Digital Signage Privacy Principles:

Critical policies and practices for digital signage networks

February 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.

Endorsing Organizations:

Pam Dixon,
World Privacy Forum

Jeff Chester,
Center for Digital Democracy

Michelle De Mooy,
Consumer Action

Susan Grant,
Consumer Federation of America

Ashley Katz,
Patient Privacy Rights

Deborah Pierce,
PrivacyActivism

Melissa Ngo,
Privacy Lives

Beth Givens,
Privacy Rights Clearinghouse