# The End to Privacy

By Conor Gilmer

***Abstract*— With almost every aspect of daily life now digitally collected, with sophisticated algorithms analysing this data, and smart technology which identifies people and retrieves in depth information on them, is privacy as we know it at an end? In this report we consider the feasibility that technological advances will result in an end to privacy, technical and non-technical obstacles to a service providing personal information at any time, the positives, negatives and other implications, and can privacy be protected in some way. As technology advances, the volume of data gathered and analysis providing insights on people, it's difficult to see how privacy can be maintained, even with commitments to obfuscating personal data and regulations protecting privacy as much as possible, we have to reconcile ourselves to a post-privacy age.**

***Index Terms*—Privacy, Facial Recognition,**

## I. Introduction

With Big Tech companies tracking our every click, our retail habits, your location betrayed by CCTV, mobile phone, or by using bank or travel cards, are the days of privacy behind us?

We enter a *Faustian pact*, subconsciously trading our privacy to companies providing services such as search, email, maps, social media, [1] online retail and payments etc., without much consideration as to what information and insights you provide them from which they can exploit for commercial gain.

With your digital footprint, your likes, dislikes, content consumption, associations, interests, location, [2] almost every metric of your existence, collected and aggregated using Artificial Intelligence and Machine Learning, even intimate information, is revealed about you.

## II. A Shazam for People

Vic Grout in "The Professor on the Train", [3] presents us with a scenario, where just by observing someone, could we deduce information from their appearance, behaviour, and some google searches.

Fictionally Sherlock Holmes could forensically derive an accurate picture from such a scenario, we would be limited and dependent on our guesswork, assumptions, our knowledge and prejudices.

Could there be a mobile phone or smart glasses App, a *Shazam for People*, [4] identifying someone from their image, accessing every minute detail about them from vast amounts of data stored online.

Is this privacy ending technology feasible? And is the intrusion tolerable?

## III. Is it Feasible?

In many ways the technological components are already available.

Phenomenal amounts of data are already collected by search engines, social media, retailers, online services and increasingly with the Internet of Things. [5]

Available technologies such as distributed storage and parallel processing capable of dealing with large datasets, [6] imposing systematic design [7] on enormous amounts of data, structured and unstructured, gathered from diverse sources and locations. [8] A unique identifier and informative metadata is crucial for data to be useful. [9]

Developments in facial recognition software [10] [11] [12], would enable a *Shazam for people*, uniquely identifying someone from a picture, a central database of images (and biometric data) and from this accessing all information on them.

Privacy is greatly compromised by artificial intelligence and machine learning algorithms ability to deduce detailed information about someone, finding co-relations and patterns, far beyond human capabilities, from what seems like innocuous information. [13]

In a 2015 study [14] on algorithms judging a person's personality based on their Facebook likes, found the algorithm needed only 10 likes to be as accurate as a work colleague of the person, 100 likes to be as accurate as an immediate family member, and 200 likes to be as accurate as a spouse or partner. [15]

It's argued AI could ascertain more intimate information such as politics, [16] sexual preference and even criminal inclination [17].

Science Daily [18] claims only four pieces of data are required to identify you, and more worryingly your credit-card information, with these technological capabilities, privacy cannot be maintained.

Perhaps non-technical obstacles are more likely to limit its development, with possible privacy/data protection legislation or people not accepting the intrusion of being constantly monitored. [19]

## IV. Advantages

For businesses it is tremendously powerful to target

potential customers with personalised marketing [20] predicting and even modifying an individual's behaviour, [21] [22] based on their profile, previous behaviour, and corelated

to others with similar profiles and patterns of behaviour. [23]

Users benefit from the convenience of suggestions for content, products and services, they're genuinely interested in, based on their profile. [24] It can be symbiotic where others benefit from data gathered on you (e.g. Google Maps using information from you, to suggest the best route to others.)

There are benefits when engaging with health services and government bodies, that your data and records are available quickly via facial recognition.

Tracking the spread of diseases [25] Ebola [26], Flu, and Coronavirus is invaluable for governments and healthcare.

