplace Station digital signs are using facial recognition technology to analyze the gender of customers shopping at certain stores.

One of the issues this digital signage installation brings up is that of the digital signage industry's view of privacy and image capture and storage. One company that sells advanced video analytics, [64]TruMedia, has adopted a self-imposed standard that no images or "personally identifying information" will be *stored* without consumer consent. This is a frequently

[63] Digital Signage Innovations- Intel Technology in Digital Signage. July 22, 2009. YouTube, <http://www.youtube.com/watch?v=ibAFvT_Vr7s>.

[64] <http://www.themarketplacestation.com/files/analytics/analytics-january-2009.pdf>.

encountered refrain; that consumer privacy is protected because images are not *stored* by a particular digital signage system.[65]

TruMedia states in its privacy policy:

> Images from our sensors are processed and converted in real-time into counts (how many) and durations (how long). Using complex proprietary algorithms these counts are further assigned to specific demographic categories such as gender and age-group. No images are ever and will ever be stored for use, review or sharing with any private or governmental body.[66]

Here, the line is drawn at the retention or storage of the data. But the data is still captured, analyzed, and used without consumer consent and very likely without meaningful con sumer knowledge.

Another argument often encountered is that images are not *recorded,* therefore privacy is protected:

> CognoVision's Anonymous Impression Metric (AIM) technology uses face-detection and people counting technology to measure the effectiveness of digital signage, and enables real-time content targeting based on audience characteristics, allowing for truly measured and targeted delivery of media. The system has been designed to completely respect privacy – no personally identifiable information is ever collected, and no images are ever recorded. [67]

The Marketplace Station is using CognoVision's AIM technology, which means that the images of shoppers are not supposed to be recorded. However, just because the companies have decided that the lack of storage or recording of the data is equivalent to privacy does not mean that consumers should be left in the dark about such technologies. And it does not mean that customers in these stores should be subject to this activity without consenting to it. There is tremendous uncertainty about where these cameras are deployed in screens, if the images are being recorded, what information is actually kept, and how the consumer consent process is supposed to work. Of course, current limits on data collection and retention are subject to change without notice to the public. Indeed, entire systems operate without any notice to the public.

Some in the industry have raised privacy concerns about the deployment of these technologies, noting that simple gaze tracking was not as much of an issue as the demographic profiling and targeting.

---

[65] See for example: NRF: STRATACACHE debuting audience measurement tech, Jan. 13, 2009, <digitalsignagetoday.con/article.php?id=21409>

[66] TruMedia Audience Measurement Systems Privacy Policy, <http://www.tru-media.com/inside.asp?ID=18>.

[67] *Dynasign Integrates CognoVision Audience Measurement Technology*, Feb. 24, 2009. <http://Digital SignageToday.com/article.php?id=21733>.

> The technologies that enable this are originally intended for shopper gaze tracking, allowing retailers to understand how many people walked by a screen or display, how many looked, at what and for how long. This is exciting, as it can open the door to real-time analytics that allow us to respond according to what works — and what doesn't.
>
> The issue at hand is that some of the firms behind this technology can also "flip the switch" to track shopper demographics such as age, ethnicity and sex. Conceptually, the idea is to "auto serve" content geared towards the type of shopper walking by and ensure that it's as relevant as possible.[68]

Mobile Marketing and Customer Loyalty programs Linked to Digital Signage

Advanced digital signage networks can be tied to loyalty programs. One early method of tracking customer behavior in stores was to use tracking devices attached to shopping carts and then linked to customer loyalty programs.

> Several companies have developed tracking systems that use RFID, GPS, or infrared sensors attached to shopping carts, hand baskets, or hand-held shopping devices to track the customer's path through the store. These systems can provide reliable information on the shopping process, and the data are easily linked to individual-level customer transaction and loyalty information.[69]

But this customer tracking model has a significant drawback: if a shopper does not use a cart or a tracking device, then the consumer tracking fails. A more modern approach is to use digital signage as a bridge between the retailer and consumer in an opt-in program. One example of this model is Hot Topic, a retailer, that has deployed 1,500 in-store kiosks and digital signs which are linked with the store's customer loyalty program.[70]

---

[68] Laura Davis-Taylor, *The In-Store Profiling Debate*, May 20, 2008. <http://www.popaidigitalblog.com/blog/articles/The_in_store_shopper_profiling_debate-439.html>.

[69] Raymond R. Burke, *The Third Wave of Marketing Intelligence*, Kelley School of Business, Indiana University, p. 112.

[70] Joab Jackson, *IT Firms Promote Interactive Digital Signs at Retail Show*, PC World, Jan. 14, 2010. <http://www.pcworld.com/printable/article/id,186959/printable.html>. See also *Hot Topic Implements NCR Netkey Self-Service* , Jan. 12, 2010. <http://www.digitialsignageexpo.net/DNNArticleView/tab...ents-NCR-Netkey-Self-Service-Kiosks-and Digital-Signage/Default.aspx>.

