Volume 1, No. 4 | July–August 2018

RAIL

The Journal of Robotics, Artificial Intelligence & Law

fastcase FULL COURT PRESS

RAIL

The Journal of Robotics,
Artificial Intelligence & Law

Volume 1, No. 4 | July–August 2018

THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW (ISSN 2575-5633 (print) /ISSN 2575-5617 (online) at $495.00 annually is published six times per year by Full Court Press, a Fastcase, Inc., imprint. Copyright 2018 Fastcase, Inc. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated into any information retrieval system without the written permission of the copyright owner. For customer support, please contact Fastcase, Inc., 711 D St. NW, Suite 200, Washington, D.C. 20004, 202.999.4777 (phone), 202.521.3462 (fax), or email customer service at support@fastcase.com.

Publishing Staff
Publisher: Morgan Morrissette Wright
Journal Designer: Sharon D. Ray
Cover Art Design: Juan Bustamante

Cite this publication as:

The Journal of Robotics, Artificial Intelligence & Law (Fastcase)

This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

A Full Court Press, Fastcase, Inc., Publication

Editorial Office

711 D St. NW, Suite 200, Washington, D.C. 20004
https://www.fastcase.com/

POSTMASTER: Send address changes to THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW, 711 D St. NW, Suite 200, Washington, D.C. 20004.

Articles and Submissions

Direct editorial inquires and send material for publication to:

Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@meyerowitzcommunications.com, 646.539.8300.

Material for publication is welcomed—articles, decisions, or other items of interest to attorneys and law firms, in-house counsel, corporate compliance officers, government agencies and their counsel, senior business executives, scientists, engineers, and anyone interested in the law governing artificial intelligence and robotics. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the Editorial Content appearing in these volumes or reprint permission, please call:

Morgan Morrissette Wright, Publisher, Full Court Press at mwright@fastcase.com or at 202.999.4878

For questions or Sales and Customer Service:

Customer Service
Available 8am–8pm Eastern Time
866.773.2782 (phone)
support@fastcase.com (email)

Sales
202.999.4777 (phone)
sales@fastcase.com (email)
ISSN 2575-5633 (print)
ISSN 2575-5617 (online)

Everything Is Not *Terminator*

Using State Law Against Deceptive AI's Use of Personal Data

John Frank Weaver*

Although killer drones and autonomous weapons get the most publicity when it comes to the dangers of artificial intelligence ("AI"),[1] there is growing evidence of the dangers posed by AI that can deceive human beings. A few examples from recent headlines:

- AI that can create videos of world leaders—or anyone—saying things they never said;[2]
- Laser phishing, which uses AI to scan an individual's social media presence and then sends "false but believable" messages from that person to his or her contacts, possibly obtaining money or personal information;[3] and
- AI that analyzes data sets containing millions of Facebook profiles to create marketing strategies to "predict and potentially control human behavior."[4]

The last technique was reportedly used in the 2016 American presidential election.[5] The Facebook profiles in question were supposedly obtained through illicit means, giving Cambridge Analytica, the entity creating the marketing strategies, a wealth of personal data to feed to its AI for analysis.[6]

The problems created by AI doing this work is immediately apparent, particularly to those involved with the technology. "The dangers of not having regulation around the sort of data you can get from Facebook and elsewhere is clear. With this, a computer can actually do psychology, it can predict and potentially control human behavior . . . It's how you brainwash someone. It's incredibly dangerous," notes Jonathan Rust, the director of the Psychometric Centre at the University of Cambridge, which did much of the research Cambridge Analytica relies on.[7] He goes on to warn, "It's no exaggeration to say that minds can be changed . . . People don't

Robotics, Artificial Intelligence & Law / July–August 2018, Vol. 1, No. 4, pp. 267–275.

ISSN 2575-5633 (print) / ISSN 2575-5617 (online)

know it's happening to them. Their attitudes are being changed behind their backs."[8]

Massachusetts Attorney General Maura Healey has announced that her office will investigate how Facebook and Cambridge Analytica obtained and used the personal data.[9] However, did Facebook and Cambridge Analytica actually break Massachusetts, or any state, law in a way that is enforceable?[10] If not, what does that say about the state of AI regulation and legal protection for individuals in this country?