Detailed data on people, the ability to identify someone using facial, biomechanical and gait [27] analysis of a picture, will assist police and security services solving crimes and locating missing people. [28]

Peoples everyday experience could be enhanced by information being available, [19] for the Visually impaired information on what the smart device camera sees, [29] can be analysed and turned into audio.

## V. Disadvantages

People value privacy and have concerns with their information available to companies and governments, perhaps not Orwellian like consequences, [30] but Search engines, social media and phone companies have information the East-German Stasi could only dream about. [31]

The storage and tracking of people's data, conflicts with civil liberties as perceived in liberal democracies, for example coronavirus tracking mobile apps proved controversial [32] (I uncomfortably acknowledge it was beneficial for countries unburdened by civil liberty concerns during the pandemic).

Data-leaks and access to data on you, puts you at risk of identity theft, and risks your personal security.

Yeung [33] highlights five fears, where predictive personalisation based on data gathered can facilitate consumer exploitation, manipulate people, discrimination against low value customers, perpetuates inequality and fuels narcissism.

Personalisation can limit your online experience, insulating you from diverse and contrary views, confining you to an echo chamber a walled garden, fermenting the polarisation of opinions. [34]

## VI. Can privacy be maintained

Privacy can be helped by encrypting data stored and transferred online, also companies obfuscated personal data, while enabling the provision of a service, [35] data deidentification, differential privacy on queries [36, p. 300] and anonymizing data so its useable without compromising privacy. [37]

Governments could legislate to protect privacy, with GDPR the EU, has been successful focusing companies on handling personal data responsibly, since there are real financial punishments for failure to do so. [38]

With legislation private data could become, a liability [9] (as well as an asset) for companies, legally obliged to maintain an individual's privacy throughout the lifecycle of their data, however unethical companies may not comply, compromising privacy.

## VII. Other Implications

With technology able to collect data on you from other people's devices, [11] [39] [1] without your knowledge or consent, is ethically and legally questionable.

Access to such information, would interfere in our lives, fundamentally affecting our behaviour, experiences, and social interaction with others. We have yet to define rules of engagement, for social media and the online world, I believe it would be naïve to expect, we could have such rules or be psychologically prepared [40] when a *Shazam for People* is in our everyday lives.

## VIII. What the future holds

Technology is only going to improve with greater capabilities and greater intrusion.

Bionic implants will provide a surreptitious way to access the technology, data from implants or smart glasses monitoring eye movements recording what attracts someone and their surroundings, people effectively becoming data gatherers. Health metrics dynamically collected and communicated to your doctor. Technology and human merging, where it augments our memory, and reasoning.[41]

## IX. Conclusion

While the power to access endless information on someone at a point of interaction, has tremendous benefits for companies and governments. The volumes of data available coupled with computational powers to analyse and deduce information, effectively renders privacy as we have known it a thing of the past.

For privacy to be maintained in some form, requires government regulation, a right to be forgotten, [42] the right to withdraw consent, [9, p. 404] a right to know what data companies store and generate about us.

Even with regulation, companies protecting our data as much as possible we have to reconcile ourselves that we are fast approaching a post-privacy age.

## References

[1] J. DeHart and C. Grant, "Visual Content Privacy Leaks on Social Media Networks.," Computers and Society (cs.CY), 22 6 2018. [Online]. Available: https://arxiv.org/abs/1806.08471.

[2] D. Curran, "Are you ready? Here is all the data Facebook and Google have on you," The Guardian, 19 10 2018. [Online]. Available: https://www.theguardian.com/commentisfree/2018/mar/28/all-the-data-facebook-google-has-on-you-privacy.

[3] V. Grout, "The 'Prof on a train' game," Turing's Radiator , 23 8 2015. [Online]. Available: https://vicgrout.net/2015/08/23/the-prof-on-a-train-game/.

[4] V. Grout, "No More Privacy Any More?," MDPI, 9 1 2019. [Online]. Available: https://www.mdpi.com/journal/information/special_issues/End_of_Privacy.

[5] B. Marr, "How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read," Forbes.com, 21 5 2018. [Online]. Available: https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/?sh=bfbf9ce60ba9.