Figure 5

Hot Topic's digital signage kiosks that link to its customer loyalty program. The kiosks contain a lens that looks back at customers.

To sign up for the Hot Topic program, customers interact with the kiosks and type in their name, date of birth, email address, mobile phone provider, mobile phone number, address, gender, and other details. The kiosk screens themselves do not appear to link to a privacy policy or the Terms and Conditions of the loyalty program. Instead, the kiosks have a FAQ section, but not a detailed privacy notice. The kiosks have a camera and lens embedded in them, (Figure 3) but it is not disclosed in any notice, nor is what the cameras are potentially capturing, recording and/or analyzing discussed in a written policy.

Nevertheless, the Hot Topic web site Terms and Conditions contains the following paragraph:

> **REGISTRATION:** To participate in , you must create a member account ("account") by registering your information with Hot Topic in a Hot Topic store, on our kiosks, or on the Web Site. You must have a valid email address to receive offers and other Program benefits. One email address per account. **It is your responsibility to read the full Terms and Conditions at the time that you register. By providing the required information to Hot Topic and creating an account, you're confirming that you've read and agreed to the Terms and Conditions.** *(emphasis added)*

One of the substantive issues with the majority of digital signage in place today is a lack of meaningful notice. Hot Topic terms and conditions "require" a consumer to read the full Terms and Conditions at the time of registration at an in-store kiosk, but it is well known that consumers rarely read notices. Indeed, a kiosk operator can easily check to see if the notice was read, but operators are not likely to do so because they would rather rely on the fiction that consumers have knowledgably consented.

As seen in the Hot Topic loyalty program, a substantial linkage can exist between the digital signage industry and mobile advertising for cell phones. Current examples are primarily opt-in, with customers taking the first step to give a retailer or business a mobile number or an email.

Another example of how this can work is Hungry Howie's pizza in Clearwater Florida. Digital signs sit in the restaurant location. The Hungry Howie's digital signage does not report back via cameras, instead, the signage focus is on interactively acquiring customer's mobile phone numbers via a touch screen. After a customer enters a mobile phone number on the screen, customers then receive a text message on their mobile phones. Upon a second opt-in, customers then receive coupons and other SMS texts via their mobile phones.[71] Customers are given the opportunity to opt out of the program.

Another digital signage-mobile example may be found in the campaigns of the company MegaPhone. MegaPhone uses trucks to host large portable digital billboards. Various interactive games run on the digital signage, which require mobile phone interaction to play. [72]

The company states in a brochure discussing case studies:

> Megaphone tracks all interactions and outcomes while aggregating data for each unique caller. Based on GPS call location, time stamping, cal length , buttons pressed, bounces, sharing, word of mouth, drop triggers, and mobile channel content engagement we can define a psychographic profile of your consumer.[73]

At the 2008 NBA All-Star Game in New Orleans, Adidas ran a campaign with MegaPhone. A portable digital sign on a large truck hosted a game called "3 stripe throw down." To play, people called a phone number shown on the game billboard. According to the case study written

---

[71] Case study: Hungry Howie's Pizza, Inc., July 31, 2009, Digital Signage Expo.net, < http://www.digitalsignageexpo.net/DNNArticleMaster/DNNArticleView/tabid/78/smid/1043/ArticleID/1667/reftab/70/Default.aspx>. For a video example of how the opt in and mobile response works and looks, see < http://www.sundropsystems.com/Products/loyaltxt.aspx#>.

[72] MegaPhone describes itself as "Making Digital Signage Interactive" on its home page. "MegaPhone is a Phonecall-Controlled, Real-Time, Multi-Player Collaborative Gaming Platform for Big Screens in Public Spaces." MegaPhone home page, <http://www.playmegaphone.com/>.

[73] MegaPhone Case Studies, <http://www.playmegaphone.com/documents/MegaPhone_InfoDocs.pdf>. See also video of the Adidas game, YouTube, MegaPhone, Sept. 8, 2008 <http://www.youtube.com/watch?v=29RSh_4A16s>.

by Megaphone, the objective of the campaign was to add the players to a mobile mailing list, and to drive foot traffic to local Adidas stores. Callers to the Adidas game receive a message with walking instruction to the Adidas store closest to the game location. The callers also have the opportunity to opt in to an Adidas SMS mailing list for special events during the all-star weekend. The Philadelphia 76ers ran a similar campaign.

While the campaign allowed for choice, a significant question to ask is if the people who called the phone number in order to play the digital billboard game had any idea that a third party was tracking their gaming interactions, aggregating data for each unique caller, and "defining a psychographic profile" of them. It is unclear how long consumer data was stored, and it is also unclear if the data was mingled with other identifiable consumer information.

MegaPhone did not have a privacy policy posted that described its privacy and data practices. The Adidas privacy policy addressed SMS programs in broad terms.[74] From a consumer perspective, it would have been a challenge for a consumer to meaningfully understand from the information available to them how their data would be handled and passed along.

