**Biometric data vs privacy and data protection: a quick update**

Commercial use of biometric data exploded in recent years: software are now able to measure physical characteristics, such as fingerprints, retinas, hand and facial geometry, as well as voices to recognize people. The technology makes people’s life easier as their hand or voice may be enough to access their phone or bank account, one single click may be enough to be tagged in hundreds of photos. However, this data cannot be replaced like a password: it needs to be well protected. The wrong use of biometric recognition systems may end up bringing several companies to Court.

Facebook has already received a [class action complaint](#facebook). Plaintiffs alleged that Facebook amassed users' biometric data secretly and without consent. Specifically, they alleged that Facebook violated their privacy because the Tag Suggestions program – which scans uploaded photographs to identify faces - did not inform users that “their biometric identifiers (face geometry) were being generated, collected or stored”.

The action is still pending. On May 5, 2016, a California District Court ruled that Illinois 2008 Biometric Information Privacy Act ([BIPA](http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57%20)) applies and that plaintiffs stated a valid claim under the Illinois Act (740 ILCS 14), which requires companies to inform the person in writing about the purpose and length of time for which her biometric identifiers are being collected, retained or used. The BIPA also requires companies to obtain consent before “disclosing” the individual’s biometric information. The BIPA allows to recover for each violation either $1,000 or actual damages for negligent violations, or $5,000 or actual damages for intentional or reckless violations.

Similarly, [Shutterfly](#norberg) - which offers online digital photo sharing, as well as facial recognition capabilities - settled in March 2016 a [class action suit](#norberg) alleging the company violated the BIPA by creating a system permitting photos to be stored and searched using facial recognition technology.

Respectively in March and May 2016, also [Google Photos service](#Google) and [Snapchat](#norberg) received putative class actions for allegedly collecting, storing and using- without informed consent and in violation of BIPA – “users’ biometric identifiers and biometric information”.

The technology industry is not the only sector using biometric recognition systems. For example, also a national tanning salon chain has been accused of violating the BIPA by collecting customers’ fingerprints without obtaining their informed written consent. In this instance, the salon chain created $1.5 million Settlement Fund to repay customers submitting valid claims.

Interestingly, there are also cases dismissing biometric data privacy cases. For example, an Illinois District Court recently dismissed an action against Smarte Carte. The company operates electronic lockers in public places that use the renter's fingerprint as a "key." Plaintiff alleged that Smarte Carte retained his fingerprint biometric information without written consent in violation of the BIPA and sued for damages. He did not allege any harm from the violation. The Court dismissed the action noting that allegations of a mere violation of the act do not qualify: “how can there be an injury from the lack of advanced consent to retain the fingerprint data beyond the rental period if there is no allegation that the information was disclosed or at risk of disclosure?”

The outcome of the pending cases will help interpreting the scope of the BIPA, and allow to better understand new liabilities and privacy obligation pending on businesses relying on biometric recognition systems.

Under a legislative stand point, there is currently no federal laws regulating the collection of biometric information. Only Texas ([Tex. Bus. & Com. Code Ann. § 503.001](http://www.statutes.legis.state.tx.us/Docs/BC/htm/BC.503.htm)) and Illinois (BIPA) implemented state laws to protect biometric information. In Texas, the penalty for each violations is higher - $25,000 - and only the Texas attorney general can bring enforcement actions.

The U.S. privacy sectoral approach brought to the enactment of various industry-specific laws governing the use of biometric information, such as for example the Gramm-Leach Bliley Act ([GLBA](https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act)) in the financial world, the Family Educational Rights and Privacy Act (34 CFR Part 99 [FERPA](http://www.ecfr.gov/cgi-bin/text-idx?rgn=div5&node=34:1.1.1.1.33)) applicable to educational institutions, and the Health Insurance Portability and Accountability Act ([HIPAA](http://www.technethics.com/hipaa-health-insurance-portability-and-accountability-act-of-1996/)) for health-care providers.

The FTC contributed to the subject as well by issuing in 2012 recommended [best practices](#FTC) for companies using facial recognition technology.

