F

Facebook

Identification: Created in 2004 by Harvard University student Mark Zuckerberg. It was based on the concept of the university's "facebook" — a directory of student names with a picture, typically organized by graduating class year.

In its first iteration, Facebook was a program called Facemash, which Zuckerberg developed, that allowed Harvard students to rank photographs of their classmates according to attractiveness. Zuckerberg obtained the photographs by hacking into Harvard's database of student identification images. Harvard University administration shut down the site a few days after Zuckerberg began disseminating it. However, a few months later Zuckerberg began development of the thefacebook.com. Thefacebook.com was launched in February 2004 and only allowed Harvard University students to join. In March of 2004, thefacebook.com expanded to Columbia University, Stanford University, and Yale University. At this time Eduardo Saverin, Dustin Moskovitz, Andrew McCollum, and Chris Hughes joined Zuckerberg in the development and management of the website. Very quickly, thefacebook.com expanded to include Ivy League universities and Boston-area colleges. It continued to expand and by 2006 Facebook was available to anyone over the age of 13. By 2012, Facebook announced it had reached its one-billionth user. Facebook is now a publicly-traded company that has a net worth in the billions of dollars. Its primary source of revenue is through advertising, with a small amount of additional revenue coming from fees and payments for virtual services, such as games.

In many ways, Facebook has become the symbol for the contradictory nature of an online social network. One facet of Facebook is its ability to assist people in maintaining social connections that extend beyond the sphere of everyday life. Conversely, Facebook is a publicly-traded company with responsibilities to its shareholders to maintain a certain level of profitability. Also, its primary source of revenue is advertising. Advertising, by its nature, must respond to its audience. Facebook, must, therefore, be able to define the characteristics of its users. This tension between the use of Facebook as a personal mode of expression, as well as a generator of revenue, informs the question of privacy and Facebook.

The impact on the privacy of individuals using Facebook has been an issue from its initial iteration as Facemash. When the Harvard University administration shut it down one of the reasons they gave was the privacy concern of disseminating students' pictures without their consent. This concern has persisted, despite Facebook's continued effort to assure its users that the information they generate by using Facebook is adequately protected.

It was reported that Facebook has participated in lobbying for the passing of the Cybersecurity Information Sharing Act (CISA) of 2015.

This act allows companies to share cybersecurity threat information with federal agencies such as the Federal Bureau of Investigations and the National Security Agency. Privacy advocates argue that the definition of a cybersecurity threat under CISA is too broadly defined and will allow companies to actively monitor users without a warrant. This information could then be provided to various federal agencies.

In 2018 Facebook faced multiple questions regarding its protection of users' personal information, security structures, and dissemination of information to third parties. Most notably, *The New York Times* reported that Cambridge Analytica, a voter-profiling company, acquired the personal information of 50 million Facebook users without users' permission in order to create a national "psychographic profile" that would be used in its work for the Trump presidential campaign. Facebook later stated that the personal information of 87 million users had been accessed without the users' permission. Facebook did make changes to the accessibility of the privacy controls as a result; however, Mark Zuckerberg and Facebook continue to be criticized for security breaches and third-party access to personal information.

Rachel Jorgensen

Further Reading

Cohen, Julie E. "Inverse Relationship Between Secrecy and Privacy." *Social Research* 77.3 (Fall 2010): 883–898.

Hoefflinger, Mike. *Becoming Facebook: The 10 Challenges that Defined the Company That's Disrupting the World*. New York, AMACON, 2017.

Newton, Lee. *Facebook Nation: Total Information Awesomeness*. New York: Springer, 2014.

Rosenberg, Matthew and Nicholas Confessore, Carole Cadwalladr. "How Trump Consultants Exploited the Facebook Data of Millions." *The New York Times*. March 17, 2018. https://nyti.ms/2GB9dK4

Rubenstein, Ira S. and Nathaniel Good. "Privacy By Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents." *Berkeley Technology Law Journal* 28.2 (Fall 2013): 1333–1413.

Trottier, Daniel. *Identity Problems in the Facebook Era*. New York, Routledge, 2014.