V. Consumer Responses to Digital Signage and Privacy Issues

Few consumers are aware that watching a video screen or interacting with a kiosk may mean they are being recorded and having their behavior, gender, age, and ethnicity analyzed. As a result, there has not been a robust public discussion of how consumers feel about these technologies.

However, some academic literature does exist. In a 2008 University of Rotterdam study, focus groups of mixed gender with an average age of 28.6 years old were queried about a digital signage use case that allowed behavioral targeting of ads using an automated recommendation system in a similar to Amazon.com's and other online retailers, but tailored for digital signage technologies deployed in brick-and-mortar retail settings. The focus groups, which drew from the EU and from the US, came up with multiple objections relating to privacy, including the following problems with the digital signage recommendation system:

- General privacy problems
- Showing private information
- Information of other people on the screen
- Don't be too personal
- Don't link buyer behavior and advertising[75]

---

[74] Adidas privacy policy, <http://www.adidas.com/us/shared/legal.asp#Link8>.

[75] Imran Ashraf, *RFID as a marketing tool, a strategic and economic analysis. Combining RFID, Digital Signage, and Recommender Systems*., 21 Feb. 2008, Dissertation, Rotterdam School of Economics, Erasmus University Rotterdam, The Netherlands. Chart, p. 65. See also generally Chapter 5.

The research concluded that regarding digital signage, the "biggest objections seem to be related to privacy and unnecessary or wrong recommendations."[76] The strongest consumer objections to the digital signage recommendation screens came when a recommendation on the digital signage screen showed the following items, roughly in order of the strength of objections from the focus groups:

- A picture of the person
- The person's name
- Previous purchases
- The product the consumer had in their hand
- Product recommendations based on a stored profile.[77]

Consumers had substantially fewer privacy issues with the screens showing a top 10 list of best-selling products, similar products based on what was in their basket, or with product recommendations based on the average customer comparable to that consumer.[78]

There was no difference in acceptance of the digital signage recommendation system between a younger audience (below 30) and an older audience (above 30). The research also found that even though the digital signage use case that was presented to the focus groups used "non-identifying information," the group perceived it as privacy-invasive, and wanted to be in control. One suggestion flowing from the research was to allow digital signage recommendation screens to be consumer initiated, versus automatically targeted. [79]

These findings were echoed by a 2009 University of California, Berkeley - University of Pennsylvania, Annenberg School for Communication study that found that a majority of Americans – 68 percent -- strongly rejected behavioral tracking online . The UC Berkeley - Annenberg study is in line with the Rotterdam study in finding that young consumers cared about privacy.

---

[76] *Id*.

[77] Some digital signage installations have already experimented with showing people's pictures on screens that are publicly viewable. For example, Permanent TSB, a retail bank in Dublin, Ireland, used a digital signage installation that took pictures of people passing by the bank and superimposed the person's picture on a credit card graphic that was then shown on the digital signage in the bank window. *Is Demonstrating Big Brother Really Necessary?* Adrian J. Cotterill, June 14, 2008, <http://www.dailydooh.com/archives/2063>. The article contains an image of the digital signage installation.

[78] *Id*, 78, Chart 5.2.3.6: Privacy Aspects, and Figure 17.

[79] *Id*, 127.

In the UC Berkeley - Annenberg study, 86 percent of young adults said they did not want tailored advertising if it resulted from following behavior on website other than one they are visiting. Fully 90 percent rejected tracking if it is the result of following what they do offline.[80]

The University of Rotterdam findings seen in light of the high rejection rate for offline tracking suggest digital signage systems that track consumer behavior may be perceived as even more invasive than online tracking delivered via the web. When a person is standing in front of a digital screen in person, what consumers are comfortable with appears to shift toward a preference for more privacy controls, rather than less. The opt-in / opt-out debate will likely have a different outcome in the digital signage context given the potentially stronger consumer attitudes toward privacy protection in this area.

VI. What are the specific privacy issues posed by digital signage networks / what risks exist?

Specific and substantive policy issues and privacy risks exist in modern digital signage networks. This section summarizes those issues and risks.

Security Camera Footage: Repurposing footage for marketing and profit

Perhaps the most egregious repurposing of data is the use of security camera footage for store marketing purposes. From the industry literature, this appears to be an established business practice at this point. It is one that needs to be examined closely.

For example, researchers who specialize in studying shopping patterns, in describing their process of gaining shopper insight, include the option of using existing security cameras to collect shopping research data on consumers:

> "The research is usually implemented by setting up one or more video cameras, recording consumer shopping activity for several hours a day, and then coding behavior at a later time, either with human-research assistant or machine – vision tools. **Existing security cameras may be used to collect the data if they provide adequate visual coverage and fidelity**." (*emphasis added*) [81]

The POPAI Recommended Code of Conduct for Tracking Consumers specifically mentions this issue:

---

[80] Turow, Hoofnagle, King et al. *Contrary to what marketers say, Americans Reject Tailored Advertising and three activities that enable it.* September, 2009. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214 >.