Personal Data v. Personal Information in American Law

Data, particularly personal data, is the lifeblood of AI.[11] With enough data, AI can create original art,[12] write natural language reports and narratives,[13] and provide and improve personal assistant services through devices like Amazon's Alexa and Echo.[14] As the examples of deceptive AI above demonstrate, AI can also use personal data to mislead human users. Despite the apparent danger, American law focuses on protecting personal information in order to prevent identity theft, but is largely unconcerned with AI and personal data.

What's the difference between personal data and personal information? Personal data is a broad category of data that includes personal information. Compare the definition of personal data from the European Union's General Data Protection Regulation ("GDPR") and the definition of personal information used in Massachusetts:[15]

- *Personal data:* any information relating to an identified or identifiable natural person.[16]
- *Personal information:* a resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident:
  - Social Security number;
  - Driver's license number or state-issued identification card number; or
  - financial account number, or credit or debit card number, with or without any required security code, access

> code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public.[17]

The EU uses personal data in an incredibly broad sense. Anything about you that can be connected to you is personal data: name, social security number, bank account, credit card, internet browsing history, Amazon purchases, social media posts and viewing habits, news articles written about and by you, tweets you are mentioned in, etc. The United States uses personal information narrowly by comparison, focusing on information that could lead to a bad actor gaining access to your credit card or finances. These definitions are consistent with the different approaches to data and privacy in the EU, where privacy and the protection of personal data are considered a fundamental right,[18] and in the United States, where one of the goals of data regulation is to ensure commerce continues to run smoothly.[19]

Did Facebook and Cambridge Analytica Violate Any State Laws?

In considering whether or not Facebook and Cambridge Analytica have violated any state laws, it is useful to look briefly at what is required in Europe. Under the GDPR, before any party can capture an individual's personal data, they must inform the subject individual how the personal data will be used[20] and must also frequently obtain the consent of that person.[21] If Facebook wants to collect your data and sell it to a third party for use in marketing, it must first tell you it is going to do that and obtain your consent. If you want to withdraw your consent, you have that right.[22] The GDPR also guarantees the "right to be forgotten," which grants individuals the right to require that entities with their personal data erase all of their personal data, subject to certain conditions.[23]

State data privacy laws in America are much more limited with regard to sharing personal data. California requires that each party collecting personally identifiable information—a term that is somewhere between personal information and personal data in terms of breadth[24]—conspicuously post its privacy policy, and that requirement has become a widely followed best practice.[25] However, consent is rarely required before a data capturer can share personal data with a third party.[26] Almost every state has a data security breach law, which, in one form or another, requires a party to notify all affected individuals when it experiences a security breach in which those individuals' personal information is compromised.[27] But those laws do not apply to personal data broadly, only to personal information. It is unclear at this time if the personal data from the Facebook accounts that Cambridge Analytica included the necessary combinations of name, addresses, credit card number, etc. to be applicable.

At least 15 states have specific statutes and/or regulations that require entities that store personal information to have data security measures.[28] However, in general, these state-specific standards may not be very useful in pursuing a legal action against Facebook or Cambridge Analytica because they are general and broadly worded. Most states have only specified that the parties protecting personal information "take reasonable measures to protect and secure" the personal information,[29] "implement and maintain reasonable procedures . . . to protect and safeguard from unlawful use or disclosure" the information,[30] "implement and maintain reasonable procedures and practices appropriate to the nature of the information, and exercise reasonable care to protect the personal information,"[31] etc. Not surprisingly, Massachusetts has provided much more detailed requirements governing how to protect the relevant personal information. These requirements include designating specific employees to maintain security programs,[32] requiring that service providers implement security measures,[33] and requiring that covered entities maintain a security system covering their computers that satisfies specific criteria, such as adopting secure user authentication protocols and encryption.[34]

With regard to the data protection statutes discussed above, Attorney General Healey might have the most success conducting discovery to address four specific issues:

1. Did the Facebook profiles obtained by Cambridge Analytica contain personal information as defined in Massachusetts law?
2. If the profiles contained personal information, when did Facebook first realize that Cambridge Analytica's

possession of the profiles constituted a leak that should be disclosed per Massachusetts law?

3. When did Facebook make that disclosure?
4. Do the data security programs used by Facebook and Cambridge Analytica satisfy Massachusetts' law?

Attorneys general in other states looking to pursue a claim against Facebook and Cambridge Analytica would look at similar questions under their laws.