Several States have data breach notification laws governing unauthorized access to residents’ biometric information, and breach response. Among the States that adopted such specification there are [Connecticut](https://www.cga.ct.gov/2015/ACT/pa/pdf/2015PA-00142-R00SB-00949-PA.pdf), [Iowa](https://coolice.legis.iowa.gov/cool-ice/default.asp?category=billinfo&service=iowacode&ga=83&input=715C), [Illinois](http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=2702), [Nebraska](http://nebraskalegislature.gov/laws/statutes.php?statute=87-802) and [Wyoming](http://legisweb.state.wy.us/2015/bills/SF0036.pdf). [North Carolina](http://www.ncga.state.nc.us/EnactedLegislation/Statutes/PDF/ByArticle/Chapter_75/Article_2A.pdf) and [Oregon](http://www.oregonlaws.org/ors/646A.604) consider the breach of biometric data as violation of personal information when in combination with the individual’s name.

Overall, considering the recent jurisprudencial debate as well as possible legislative developments, businesses shall plan well ahead before utilizing facial recognition systems. For example, it could be useful to thing about how could the concepts of transparency and consent apply to the treatment of biometric data, or how to apply a retention policy to such information.

More information is available at <http://www.technethics.com/?s=biometrics>

In re Facebook Biometric Info. Privacy Litig., 2016 U.S. Dist. LEXIS 60046 \* (N.D. Cal. May 5, 2016), is available at

*Pezen v. Facebook Inc., 1:15-cv-03484 (N.D. Ill. Apr. 21, 2015), Licata v. Facebook Inc., 1:15-cv-04022 (N.D. Ill. May 5, 2015), Patel v. Facebook Inc., 1:15-cv- 04265 (N.D. Ill. May 14, 2015), and Gullen v. Facebook Inc., 1:15-cv-07861 (N.D. Ill. Aug. 31, 2015) a*

*Norberg v. Shutterfly, Inc.*, 1:15-cv-05351 (N.D. Ill. June 17, 2015) Open PDF

(Rivera v. Google, Inc., No. 16-02714 (N.D. Ill. filed Mar. 1, 2016)) is available at <https://www.scribd.com/doc/305110213/RiveraVGoogle-Complaint?secret_password=pF0ud1GFWgzOXG4Avxd3>

Martinez v. Snapchat, Inc., No. BC621391 (Cal. Super. Ct. filed May 23, 2016) is available at <https://www.scribd.com/doc/316358704/MartinezVSnapchat-Complaint?secret_password=8wTj6laMavOvy352aEOE>

Collough v. Smarte Carte, Inc., 2016 U.S. Dist. LEXIS 100404 \* (N.D. Ill. Aug. 1, 2016)

FTC, *Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies* is available at <https://www.ftc.gov/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies>

More information on Sekura v. L.A. Tan Enterprises, Inc. is available at <http://www.fingerprintsettlement.com/>

Texas ([Tex. Bus. & Com. Code Ann. § 503.001](http://www.statutes.legis.state.tx.us/Docs/BC/htm/BC.503.htm))

Nebraska revised statute is available at <http://nebraskalegislature.gov/laws/statutes.php?statute=87-802>

Connecticut Public Act No. 15-142 is available at <https://www.cga.ct.gov/2015/act/pa/pdf/2015PA-00142-R00SB-00949-PA.pdf>

[Connecticut](https://www.cga.ct.gov/2015/ACT/pa/pdf/2015PA-00142-R00SB-00949-PA.pdf), [Iowa](https://coolice.legis.iowa.gov/cool-ice/default.asp?category=billinfo&service=iowacode&ga=83&input=715C), [Illinois](http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=2702), [Nebraska](http://nebraskalegislature.gov/laws/statutes.php?statute=87-802). The [North Carolina Identity Theft Protection Act](http://www.ncga.state.nc.us/EnactedLegislation/Statutes/PDF/ByArticle/Chapter_75/Article_2A.pdf)

### Oregon ORS 646A.604 is available at <http://www.oregonlaws.org/ors/646A.604>

Wyoming WY Stat § 6-3-901 is available at <http://legisweb.state.wy.us/2015/bills/SF0036.pdf>

Follow us on[](https://twitter.com/CGCFirm)& Like us on**[](https://www.facebook.com/Technethics?fref=ts)**

**Notes for uploading**

**Date** April 1, 2015

**Tag** DATA PROTECTION

**Keywords:**

**Jurisdiction:** Illinois

**Category** Privacy

**Sub-Category** Case Law