[81] Raymond R. Burke, Retail Shoppability: A Measure of the Worlds Best Stores, 2005. p. 13. Originally published in Future Retail Now: 40 of the World's Best Stores, Retail Industry Leaders Association. <http://kelley.iu.edu/features/archive/fall_2007/shoppability2.html>.

- Using video or image data from surveillance, security, or loss-prevention systems may violate Federal, State and/or local laws, and is generally not recommended. If this practice is allowed by law, marketers must use separate computer systems and storage devices from those used to store the security/surveillance data. These computer systems and storage devices must be password protected with different passwords used than for the security/surveillance systems. (See Appendix A of this report for document.)

There is a lack of transparency around the use of surveillance footage for marketing purposes.

Lack of Transparency or Notice to consumer

Transparency and Consumer notice in the digital signage ecosystem is woefully lacking. First, the collection of consumer images can be extremely difficult to detect, if not nearly impossible. Digital signage does not usually come with a notice to the consumer that they are being recorded when they look at the screen. Digital signage does not usually come with any notice that facial recognition technology is being used to target ads to the consumer based on gender, age, and possibly ethnicity. And while some digital signage has obvious cameras affixed to it, other signage uses pinhole cameras that are extremely difficult to detect.

One manufacturer touted its pinhole cameras, one of which was shown tucked into an end-cap display in a way that would not be noticeable to most consumers:

> At the heart of the platform will be a custom-designed DSP chip that will receive incoming visual data from an attached pinhole camera. The screen display unit will then be able to log viewer statistics based on their age, gender, and ethnicity and will be capable of reacting to these details based on the demands of the site display.[82]

Second, even when consumers are expressly asked to interact with digital signage and give information (such as calling a mobile number to play a game or to sign up for a coupon) the amount of meaningful information a consumer receives about the collection and use of the data is generally absent. As discussed earlier, privacy policies posted on web sites generally do not discuss digital signage installations or networks. Even if they do, it is unreasonable to provide notice to consumers of digital signage privacy issues on a web site instead of providing notice directly at the place the cameras or sensors are located.

Thirdly, when consumers are notified about recording, the notification can be euphemistic at best. A notification sign under a security TV at one Wal-Mart in Oceanside, California stated: "in order to bring you low prices, we use closed circuit televisions and electronic merchandise tagging systems." That notice strongly suggests that the camera is for security and says nothing about collecting consumer information, and no other signs discussed the myriad other video and consumer tracking activity occurring at Wal-Mart.

---

[82] *1-2-1 View Developing Audience Measurement Chip*, Dec. 16, 2008. <http;//www.digitalsigagetoday.com/article.php?id=21238>.

A Walgreens in Encinitas, California, labeled each security camera with a large card that said "security camera." One screen was not labeled this way, but instead said: "Providing safety and savings: video recording in process." (Figure 6). What do these kinds of notices mean to consumers? Do the notices correspond to the reality of how the footage is actually being used? Do the notices cover all instances of consumer tracking in the retail space? Are the notices deliberately misleading?

Figure 6

A video recording notice in a retail store. Is the video used only for security purposes?

In a blog discussion of notice to consumer and what consumers would accept regarding gaze tracking tools, one industry expert had this to say:

> Mark Lilien of the Retail Technology Group had an interesting perspective, feeling that gaze tracking tools would be accepted as long as the retailer posts a sign telling folks that the store uses video surveillance. But rather than making it seem like an invasion of

privacy, convey it in a positive light such as, "we're using the finest technology in the world to help us stock what our customers want most.[83]

Lack of Consent, Opt-in, Opt-Out

In some instances, for example, in some loyalty card programs tied to digital signs, there are opt-in and opt-out structures available for consumers. For example, Hot Topic's loyalty program offers such a structure for text messages and other marketing messages. But how does a consumer consent to being recorded and analyzed and targeted by digital signs that employ hidden or pinhole-sized cameras or sensors? How does a consumer opt out of being recorded in the first place? How does a consumer opt out of having her image captured by a camera and then analyzed by facial recognition software and then used for demographic marketing analysis or feedback on ad effectiveness? How does a consumer opt out of being offered targeted ads based on what her age is, or gender, or ethnicity? Does a consumer "passively consent" to this activity by simply walking into a store, or passing by a digital signage installation?

In many if not most instances, digital signage installations that capture images of customers or individuals have no consent structures in place. The only meaningful opt out available to people is to wear clothing that obscures their face, such as a hoodie and sunglasses. In the preponderance of situations, consumers images are being captured and analyzed without their consent, knowledge, or understanding.

Identifiable data capture – anonymity

As discussed throughout this report, digital signage networks can use advanced video analytics to capture, record, and analyze images of individuals. That this is occurring is unambiguous. What is ambiguous is the way industry defines privacy and anonymity. The digital signage industry has come up with non-standard and self-serving statements about anonymity and privacy. Somehow, there are widespread views in the industry that video images of identifiable individuals are neither considered to be private information nor identifiable information.

