Deep Fakes and Big Data: the Next Level of Cyber Warfare

Sze-Fung Lee/ Research Assistant
Benjamin C. M. Fung/ Professor
School of Information Studies at McGill University, Canada

Most people are unaware of the personal security risks confronting them when they make use of 21st Century technology. Threats are embedded in the facial recognition technology that opens your iPhone, Chatbots on your online shopping sites, and unmanned aerial vehicles (UAV) deployed in military operations. These technologies form a juggernaut of sophisticated devices storing your most personal details and posing significant security threats.

Every day, huge amounts of personal data are being vacuumed up by social media and communication apps alone. Platforms that do not provide end-to-end encryption, such as Twitter, Facebook messenger, and Snapchat, among the most popular social media apps, are particularly vulnerable to privacy breaches affecting consumers. Users of Chinese social media apps like WeChat and Tik Tok are at even greater risk as demonstrated by recent revelations of malpractice by the two providers. WeChat was exposed for secretly scanning users' stored photos, without authorization[1]. Tik Tok introduced a change in its US privacy policy earlier, allowing the app to collect users' biometric identifiers and biometric information such as faceprints and voiceprints[2]. The two applications have active users numbering 1.2 billion[3] and 700 million[4] respectively, according to 2020 statistics. Imagine the wealth of data amassed by the two apps, making unwitting users potential victims of mass surveillance, extortion, defamation, and disinformation. Indeed, the more collected data is available to feed AI algorithms, the more efficient and pernicious AI becomes in its capability to manipulate or abuse personal and biometric data. This creates a vicious cycle that continually advances the danger of data being deliberately used for criminal purposes.

Deep Fakes—the Next Level of Cyber and Information Warfare

Deep Fakes are constructed by machine learning and supported by a specific deep learning application known as the Generative Adversarial Networks (GAN), where two self-supervised algorithms can "learn" from each other. After thousands of training cycles, GAN's algorithms have become skillful at producing synthetic images that are hyper realistic deep fakes, making them exceptionally difficult to detect with the human eye[5][6]. Deployed for the purpose of spreading disinformation, deep fakes raise potentially disastrous consequences for leaders of democratic governments, as well as to international security.

Domestically, deep fakes are capable of assisting cyber-criminals to commit crimes of identity theft, fraud, blackmail and other malfeasance. All that is required is to gaining access to the targets' personal information and private data by deceiving the biometric security in smart technologies. For example, major banks like

---

[1] Boris, T. (2021). 'WeChat to stop scanning photos in background after influencers' exposè using Apple's Record App Activity'. Tech Times. Available at https://www.techtimes.com/articles/266431/20211009/wechat-stop-scanning-photos-background-wechat-scanning-photos-apple-record-app-activity.htm

[2] .Perez, S. (2021). 'TikTok just gave itself permission to collect biometric data on US users, including "faceprints and voiceprints"'. *TechCrunch*. Available at https://techcrunch.com/2021/06/03/tiktok-just-gave-itself-permission-to-collect-biometric-data-on-u-s-users-including-faceprints-and-voiceprints/

[3] Boris, T. (2021). 'WeChat to stop scanning photos in background after influencers' exposè using Apple's Record App Activity'. *Tech Times*. Available at https://www.techtimes.com/articles/266431/20211009/wechat-stop-scanning-photos-background-wechat-scanning-photos-apple-record-app-activity.htm

[4] Iqbal, M. (2021). 'TikTok Revenue and Usage Statistics (2021).' *Business of Apps*. Available at https://www.businessofapps.com/data/tik-tok-statistics/

[5] Chesney, R. and Citron, D. (2019). 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security'. *California Law Review*, Vol. 107, pp.1753-1819.

[6] Rossler, A. *et al.* (2019) "2019 Ieee/cvf International Conference on Computer Vision (iccv)," in *Faceforensics : Learning to Detect Manipulated Facial Images*. IEEE, pp. 1–11. doi: 10.1109/ICCV.2019.00009.

CIBC and RBC use voice verification security (voice ID) for their authentication services[7][8]. Despite the banks repeated reassurances that their authentication systems are secure, the BBC conducted tests that defeated the voice recognition security system of HSBC by deception, in 2017[9]. The test revealed that biometric security can be bypassed by sophisticated simulation, using deep fake technology. With sufficient data to feed the AI algorithm and the knowledge of how to apply it, a malefactor could impersonate literally anyone, doing anything in a fabricated video. Consider deep fake productions of former US president Obama's profanity laden outburst against Donald Trump [10] or instances of celebrities performing pornographic acts.