[6] A. F. Gates, O. Natkovich, S. Chopra, P. Kamath, S. Narayanamurthy, C. Olston, B. Reed, S. Srinivasan and U. Srivastava, "Building a high-level dataflow system on top of Map-Reduce: the Pig experience," 2009. [Online]. Available: https://dl.acm.org/doi/10.14778/1687553.1687568.

[7] X. . Wu, X. . Zhu, G. . Wu and W. . Ding, "Data mining with big data," *IEEE Transactions on Knowledge and Data Engineering,* vol. 26, no. 1, pp. 97-107, 2014.

[8] A. Danna and O. H. Gandy Jnr, "All That Glitters Is Not Gold: Digging Beneath the Surface of Data Mining," Journal of Business Ethics , 2002. [Online]. Available: https://repository.library.georgetown.edu/handle/10822/1006759.

[9] J. J. Berman, Principles and Practice of Big Data, Second Edition ed., Academic Press, 2018.

[10] G. Guo and H.-J. Zhang, "Boosting for fast face recognition," www.face-fac.org, 2001. [Online]. Available: http://face-rec.org/algorithms/boosting-ensemble/ratfg-rts01guo.pdf.

[11] B. Guarino, "Russia's new FindFace app identifies strangers in a crowd with 70 percent accuracy," The Washington Post, 18 5 2016. [Online]. Available: https://www.washingtonpost.com/news/morning-mix/wp/2016/05/18/russias-new-findface-app-identifies-strangers-in-a-crowd-with-70-percent-accuracy/.

[12] S. Walker, "Face recognition app taking Russia by storm may bring end to public anonymity," The Guardian, 17 5 2016. [Online]. Available: https://www.theguardian.com/technology/2016/may/17/findface-face-recognition-app-end-public-anonymity-vkontakte.

[13] Y. Inbar, "Mining Big Data to Extract Patterns and Predict Real-Life Outcomes [Michal Kosinski]," Centre for Open Source, 2 2 2017. [Online]. Available: https://osf.io/rg9xu/#!.

[14] W. . Youyou, M. . Kosinski and D. . Stillwell, "Computer-based personality judgments are more accurate than those made by humans," *Proceedings of the National Academy of Sciences of the United States of America,* vol. 112, no. 4, pp. 1036-1040, 2015.

[15] C. B. Parker, "Michal Kosinski: Computers Are Better Judges of Your Personality Than Friends," Sanford Graduate School of Business, 23 1 2015. [Online]. Available: https://www.gsb.stanford.edu/insights/michal-kosinski-computers-are-better-judges-your-personality-friends.

[16] S. Levin, "Face-reading AI will be able to detect your politics and IQ, professor says," The Guardian, 12 9 2017. [Online]. Available: https://www.theguardian.com/technology/2017/sep/12/artificial-intelligence-face-recognition-michal-kosinski.

[17] A. Charles, "Why Minority Report was spot on," The Guardian, 16 6 2010. [Online]. Available: https://www.theguardian.com/technology/2010/jun/16/minority-report-technology-comes-true.

[18] Massachusetts Institute of Technology, "Privacy challenges: Just four vague pieces of info can identify you, and your credit card," Science Daily, 29 01 2015. [Online]. Available: https://www.sciencedaily.com/releases/2015/01/150129160856.htm.

[19] M. Honan, "I, Glasshole: My Year With Google Glass," Wired.com, 30 12 2013. [Online]. Available: https://www.wired.com/2013/12/glasshole/.

[20] R. Gray, "Minority Report-style advertising billboards to target consumers," Telegraph Technology, 1 8 2010. [Online]. Available: https://www.telegraph.co.uk/technology/news/7920057/Minority-Report-style-advertising-billboards-to-target-consumers.html.

[21] S. . Zuboff, "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization," *Journal of Information Technology,* vol. 30, no. 1, pp. 75-89, 2015.

[22] T. . Bartley, "The Digital Surveillance Society," *Contemporary Sociology,* vol. 48, no. 6, pp. 622-627, 2019.

[23] S. Zuboff, "A Digital Declaration: Big Data as Surveillance Capitalism," Frankfurter Allgemeine Zeitung, 14 9 2014. [Online]. Available: http://www.faz.net/1.3152525.