It is difficult to argue that a camera collecting and analyzing images with facial recognition technology to glean audience characteristics such as gender and age is not using *personally identifiable information*. An individual's face is personally identifiable information. Period.[84] As long as the digital signage industry uses its own convenient definitions of *personally identifiable*, *stored*, and *recorded*, then the industry will be out of step with consumers. .

---

[83] Laura Davis-Taylor, *The In-Store Profiling Debate*, May 20, 2008. <http://www.popaidigitalblog.com/blog/articles/The_in_store_shopper_profiling_debate-439.html>.

[84] See, for example, the Privacy Act of 1974 that provides that a photograph is a record about an individual. 5 U.S.C. § 552a(a)(4) (definition of record).

Discrimination by Age, gender, and ethnicity

There is no question that age discrimination is a possibility with this technology. Targeting by age, gender and in some cases ethnicity is happening right now. One company selling technology capable of accomplishing this targeting wrote:

> "The latest version of the company's iCapture audience-measurement system can instantly identify older shoppers; earlier versions of the software could delineate between an adult and a child as well as determine gender and ethnicity. Coupled with the company's PROM (proactive Merchandising) software, iCapture allows retailers and marketers to target senior shoppers by serving up ads that are interesting and relevant to them.
>
> "We believe we have come up with a breakthrough in targeted marketing by allowing retailers and marketers to display age-appropriate content on a real-time basis, said George Murphy, CEO, TruMedia."[85]

This "breakthrough" came in 2008, and the technology has matured even further since that time. The question becomes: how does a senior being targeted by his or her age consent to that activity? How do they opt in or opt out of the targeted ad? The ad is being targeted to them because of how they look in the camera. There is no hiding behind a computer or deleting a cookie or downloading an "opt-out cookie." A sign telling a consumer they may see ads based on their race, gender and age might inform them of the program, but how can a person effectively give their permission for being targeted by their demographics?

It is not difficult to envision improper uses of this targeting capability. There are not appropriate or even any apparent controls in place to prevent this from happening.

Data retention issues

Some companies in the digital signage space state they do not store images collected from digital signage that captures images for video analytics, and they conclude therefore that privacy is protected. However, even in 2008 companies acknowledged in a New York Times article that image retention could be accomplished:

> "The companies that make these systems, like Quividi and TruMedia Technologies, say that with a slight technological addition, they could easily store pictures of people who look at their cameras."[86]

There is no enforceable standard that would force companies to erase data captured from digital signs and billboards, either facial recognition data, aggregate statistics, images, or other data. If a

---

[85] Digital signage today, *TruMedia's PROM software targets digital signage ads*, August 19, 2008. <digitalsignagetoday.com/article.php?id=20430>.

[86] Stephanie Clifford, *Billboards That Look Back*, New York Times, May 31, 2008.

company wanted to put up digital signage that recorded every passerby or shopper, and stored that footage for later marketing or other use, it could. Who would know?

Sensitive information

When digital signage is used in areas where sensitive information such as financial or medical data could be captured, privacy concerns become more pointed. An example is use of images of individuals purchasing health products or prescriptions. Some in industry have raised additional security concerns in this area.

When Cardinal Health launched its Pharmacy Health Network in August 2009, the launch included flat-panel LCD screens placed in independent and franchised pharmacies throughout the United States. The idea was that video advertisements would run on the screens while people waited for prescriptions to be filled. Cardinal Health stated it would make the Pharmacy Health Network (PHNTV) available to more than 5,000 independent retail and franchised pharmacies throughout the United States.[87] The screens do not appear to record images of consumers. Nevertheless, the launch of the network attracted the attention of a CEO of a digital signage company, who wrote an open letter to the Chairman and CEO of Cardinal Health warning the company of broader potential security issues with digital signage installations.

> "Because the PHNTV media player device is likely to sit on the same network segment as confidential patient information, any mildly capable hacker who is able to penetrate the digital signage player (especially one running Windows and using unencrypted HTTP transfers) now has a rogue device within the trusted Pharmacy Network from which they may attempt to access confidential patient information."[88]

The author suggested three ways to solve the problem, and also noted that he did not want the significant security risks raised by the deployment of a third party system in any trusted medical or health network to become a "Canary in the coalmine example we all look back on in 10 years and recall as the great big lawsuit that made security a real topic in Out Of Home Digital."

One blog commenter on the letter voiced the opinion that the system as implemented was not likely to fall afoul of best practices because the implementation did not collect data from the signs.[89]

---

[87] Cardinal Health launches in-store retail pharmacy digital advertising program. August 11, 2009, Press Release. <http://www.cardinal.com/content/news/8112009_112654.asp>. See also a more detailed description of the network and a demo video loop at <http://www.phntv.com/>.

[88] *An Open Letter from Chris Riegel, CEO STRATACACHE to Mr. Goeorge Barrett., Chairman and CEO, Cardinal Health*, August 13, 2009. Available at <http://www.dailydooh.com/archives/14964/print/>.

[89] *Id*.