See also: Computers and privacy; Cyberspace Information Sharing Act (CISA); Data collection; Marketing; Social media

Facial recognition technology

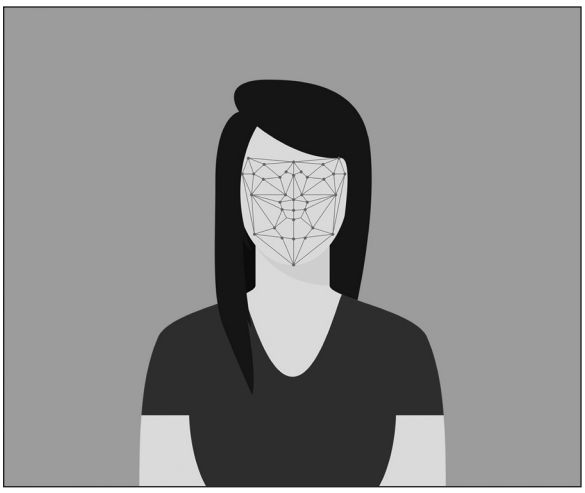
Identification: A biometric technology that identifies people by measuring and analyzing their physiological or behavioral characteristics.

Biometric technologies were developed to identify people through characteristics such as their faces, fingerprints, hands, eye retinas and irises, voice, and gait. Unlike conventional identification methods, including a card to gain access to a space or a password to log on to a computer system, biometric technologies determine characteristics that are unique to each person and would be difficult to alter.

There has been strong opposition to the commercial use of facial recognition technology (FRT). Google removed facial recognition apps and services. Europe ordered Facebook to discontinue the use of facial recognition for photo tagging. When he was in office, Senator Al Franken (D-MN) raised concerns about NameTag. Franken wrote to an app developer, calling for the delay of the app's release until best practices are established. Some leading privacy groups recommended that FRT be suspended until adequate safeguards were implemented.

An FRT system has four basic parts: a camera to capture an image, an algorithm to create a faceprint (also known as a facial template), a database of stored images, and an algorithm to compare the captured image to the database of images or a single image in the database. The quality of these components determines the effectiveness of the system. Also, the more similar the environments in which the images are compared—such as the background, lighting conditions, camera distance, and size and orientation of the head—the better a facial recognition technology system will perform.

FRTs are able to perform several functions, including (1) detecting a face in an image;



Flat Recognition Facial Face Woman System. (By teguhjatipras.)

(2) estimating personal characteristics, such as an individual's age, race, or gender; (3) verifying identity by accepting or denying the identity claimed by a person; and (4) identifying an individual by matching an image of an unknown person to a gallery of known people. FRT systems can generate two types of errors—false positives (reporting an incorrect match) or false negatives (not reporting a match when one exists). Studies of FRT algorithms have indicated that this technology has improved over time. Error rates continue to decline, and algorithms are getting better at identifying individuals from images of poor quality or that are captured under low light. Also, certain controlled tests have indicated that facial recognition algorithms surpassed humans in accurately identifying whether pairs of face images, taken under different lighting, were images of the same person or of different people.

Various federal agencies, privacy and consumer organizations, and some industry representatives have raised serious issues regarding the commercial use of FRT, including the technology's ability to identify and monitor individuals in public spaces without their knowledge, and around the collection, use, and sharing of personal data associated with the technology. FRT proponents argue that the technology has raised no new privacy risks or that such risks can be reduced.

Despite these concerns, FRT continues to improve rapidly in accuracy. Individuals continue to upload billions of pictures to social networking and other Internet sites, which develop a large repository of facial images. These images in turn are often linked to names or other personal information. The combination of these two trends may make it feasible to soon identify almost any individual in several public spaces. Privacy organizations, who have expressed concerns about the commercial application of facial recognition technology, have generally focused on (1) how it affects the ability of individuals to remain relatively anonymous in public; (2) the capacity to track individuals across locations; and (3) use of facial recognition without the individuals' knowledge or consent.

In rebuttal, FRT supporters have argued that

(1) individuals should not expect complete anonymity in public (individuals effectively relinquish some of their anonymity when they make their faces public);

(2) privacy and anonymity are not synonymous and that relinquishing complete anonymity is not the total abandonment of privacy (they also argue that capturing a facial image or faceprint in public does not necessarily infringe on an individual's anonymity because it does not directly reveal a name, Social Security number, or any other similar personal information);

(3) surveillance is already present in ordinary American life (commercial entities already routinely install security cameras) and that facial recognition does not increase their use;

(4) privacy advocacy organizations may have exaggerated the capabilities of FRT systems because cameras usually are not interconnected and it is not practical to implement commercial applications that would use multiple

cameras to track individuals' movements; and

(5) consumers seem willing to exchange some privacy for the security supposedly provided by surveillance technology.