Perceptibly, when deep fakes are applied to spread disinformation, the effect may not end at defaming a public official and damaging his public image. Fair elections may be imperiled with resultant damage to the polars of democratic society. Given the relatively low cost, simple access, and authentic appearance of deep fake misrepresentation, the world is seeing more frequent and intensified use of the technology. State-sponsored disinformation runs at large through covert channels to stirring chaos among political and economic rivals around the world. It foments polarization, tearing the fabric of social and institutional orders. Additionally, when deep fakes are tailored to spark radical actions of certain target group; for instance, diaspora communities, or even far-right groups and extremists, such consequences would not only limit to the former frequently becoming vilified and victimized, but also long civil unrest that fundamentally undermining the state's authority and its liberal democracy.

Advances in AI affect the whole spectrum of security, at the personal and international levels. The situation likely will get worse in the foreseeable future. The remedy must be to strike a balance between technological advances and how it may be used, without compromising security and freedom of expression. That, however, is the most challenging question of all.

Biography

Sze-Fung Lee is a research assistant at McGill University. She holds a Master's Degree in International Security from University of Warwick. Her research interests are in security policy, hybrid warfare, nuclear proliferation, and the politics of Hong Kong. Benjamin Fung is a professor and Canada Research Chair in Data Mining for Cybersecurity at McGill University.

Bibliography

Boris, T. (2021). 'WeChat to stop scanning photos in background after influencers' exposè using Apple's Record App Activity'. *Tech Times*. Available at https://www.techtimes.com/articles/266431/20211009/wechat-stop-scanning-photos-background-wechat-scanning-photos-apple-record-app-activity.htm

Chesney, R. and Citron, D. (2019). 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security'. *California Law Review*, Vol. 107, pp.1753-1819.

Iqbal, M. (2021). 'TikTok Revenue and Usage Statistics (2021).' *Business of Apps*. Available at https://www.businessofapps.com/data/tik-tok-statistics/

[7] Perala, A. (2021). 'CIBC launches biometric onboarding service for Canadians'. *Find Biometrics*. Available at https://findbiometrics.com/cibc-launches-biometric-onboarding-service-canadians-080304/

[8] 'RBC secure voice'. Available at https://www.rbc.com/pensioners/files/RBC_Secure_Voice_FAQs_for_Pensioners_Eng.pdf

[9] Simmons, D. (2017). 'BBC fools HSBC voice recognition security system'. *BBC News*. Available at https://www.bbc.com/news/technology-39965545

[10] Vaccari, C. and Chadwick, A. (2020). 'Deepfakes' are here. These deceptive videos erode trust in all news media'. *The Washington Post*. Available at https://www.washingtonpost.com/politics/2020/05/28/deepfakes-are-here-these-deceptive-videos-erode-trust-all-news-media/

Kreps, S. and McCain, M. (2019). 'Not Your Father's Bots—AI Is Making Fake News Look Real'. *Foreign Affairs*. Available at https://www.foreignaffairs.com/articles/2019-08-02/not-your-fathers-bots

Perala, A. (2021). 'CIBC launches biometric onboarding service for Canadians'. *Find Biometrics*. Available at https://findbiometrics.com/cibc-launches-biometric-onboarding-service-canadians-080304/

Perez, S. (2021). 'TikTok just gave itself permission to collect biometric data on US users, including "faceprints and voiceprints"'. *TechCrunch*. Available at https://techcrunch.com/2021/06/03/tiktok-just-gave-itself-permission-to-collect-biometric-data-on-u-s-users-including-faceprints-and-voiceprints/

Rossler, A. *et al.* (2019) "2019 Ieee/cvf International Conference on Computer Vision (iccv)," in *Faceforensics : Learning to Detect Manipulated Facial Images*. IEEE, pp. 1–11. doi: 10.1109/ICCV.2019.00009.

RBC. 'RBC secure voice'. Available at https://www.rbc.com/pensioners/files/RBC_Secure_Voice_FAQs_for_Pensioners_Eng.pdf

Simmons, D. (2017). 'BBC fools HSBC voice recognition security system'. *BBC News*. Available at https://www.bbc.com/news/technology-39965545

Vaccari, C. and Chadwick, A. (2020). 'Deepfakes' are here. These deceptive videos erode trust in all news media'. *The Washington Post*. Available at https://www.washingtonpost.com/politics/2020/05/28/deepfakes-are-here-these-deceptive-videos-erode-trust-all-news-media/