Another issue related to digital sign deployment is wireless security. Many digital sign networks send information using wireless connections at some point in the infrastructure.[90] There are no available statistics on wireless security practices in the digital signage industry, but it is an area of concern for spying and for data breach. An intriguing concept to consider is how – or even if -- a company using a digital signage vendor that was compromised would give consumers notice of data breach.

Information Captured on Children and Teens

Digital signage that captures data from teens and especially from children under the age of 13 may run afoul of the policy that is the basis for Children's Online Privacy Protection Act, or COPPA.[91] COPPA applies to information collected online and requires affirmative parental consent, but *online* is ambiguously defined in COPPA. Most companies with digital signage networks appear to be silent on COPPA compliance in regards to, for example, audience measurement techniques and ad targeting. Some companies with digital signage installations have acknowledged that targeting teens and children is inappropriate in general terms, but not in terms specific to the digital signage program.

Generally, taking images of children for audience surveillance purposes raises multiple issues that have not been addressed yet.

Combination of offline and online data and data from digital signage

One of the goals of placing advanced video analytics into digital signage networks is to tie that data to other data sources. This is understood within the industry:

> "More sophisticated shopper analytics will be combined with other data sources, including loyalty programs and inventory management systems..." [92]

Loyalty programs are fairly simple to link to digital signage, as are mobile telephone numbers. The Castrol case in the UK shows how marketers will, if they can, link digital signage governmental databases for marketing purposes. The linking of digital video signage data to additional data sources is particularly sensitive because of the issue of identifiability.

VII. What has been done by industry regarding privacy?

---

[90] Deena M. Amato-McCoy, *Stepping it Up: Traffic-Counting Technology Improves Marketing, Sales*, Chain Store Age, Vol. 84, No. 5, May 2008. "By eliminating the cabling expense required with wired solutions, wireless options can be used in new settings, including across store departments and fitting rooms."

[91] Children's Online Privacy Protection Act, < http://www.ftc.gov/ogc/coppa1.htm>.

[92] Deena M. Amato-McCoy, *Stepping it Up: Traffic-Counting Technology Improves Marketing, Sales*, Chain Store Age, Vol. 84, No. 5, May 2008. Quote from John Szczygiel, president, Mate Intelligent Video.

The industry view of privacy has been officially articulated in a ***Recommended Code of Conduct for Consumer Tracking Methods*** that has been provided to the World Privacy Forum. The code of conduct is contained in full in Appendix A.

The code was created by members of POPAI, and took several years and went through several iterations. An early draft of the code of conduct contained a discussion of "passive consent" and active consent by consumers, among other issues. The final version outlines the technologies in use today, and lists those technologies in a general hierarchy of risk. For example, tracking a consumer's path through a store is seen as a low privacy risk, but "Any method used to personally or uniquely identify consumers, when combined with loyalty program data, or 3rd party marketing data" is categorized as a high privacy risk.

The document represents an important first step in acknowledging the privacy issues inherent in the digital signage industry, however, the document does not begin to approach a point of reasonable tension between consumer interests and industry interests.

VIII. Recommendations

There is no public awareness of the capabilities of digital signage, and that has to change before for any debate over regulation or legislation can start. Nevertheless, it is possible to identify from other privacy arenas the types of standards that should be considered for users of digital signage. Full recommendations will only be possible at a later stage. Here are some preliminary ideas.

1. The full present and future capabilities of digital signage should be publicly disclosed and discussed. There needs to be a full debate on what should be considered as anonymous information. Digital signage that collects or stores any consumer information should require actual, real-time notice to consumers. The extent of the notice may vary with the type of information collected. A sign that merely counts the number of consumers who pass raises fewer concerns than a sign that identifies the age, gender, or ethnicity of consumers. A sign that combines visual information with known identifiable information (e.g., from a frequent shopper card) raises the highest level of concern. The length of time information will be stored is another factor.

2. Self-regulation for privacy has been consistently failed in the past to provide fair, adequate, or balanced protections for consumers. No industry self-regulatory standards should be invited or accepted by regulators unless consumer representatives have been involved in the development of the standards.

3. Showing different consumers different advertisements is one thing. Using digital signage consumer identification capabilities to support differential pricing or other material differential offerings is a much more serious concern. At a minimum, some differential practices should be disclosed in real time, and other differential practices should be banned.

4. Consumer information collected through digital signage should be covered by complete and detailed privacy and security policies that reflect full implementation of Fair Information Practices.

5. If consumer information (including videos) is to be disclosed in response to subpoenas or court orders, every effort should be made to notify consumers in advance unless a law enforcement interest requires that notice be withheld.

6. The use of digital signage with any information collection capabilities – no matter how minor – should be expressly prohibited by law in some areas, such as changing rooms; schools; children's play areas; bathrooms; locker rooms; health care facilities (including pharmacies in supermarkets); places where over-the-counter drugs and health foods are sold; government offices; video, book and magazine stores and other places where First Amendment interests are exercised; hotel rooms; and other places.

7. Any choices offered to consumers with respect to the recording of their information or activities through digital signage should be made only after full, fair, and complete notice. Choices should require consumers to express affirmative consent, and the choices should no be expressed simply as an adjunct to a cell phone call or other activity.

