July 2015

FACIAL RECOGNITION TECHNOLOGY

Commercial Uses, Privacy Issues, and Applicable Federal Law

Why GAO Did This Study

Facial recognition technology—which can verify or identify an individual from a facial image—has rapidly improved in performance and now can surpass human performance in some cases. The Department of Commerce has convened stakeholders to review privacy issues related to commercial use of this technology, which GAO was also asked to examine.

This report examines (1) uses of facial recognition technology, (2) privacy issues that have been raised, (3) proposed best practices and industry privacy policies, and (4) potentially applicable privacy protections under federal law. The scope of this report includes use of the technology in commercial settings but not by government agencies. To address these objectives, GAO analyzed laws, regulations, and documents; interviewed federal agencies; and interviewed officials and reviewed privacy policies and proposals of companies, trade groups, and privacy groups. Companies were selected because they were among the largest in industries identified as potential major users of the technology, and privacy groups were selected because they had written on this issue.

What GAO Recommends

GAO makes no recommendations in this report. However, GAO suggested in GAO-13-663 that Congress consider strengthening the consumer privacy framework to reflect changes in technology and the marketplace, and facial recognition technology is such a change. GAO maintains that the current privacy framework in commercial settings warrants reconsideration.

View GAO-15-621. For more information, contact Alicia Puente Cackley at (202) 512-8678 or cackleya@gao.gov.

What GAO Found

Facial recognition technology can be used in numerous consumer and business applications, but the extent of its current use in commercial settings is not fully known. The technology is commonly used in software that manages personal photographs and in social networking applications to identify friends. In addition, several companies use the technology to provide secure access to computers, phones, and gaming systems in lieu of a password. Facial recognition technology can have applications for customer service and marketing, but at present, use in the United States of the technology for such purposes appears to be largely for detecting characteristics (such as age or gender) to tailor digital advertising, rather than identifying unique individuals. Some security systems serving retailers, banks, and casinos incorporate facial recognition technology, but the extent of such use at present is not fully known.

Privacy advocacy organizations, government agencies, and others have cited several privacy concerns related to the commercial use of facial recognition technology. They say that if its use became widespread, it could give businesses or individuals the ability to identify almost anyone in public without their knowledge or consent and to track people's locations, movements, and companions. They have also raised concerns that information collected or associated with facial recognition technology could be used, shared, or sold in ways that consumers do not understand, anticipate, or consent to. Some stakeholders disagree that the technology presents new or unusual privacy risks, noting, among other things, that individuals should not expect complete anonymity in public and that some loss of privacy is offset by the benefits the technology offers consumers and businesses.

Several government, industry, and privacy organizations have proposed or are developing voluntary privacy guidelines for commercial use of facial recognition technology. Suggested best practices vary, but most call for disclosing the technology's use and obtaining consent before using it to identify someone from anonymous images. The privacy policies of companies GAO reviewed varied in whether and how they addressed facial recognition technology.

No federal privacy law expressly regulates commercial uses of facial recognition technology, and laws do not fully address key privacy issues stakeholders have raised, such as the circumstances under which the technology may be used to identify individuals or track their whereabouts and companions. Laws governing the collection, use, and storage of personal information may potentially apply to the commercial use of facial recognition in specific contexts, such as information collected by health care entities and financial institutions. In addition, the Federal Trade Commission Act has been interpreted to require companies to abide by their stated privacy policies. Stakeholder views vary on the efficacy of voluntary and self-regulatory approaches versus legislation and regulation to protect privacy. GAO has previously concluded that gaps exist in the consumer privacy framework, and the privacy issues that have been raised by facial recognition technology serve as yet another example of the need to adapt federal privacy law to reflect new technologies.

_____ **United States Government Accountability Office**