

Facial Recognition and Privacy

by [Harley Geiger](#) [1]

December 6, 2011

Facial recognition technology is increasingly used in a variety of ways – from security and authentication to photo tagging on social networks and targeted advertising on digital signs in stores. Facial recognition software packages are freely available online, and the technology is fast making its way into mobile phones. Facial recognition poses complex privacy issues that do not fit squarely with present laws.

Today CDT released “Seeing is ID’ng,” a [report on facial recognition and privacy](#) [2]. The report describes the state of facial recognition technology and its commercial applications, the lack of laws that address facial recognition, and policy approaches to preserving consumer privacy.

CDT’s report comes a day in advance of a Federal Trade Commission (FTC) [workshop](#) [3] exploring the privacy implications of facial recognition and potential policy solutions. I will present the CDT report at the workshop. The FTC workshop was prompted by a [letter](#) [4] from Sen. Jay Rockefeller (D-WV), Chairman of the Senate Commerce Committee, directing the FTC to develop recommendations on privacy protection for facial recognition.

CDT’s report urges the FTC to consider a mix of government regulation, industry self-regulation, and privacy enhancing technologies that can give consumers more control over how facial recognition is used without unduly limiting the benefits of the technology or burdening free expression.

The key privacy interest that commercial facial recognition affects is, of course, identification of an individual through facial features alone. Without facial recognition technology, it is very difficult for a stranger to easily and quickly identify an individual on this basis. Individuals in public currently expect that most businesses and passersby cannot recognize their faces, fewer still can connect a name to their faces, and few – if any – can [associate](#) [5] their faces with internet behavior, travel patterns, or other personal information. Facial recognition technology fundamentally changes this dynamic, enabling any marketer or random stranger to collect – openly or in secret – and share the identities and associated personal information of any individual in public.

Deployed widely enough, a network of facial recognition cameras can track millions of [individuals](#) [6] as they move from place to place. Unlike other tracking methods, such as GPS or RFID, facial recognition does not require the tracked individual to carry any special device or tag, reducing consumers’ ability to thwart unwanted tracking. Once built, databases assembled with facial recognition for commercial use can be accessed or re-purposed for [law enforcement surveillance](#) [7].

Although the issue is growing more serious, CDT does not believe that Congress should seek legislative solutions for facial recognition alone. Establishing privacy laws for facial recognition in isolation will likely be ineffective – if consumer tracking via facial recognition or other biometrics were prohibited, consumers would still be tracked through numerous alternative methods.

Instead, as CDT has long [advocated](#) [8], Congress should pass a comprehensive consumer privacy law that includes biometrics and is based on the Fair Information Practice Principles. As the U.S. Dept. of Commerce proposed in its “[Green Paper](#) [9],” Federal agencies should play a crucial role in developing and enforcing voluntary self-regulatory privacy codes that cover facial recognition – like the DSF [Digital Signage Privacy Standards](#) [10]. Any self-regulatory process must offer businesses tangible incentives, the development of the rules must include input from consumer groups, and the rules must be consistently enforced.

In terms of specific policy stipulations, CDT [believes](#) [11] companies should generally obtain informed, affirmative consent prior to identifying individuals via facial characteristics in public places or in places open to the public, such as stores. CDT also believes companies should provide

consumers with clear, prominent notice of their use of “anonymous” facial detection in public places.

The lack of adequate protection in current law and the limitations of self-regulation when not backed by an enforcement mechanism highlight again the point that CDT has been making consistently about consumer privacy: The only effective way to address privacy is with a mix of baseline consumer privacy legislation, industry self-regulation, and privacy by design.

Publicly available facial recognition is a transformative technology that demands nuanced solutions to preserve consumer privacy and free expression. At the FTC workshop and through other activities, CDT will be seeking to move policy in the right direction.

The copyright © 2013 by the Center for Democracy & Technology. CDT can be freely copied and used as long as you make no substantive changes and clearly give us credit. [Details](#).

Source URL: <https://www.cdt.org/blogs/harley-geiger/612facial-recognition-and-privacy>

Links:

- [1] <https://www.cdt.org/personnel/harley-geiger>
- [2] <http://cdt.org/report/seeing-iding-facial-recognition-and-privacy>
- [3] <http://www.ftc.gov/bcp/workshops/facefacts/>
- [4] http://www.washingtonpost.com/blogs/post-tech/post/rockefeller-web-facial-recognition-technology-needs-ftc-scrutiny/2011/10/19/gIQAHEQsXL_blog.html
- [5] <http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ>
- [6] <http://www.naomiklein.org/articles/2008/05/chinas-all-seeing-eye>
- [7] http://www.nextgov.com/nextgov/ng_20111007_6100.php?oref=rss
- [8] <http://www.cdt.org/policy/recommendations-comprehensive-privacy-protection-framework#1>
- [9] <http://www.commerce.gov/node/12471>
- [10] <http://www.digitalsignagefederation.org/Resources/Documents/Articles%20and%20Whitepapers/DSF%20Digital%20Signage%20Privacy%20Standards%202-2011%20%283%29.pdf>
- [11] <http://www.cdt.org/policy/safeguarding-privacy-digital-signage-industry#3>