8. The collection of information about children under the age of 13 and of teenagers should be the subject of special consideration and separate regulation.

IX. Conclusion

New forms of sophisticated digital sign networks are being deployed widely by retailers and others in both public and private spaces. Few consumers, legislators, regulators, or policy makers are aware of the capabilities of digital signs or of the extent of their use. The technology presents new problems and highlights old conflicts about privacy, public spaces, and the need for a meaningful debate. The privacy problems inherent in digital networks are profound, and to date these issues have not been adequately addressed by anyone.

Digital signage networks, if left unaddressed, have the potential to create a new form of secret and highly sophisticated marketing surveillance, with the prospect of unfairness, discrimination,

and abuses of personal information. Industry has taken a small step with its draft code of conduct, but the issues are too broad and too important to be left to industry control alone.

Much more needs to be done. This report by the World Privacy Forum seeks to shed light in a dark area and to start a more robust public debate. We cannot allow secret surveillance cameras to become the signs of our times.

Appendix A: POPAI Recommended Code of Conduct for Consumer Tracking Methods

The following document is the recommended code of conduct for businesses engaging in consumer tracking. The document is entirely non-binding, and was created entirely by industry participants. The document is reproduced here in full with no changes.

Best Practices: Recommended Code of Conduct for Consumer Tracking Methods

Summary:
While technology imposes few restrictions on data collection in retail settings, marketers should safeguard consumer privacy. This document provides recommendations to marketers on boundaries regarding consumer observations and how marketing insights should be used.

1. Introduction

Technological advances have made it effortless and inexpensive to track consumers in stores, through surveillance or other types of camera or recording media. On the one had, there is huge demand to gather shopper insights in order to profitably market the right products to the investing consumer and provide a hassle-free shopping experience. On the other hand, the ability to record and track a customer's every move through the store, identify customers facially and demographically, and pinpoint where and what customers are looking at, picking up, and putting into their shopping carts through Observed Tracking Data (OTD) raises privacy issues and sends shivers down the spine of even the boldest marketer. While the federal government has recognized dangers in the realm of mobile marketing and healthcare and has subsequently passed laws to protect consumers, no such laws exist for data collection in retail settings.

Clearly, there is a need for guidelines on data gathering and storing so that consumers are protected and the ethical boundary has not been crossed. For instance, it may be good business practice for marketers to track purchases through loyalty cards, or track how many people paused before a certain display. However, it may not be okay to record and store facial data for marketing purposes without the consent of the customer. Consequently, this document was created to provide recommendations on collecting data in ethical manners and to encourage marketers to consider ethical issues before collecting data. This document is not meant to be a replacement for federal and state laws; federal and state laws obviously take precedence over this document and should always be consulted to ensure compliance with the law.

2. Methods of OTD Collection

Before considering recommendations, it is important to categorize different OTD collection mechanisms by the degree of privacy exposure they may create for the consumer. Once the level of risk is ascertained, measures can then be taken to protect consumer privacy. There are three major levels of risk: low, medium, and high. Typically, low risk methods do not track consumers nor gather identifiable data. Medium risk methods gather tracking data but do not identify consumers. High risk methods identify customers in the process of tracking them.

2.1 - Low Risk OTD Collection Methods

- Infrared or laser beam motion detectors

- Sonar and other non-recording, sound-based motion detectors
- Overhead path tracking systems that are capable of generating on-premise, aggregate "heat maps" of consumer presence, but are not able to track or record individual consumer paths.

2.2 - Medium Risk OTD Collection Methods

- Overhead camera-based path tracking systems or "gaze tracking" systems that are able to track and/or record individual consumer paths, but do not uniquely or individually identify consumers.
- Sensor-laden shopping carts that track and/or record individual consumer paths, but are not able to uniquely or individually identify consumers.
- RFID or other wired or wireless tracking devices knowingly worn or carried by consumer, or used on shopping carts and baskets to track consumer behavior, but are not able to personally or uniquely identify consumers.
- Any method where information can be used to collect demographic or psychographic information, but cannot be used to individually or uniquely identify consumers.

2.3 High Risk OTD Collection Methods

- Personally identifiable OTD collection via mobile phone or mobile computing device via wireless (cellular, Bluetooth, etc.) connection.
- Any method capable of identifying consumers based on past purchases, loyalty card programs, or other behavioral patterns collected by OTD collection methods.
- Any camera-based OTD system that collects and stores visual data.
- Any method used to personally or uniquely identify consumers, when combined with loyalty program data, or 3rd party marketing data.

3. The Code of Conduct

The Code describes recommended practices for OTD collection and marketing activities in three categories: Data Collection, Storage and Security, Disclosure, and Cross-Channel and Cross-Domain Marketing.