[24] A. Mahdawi, "It's not just A-levels – algorithms have a nightmarish new power over our lives," The Guardian - Opinion, 19 8 2020. [Online]. Available: https://www.theguardian.com/commentisfree/2020/aug/19/its-not-just-a-levels-algorithms-have-a-nightmarish-new-power-over-our-lives.

[25] M. U. Ilyas and J. S. Alowibdi, "Disease Tracking in GCC Region Using Arabic Language Tweets," Companion Proceedings of the The Web Conference 2018, 4 2018. [Online]. Available: https://doi.acm.org/10.1145/3184558.3186357.

[26] M. Wall, "Ebola: Can big data analytics help contain its spread?," BBC Business, 14 10 2014. [Online]. Available: https://www.bbc.com/news/business-29617831.

[27] M. Nirenberg, "Gait, Footprints, and Footwear: How Forensic Podiatry Can Identify Criminals," Police Chief Magazine, 1 2016. [Online]. Available: https://www.policechiefmagazine.org/gait-footprints-and-footwear-how-forensic-podiatry-can-identify-criminals/.

[28] A. Cuthbertson, "Indian Police trace 3000 missing children in just four days using facial recognition technology," Independent, 24 4 2018. [Online]. Available: https://www.independent.co.uk/life-style/gadgets-and-tech/news/india-police-missing-children-facial-recognition-tech-trace-find-reunite-a8320406.html.

[29] T. Macaulay, "Google's AI-powered smart glasses help the blind to see," The Nextweb, 9 3 2020. [Online]. Available: https://thenextweb.com/plugged/2020/03/09/googles-ai-powered-smart-glasses-help-the-blind-to-see.

[30] G. Orwell, "1984 (Nineteen Eighty Four)," fadedpage.com, 1949. [Online]. Available: https://www.fadedpage.com/showbook.php?pid=20120511.

[31] A. Curry, "Piecing Together the Dark Legacy of East Germany's Secret Police," Wired.com, 18 1 2008. [Online]. Available: https://www.wired.com/politics/security/magazine/16-02/ff_stasi?currentPage=all.

[32] P. Lapolla and R. Lee, "Privacy versus safety in contact-tracing apps for coronavirus disease 2019," Digital Health, 20 7 2020. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7364796/.

[33] K. . Yeung, "Five fears about mass predictive personalisation in an age of surveillance capitalism," *International Data Privacy Law,* vol. 8, no. 3, pp. 258-269, 2018.

[34] "Cambridge Analytica Was Doing Marketing, Not Black Magic," , . [Online]. Available: https://reason.com/blog/2018/03/19/cambridge-analytica.

[35] Y. Du, G. Cai, X. Zhang, T. Liu and J. Jiang, "An Efficient Dummy-Based Location Privacy-Preserving Scheme for Internet of Things Services," Information 2019, 5 9 2019. [Online]. Available: https://www.mdpi.com/2078-2489/10/9/278.

[36] R. Buyya, R. N. Calheiros and A. V. Dastjerdi, Big Data Principles and Paradigms, Cambridge MA: Morgan Kaufmann, 2016.

[37] K. Nagaraj, S. GS and A. Sridhar, "Encrypting and Preserving Sensitive Attributes in Customer Churn Data Using Novel Dragonfly Based Pseudonymizer Approach," Information 2019, 31 8 2019. [Online]. Available: https://www.mdpi.com/2078-2489/10/9/274..

[38] "General Data Protection Regulation (GDPR)," Intersoft Consulting / EU, 14 4 2016. [Online]. Available: https://gdpr-info.eu/.

[39] J. DeHart, C. Grant and M. Stell, "Social Media and the Scourge of Visual Privacy," MDPI, 21 1 2020. [Online]. Available: https://www.mdpi.com/2078-2489/11/2/57.

[40] M. Aiken, The Cyber Effect, New York: Random House, 2017.

[41] R. C. Kurzweil, "The Singularity Is Near," 2005. [Online]. Available: https://amazon.com/singularity-near-humans-transcend-biology/dp/0143037889.

[42] "Right to erasure," Information Commissioner's Office, [Online]. Available: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/.