C|NET

How we can protect your vulnerable facial recognition data

The moment your facial recognition data is leaked, your identity may be forever compromised, as your facial features cannot be altered.

Nik Antoun June 11, 2020 4:22 p.m. PT

Sunartek Labs

Facial recognition technology is a game-changing feature that enables you to replace traditional passcodes and touch-identification use-cases. As an application end-user in the United States, you are justifiably concerned that data protection laws are insufficient to ensure the security of personal information that is stored in company databases.

The issue is that companies are not required by law to encrypt biometric data collected from end-users. This is a critical problem: in 2019, there were over five thousand data breaches, with nearly eight billion exposed records; this is an increase of thirty-three percent over the last year (Hodge). Without database encryption, a compromised security layer makes the data accessible to a hacker, rather than rendering the breached data unreadable.

The following sections prescribes a single solution with multiple steps that will enable you to help the movement on indubitably protecting your facial recognition data.

Identify Your Political Leaders

Our lawmakers in Congress are best-equipped for enabling changes to the database security and privacy practices of American-based companies. Proponents of regulated facial recognition data can turn to technology to find guidance:

- ✦ Use internet-based resources to identify the political leaders in your area.
- ✦ Understand the political direction, in terms of technology, that each representative is currently following.

If your representative is technically adept and understands the underlying issues with advanced identification technology, you will be able to initiate support for your proposal. However, if your political leaders are indifferent or not educated to this technical cause, you will have to provide a comprehensive narrative to support the urgency of unprotected databased that contains facial recognition data.

Contact and Advise Your Local State Representative to Introduce a Bill that Requires Database Encryption

Once you have identified your local congressperson and you understand their political path, in addition to their technical awareness, you can formulate your problem and solution statement to the direction you wish them to take on behalf of their constituents.

- ✦ Compose a letter or narrative to assist you over a phone call that summarizes your proposal.
- ✦ Have an active conversation.
- ✦ Be prepared with additional information to support database encryption.

If your Representative expresses that facial recognition is not widely used in your community and that they have more pressing matters to tend to, you can educate the office that biometric privacy leaks can permanently tarnish any individual's identity.

Educate and Promote Activism for People to Get Involved

There are many organized conferences focussed on database management and integrity that you can attend in order to locate and influence like-minded people that supports legally required database encryption and cybersecurity measures.

- ✦ Use the internet to find conferences that promote biometric data and cybersecurity.

- ✦ Identify sessions that promote the involvement of law-based regulations to improve cybersecurity for biometrical data.
- ✦ Network and establish connections with like-minded individuals, and organize a petition that demands changes to data protection laws.
- ✦ Promote the movement to implement nationwide requirements to encrypt databases that hold facial recognition data.

If you cannot travel to some of these events, find out if there are any virtual conferences that discusses the same issues. Another option is to create online informational content, such as articles and videos, which results to creating public awareness.

Conclusion

Be tenacious, informed, and persuasive so that others will join the call-to-action for lawmakers to pass and enforce the regulatory requirements for database encryption of personal and biometric data. Legal protection of facial recognition data will reduce end-user anxiety that their personal identity will be compromised and used for nefarious purposes.

Acknowledgement

Our thanks goes out to Nik Antoun for sharing his knowledge on facial recognition technology, and how to spread public awareness over the consequences of unprotected facial recognition data.

Nik Antoun is a Special Agent in Cybersecurity for the FBI. He has a Bachelor's of Science in Computer Science and Cybersecurity and a Bachelor's of Arts in Science, Technology, and Society.

References

43% of cloud databases are currently unencrypted. 7 February 2020. 1 May 2020. <https://www.helpnetsecurity.com/2020/02/07/cloud-databases-unencrypted/>.

Doffman, Zak. *New Data Breach Has Exposed Millions Of Fingerprint And Facial Recognition Records: Report*. 14 August 2019. 30 April 2020. <https://www.forbes.com/sites/zakdoffman/2019/08/14/new-data-breach-has-exposed-millions-of-fingerprint-and-facial-recognition-records-report/#37764c8c46c6>.

Facial Recognition System. Sunartek Labs, 2020, <https://www.sunartek.com/facial-recognition-system/>.

Guinness, Harry. *How Secure Are Face ID and Touch ID?* 23 October 2018. 29 April 2020. <https://www.howtogeek.com/350676/how-secure-are-face-id-and-touch-id/>.

Hewage, Chaminda. *Privacy and Security at Stake with the Increased Use of Biometrics?* 10 April 2020. 30 April 2020. <https://www.infosecurity-magazine.com/next-gen-infosec/stake-increase-biometrics/>.

Hodge, Rae. *"Welcome to the 2019 Data Breach Hall of Shame."* CNET, 27 Dec. 2019, 4:00am, <https://www.cnet.com/news/2019-data-breach-hall-of-shame-these-were-the-biggest-data-breaches-of-the-year/>.

Willingham, AJ. *"25 Ways to Be Politically Active (Whether You Lean Left or Right)."* CNN, Cable News Network, 23 Jan. 2017, www.cnn.com/2016/11/15/politics/ways-to-be-more-politically-active-trnd/index.html>.

[Word Count: 595]