2.1. Data Collection, Storage and Security

- OTD collection venues that house HIPAA-compliant entities (for example, a supermarket that contains a pharmacy) must adhere to all Federal laws governing the collection and use of marketing data in and around HIPAA-compliant sites. Typically, **no** OTD collection methods may be used in the HIPAA-compliant areas themselves, and special care must be taken to ensure that no method that allows for the unique or individual identification of consumers is used to track consumer behavior near the HIPAA sites. Click here or visit www.hipaa.org to learn more.
- OTD collection mechanisms capable of uniquely identifying a minor (i.e., a consumer under 13 years of age or the age required by state or local law) cannot be used at the OTD collection site.

- In no event should image, video or biometric data used to generate OTD be stored without an explicit consumer opt-in to do so. Collecting image or biometric data for marketing purposes may violate Federal, state or local laws, including **Federal Domestic Violence Laws**. If collecting image or biometric data is allowed in a venue's jurisdiction through OTD methods, the data should be stored for up to 3 months or the maximum period allowed by law.
- Using video or image data from surveillance, security, or loss-prevention systems may violate Federal, State and/or local laws, and is generally not recommended. If this practice is allowed by law, marketers must use separate computer systems and storage devices from those used to store the security/surveillance data. These computer systems and storage devices must be password protected with different passwords used than for the security/surveillance systems.
- Any and all collected OTD that can be positively associated with a unique consumer should be treated as Non-Public Personal Information (NPPI), and must be stored on a sufficiently secure computer system, such as one that conforms to the Payment Card Industry (PCI) standards for NPPI storage. Any OTD that could potentially be misused to create public safety hazards must be treated as NPPI and be handled as described above.
- It is a violation of Federal law to use certain types of marketing data (for example, demographic data) to offer special promotions to one group of consumers but not another. Marketing practices that make use of demographic or psychographic OTD may not be used to create promotions that vary the pricing or availability of an item or items, or change requirements and availability of financing options, if applicable.

Click here or visit http://www.consumerprivacyguide.org/law/ for brief information on consumer privacy laws.

2.2. Disclosure

- Marketers must provide a disclosure notice (the "Notice") to consumers who may be monitored (intentionally or incidentally) by OTD activities.
- The Notice should be easily understandable, unambiguous, and current. It should not contain any false or misleading information about the nature of the OTD collection methods or the intended use of any collected data.
- The Notice should describe the OTD collection methods in effect and whether data collected via OTD methods will be combined with other data including, but not limited to register receipt information, credit card or any NPPI or data collected by 3rd party and/or affiliate marketers.
- The Notice should be posted in at least one location at each site where the OTD collection is taking place, preferably at every entrance.
- The Notice itself must meet all ADA guidelines and must be free of obstructions that might inhibit visibility.
- The Notice must contain information about all available opt-in and opt-out mechanisms such as a consumer-accessible telephone that can be accessed for no fee in order to opt out.
- When OTD requires the use of a consumer's cell phone, mobile computing device, email messages, or SMS text messages, or links OTD data with a telephone number or

Bluetooth device, marketers must also comply with the Mobile Marketing Association's Global Code of Conduct, mobile marketing laws, FTC Telemarketing Sales Rule, other FTC rules, and the National Do Not Call Registry.

2.3. Cross-Channel and Cross-Domain Marketing

Cross-channel OTD marketing occurs when data from multiple sources, such as in-store, catalogs, online, and OTD are combined with the intent of tracking a consumer across multiple properties, retail environment, or other public or private spaces.

- Consumers should be made aware of the use of their OTD data and other marketing data. Such information should be included in the Notice.
- Cross-channel marketing is considered High Risk for OTD collection mechanisms. Therefore, consumers should opt-in before data is combined in cross-domain ways. Furthermore, the consumer should also re-opt in to the program each time he or she enters a new venue where the cross-domain OTD marketing program takes place.
- Disclosure notices should be located at every OTD collection site participating in the program, and follow all other best practices for OTD data collection.
- Disclosure notices for cross-domain OTD marketing programs must contain a complete list of all Marketers and other entities participating in the program (for OTD collection or other purposes), as well as a complete list of all OTD collection practices and the physical locations of the OTD collection devices.

3. Participation

This document is not a contract or legal document, and is non-binding. However, adherence to the Code is strongly recommended to ensure that consumer privacy is safeguarded.

Credits:

Author: Pam Dixon, executive director, World Privacy Forum

Contributor: Robert Gellman http://www.bobgellman.com

For More Information and Document Updates:

PDF version of full report is located at
<http://www.worldprivacyforum.org/pdf/onewaymirrorsociety.pdf >

For updates to this report and other documents related to the report, see the World Privacy Forum <http://www.worldprivacyforum.org/ >

For More Information Contact:

World Privacy Forum
www.worldprivacyforum.org
+1 760.436.2489

The World Privacy Forum is a 501 (C) (3) non-profit, tax-exempt organization. Its focus is on public interest research and consumer education relating to privacy topics.

Document history:

Document published January 27, 2010.

#####

Thank you for the opportunity to comment, and thank you for your excellent work in this area.

Respectfully submitted,

/s

Pam Dixon

World Privacy Forum
www.worldprivacyforum.org