Generally, FRT supporters assert that there are trade-offs between some loss of privacy and the benefits that new technologies give to consumers and businesses, and to economic growth that such technology supposedly creates.

Many FRT supporters also argue that (1) consumers' expectations and ideas of privacy have evolved because of technological innovation (for example, consumers have reportedly demonstrated their willingness to share private information in public settings—such as by posting to social networking sites to obtain benefits such as photo sharing and management; (2) the need for consent should depend on the context (i.e., the context in which FRT is used should have a bearing on issues of consumer consent); and (3) FRT should not be singled out because the privacy issues associated with FRT are largely identical to those of any biometric technologies, including voice or gait recognition, which also can identify individuals from some distance without their knowledge. Several FRT technology companies have said that lawmakers should protect personal information gathered from all biometrics, not only FRT. In addition, they argue that businesses that use the security technology should not be required to obtain consent before the technology is used because obtaining consent is not required for social networking sites, which have repositories of facial images that can be used to identify individuals more broadly.

Several government, industry, and privacy organizations have proposed or are developing privacy guidelines governing the commercial use of FRT, including describing how commercial organizations collect, use, and store data. FRT is found in several different consumer and business applications, but the extent of its current use in commercial settings is still largely unknown. The technology is commonly used in software that manages personal photographs and in social networking applications to identify friends. Also, several companies use FRT instead of a password to provide secure access to computers, phones, and gaming systems. FRT may have applications for customer service and marketing; however, in the United States, use 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 in retail stores, banks, and casinos incorporate facial recognition technology.

Many, including privacy groups and government agencies, have asserted several privacy concerns on the commercial use of FRT. They claim that, if FRT use became widespread, it could allow businesses or individuals to identify almost everyone in public without their knowledge or consent and to monitor the locations, movements, and associates of individuals. They have also expressed concerns that information collected or associated with FRT could be used, shared, or sold in ways that consumers do not understand, anticipate, or want to consent to. Some stakeholders disagree that the technology presents new or unusual privacy risks, again citing that individuals should not expect absolute anonymity in public and that some privacy loss is offset by the benefits that the technology gives to consumers and businesses.

Many government, industry, and privacy organizations have proposed voluntary privacy guidelines for commercial FRT use. 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.

No federal privacy law expressly regulates commercial uses of facial recognition technology, and laws do not fully address key privacy issues raised by stakeholders, 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 circumstances, such as information collected by healthcare entities and financial institutions. Also, courts have interpreted the Federal Trade Commission Act to require companies to abide by their stated privacy policies.

Face recognition data can be accessed without an individual's knowledge. With commercial uses of FRT increasing and replacing older access methods such as password log-ins, the technology continues to raise vexing privacy questions.

Facebook first started using FRT by licensing technology from another company, Face.com, which it acquired in 2012. Facebook then introduced a new app, known as Moments, using the same technology as in tag suggestions, which groups photos in a user's smartphone based on the faces identified. Photos can then be shared with specific friends as opposed to uploading them to Facebook. When a person is identified in a picture on Facebook, the biometric software remembers the face so it can be tagged in other photographs. Its current system (since 2016) is known as DeepFace.

Facebook Inc. claims that FRT enhances the user experience. However, privacy advocates argue that the company's technology, which was halted in Europe and Canada after privacy concerns were raised, should be implemented only with explicit permission or consent. In Europe, strict privacy laws forced Facebook in 2012 to delete data collected for its tag-suggestion feature following a probe by Irish authorities. Canadian authorities forced Facebook to turn off its tag suggestions in that country.

Facebook was sued for its FRT policy and practices in Illinois, which has one of America's strictest biometric privacy laws. The plaintiffs alleged that Facebook failed to notify users that the service was collecting facial data on users tagged in photos. The photo publishing site Shutterfly Inc. was sued in Illinois over that company's photo tagging feature.

Facebook attempted to defend its use of FRT, which develops a unique faceprint and which may be used to identify someone when he or she has already been identified through tagging. The technology powers a photo feature called tag suggestions, which is automatically turned on when users sign up for a Facebook account. The suggestions are made only to a user's friends. Tag suggestions make it easy for friends to tag each other in photos. When someone is alerted that he or she has been tagged in a photo, it is easier to take action, whether it is commenting, contacting the person who shared it, or reporting it to Facebook. Users can opt out at any time. However, this requires that they change their settings.

Privacy activists complained that the U.S. government's approach to regulating the use of face data by companies is insufficient in protecting privacy because face recognition data may be collected without a person's knowledge. These activists further argue that facial recognition is one of those categories of data where a very clear consent is necessary.

Some business leaders have opposed requiring prior consent. They argue that fears that facial data may be used to track people have been exaggerated because the technology supposedly reveals less information about a person's habits than most customers would reveal by using a mobile phone that also tracks and shares location data.

Privacy advocates have provided examples companies that obtained proper consent for FRT implementation. Google, for example, provides users of its Google app with the option to use face identification by turning on the "find my face" feature. Companies such as Microsoft Corporation, which was placing FRT into Windows 10, and MasterCard, which had plans for selfie verification for online payments, require the download of an app or the purchase of hardware.

Industries using FRT have generally agreed that a code of conduct should be implemented that would require companies using facial recognition to be transparent about their use of the technology. A notice or a sign might be the answer, but how much information would be required and through what means to gain consent of those being surveilled by FRT remain a hotly disputed issue.

Gretchen Nobahar

Further Reading

Cackley, Alicia Puente. *Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law: Report to the Ranking Member, Subcommittee on Privacy, Technology and the Law, Committee on the Judiciary, U.S. Senate*. Washington, DC: United States Government Accountability Office, 2015.

Denham, Elizabeth. *Investigation into the Use of Facial Recognition Technology by the Insurance Corporation of British Columbia*. Victoria: Office of the Information and Privacy Commissioner for British Columbia, 2012.

Dumas, M. Barry. *Diving into the Bitstream: Information Technology Meets Society in a Digital World*. New York: Routledge, 2012.

Kallen, Stuart A. *Are Privacy Rights Being Violated?* Detroit, MI: Greenhaven, 2006.

Laptop Computer–Based Facial Recognition System Assessment. Oak Ridge, TN: Oak Ridge Y-12 Plant, 2001.

Lee, Newton. *Facebook Nation: Total Information Awareness*. New York: Springer, 2013.

Li, Stan Z., and Anil K. Jain. *Handbook of Face Recognition,* 2nd ed. London: Springer London, 2011.

Mago, V. K. *Cross-Disciplinary Applications of Artificial Intelligence and Pattern Recognition Advancing Technologies*. Hershey, PA: Information Science Reference, 2012.

Marks, Murray K. *Computer-Graphic Facial Reconstruction*. Burlington, MA: Elsevier Academic Press, 2005.

What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing before the Subcommittee on Privacy, Technology and the Law of the Committee on the Judiciary, United States Senate, One Hundred Twelfth Congress, Second Session, July 18, 2014.

See also: Apps; Biometrics; Computers and privacy; Consumer privacy; Facebook; Google; Next Generation Identification

Fair Credit Reporting Act

Identification: Fair Credit Reporting Act (FCRA), Public Law No. 91–508, of 1970. An act that created new standards for credit reporting agencies (CRAs) to protect the privacy of consumers in credit reporting.

The Fair Credit Reporting Act (FCRA) fundamentally changed the way CRAs interact with businesses and the general public. Not all companies disseminating information are governed by the FCRA, but typically for-profit entities distributing information about private individuals do have to follow FCRA requirements. To enforce these new rights and responsibilities, the FCRA provides private rights of action for citizens alleging violations of the FCRA. The Federal Trade Commission (FTC) may also begin criminal actions for deceptive or unfair trade practices. In addition, the FCRA statutorily exempted CRAs from certain common law torts.

A CRA is an entity that, broadly speaking, gathers, organizes, and disseminates information about consumers to help evaluate their credit. Normally this information is in the form of a credit report. CRAs facilitate the movement of credit from lenders to borrowers by providing information to lenders concerning the credit history of borrowers. Credit history is strongly predictive of future borrower behavior, so lenders use this information to match borrowers to loans, interest rates, and other terms of the transaction. CRAs are vital because they gather and collate cost-effectively more information than a lender, such as a bank, could gather about a borrower. CRAs also play a vital role in changing borrower behavior because the prospect of a negative credit report provides inducement for borrowers to engage in responsible practices. The three major CRAs in the United States are Equifax, Experian, and TransUnion.

The FCRA was the result of consumer concerns about the scope of privatized data banks and the personal information that these banks held and gave to third parties. Before the FCRA,