If this discovery does not yield information sufficient to pursue a complaint under data protection statutes, states could seek remedy under their consumer protection acts, alleging that Facebook and Cambridge Analytica engaged in unfair and deceptive trade practices by sharing more personal data with a third party than permitted by an individual's privacy settings (for Facebook) and by using individuals' personal data for illicit persuasion and other purposes without their consent or knowledge (for Cambridge Analytica). It is unclear how successful this strategy would be. On the one hand, the Federal Trade Commission initiated a complaint against Facebook in 2011, alleging that the company's privacy settings were deceptive.[35] That complaint resulted in a consent decree in which Facebook agreed to implement a data privacy system and to obtain a user's consent before sharing his or her personal data—not just personal information—with a third party in a way that exceeds that user's privacy settings.[36]

However, in some ways the federal government had an advantage in that there was no statute governing the notice and consent necessary before entities like Facebook can use a user's personal data or personal information. In contrast, states may find that the standards created by their data protection acts thwart complaints like the FTC's. Courts could reasonably ask how could Facebook or Cambridge Analytica have engaged in unfair or deceptive trade practices if (a) their treatment of personal information complied with the relevant state laws, and (b) state laws are silent on personal data?

What Does the State of Personal Data Governance Mean for AI Regulation?

Episodes like the Cambridge Analytica affair underscore the importance of elected officials, government regulators, and public policy makers regulating all elements of AI, including personal data. The data security privacy laws in the United States, at both the federal and state levels, are woefully inadequate to govern how AI uses personal data. By focusing on personal information and traditional identity theft, American law ignores the danger of deceptive AI that either uses personal data to pose as a real person or to market deceptive information. Whether this inaction is due to ignorance, lack of interest, lack of will, a conscious decision to favor ecommerce over individual privacy, or some combination, the deceptive AI activities identified at the beginning of this article should alert legislators and policy makers that decisive statutory and regulatory action is required. Fortunately, there are numerous models to follow, from the EU's strategy of ensuring that everyone is able to protect and maintain control over their personal data[37] to the concept of governing the life cycle of personal data.[38]

I can understand the concerns regarding early regulation of AI technology—even if I do not agree with them—but Cambridge Analytica demonstrates that there can be no concerns regarding regulating AI's fuel, personal data. The only concern is not regulating it.

Notes

[*] John Frank Weaver, an associate at McLane Middleton and a member of the firm's privacy and data security practice groups, is the "Everything Is Not *Terminator*" columnist for *The Journal of Robotics, Artificial Intelligence & Law.* Mr. Weaver, who may be contacted at john.weaver@mclane.com, has a diverse practice that focuses on land use, real estate, telecommunications, and emerging technologies, including artificial intelligence, self-driving vehicles, and drones.

[1] *See* Campaign to Stop Killer Robots, https://www.stopkillerrobots.org/; Ban Lethal Autonomous Weapons, https://autonomousweapons.org/.

[2] Supasorn Suwajanakorn, Steven M. Seitz, & Ira Kemelmacher-Shlizerman, *Synthesizing Obama: Learning Lip Sync from Audio,* http://grail.cs.washington.edu/projects/AudioToObama.

[3] Charlie Warzel, "Infocalypse Now," *Buzzfeed,* February 11, 2018, https://www.buzzfeed.com/charliewarzel/the-terrifying-future-of-fake-news?utm_term=.unYkdQY8x#.jsGvbP3MO.

[4] Carole Cadwalladr, "Robert Mercer: the big data billionaire waging war on mainstream media," *The Guardian,* February 26, 2017, https://www.theguardian.com/politics/2017/feb/26/robert-mercer-breitbart-war-on-media-steve-bannon-donald-trump-nigel-farage.

[5] Carole Cadwalladr, "The Cambridge Analytica Files," *The Guardian,* March 18, 2018, https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump.

6. Matthew Rosenberg, Nicholas Confessore, & Carole Cadwalladr, "How Trump Consultants Exploited the Facebook Data of Millions," *New York Times,* March 17, 2018, https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

7. Carole Cadwalladr, *supra* note 4.

8. *Id.*

9. Jennifer Hansler, "Massachusetts AG to investigate Facebook, Cambridge Analytica," *CNN,* March 18, 2018, https://www.cnn.com/2018/03/18/politics/massachusetts-ag-cambridge-analytica/index.html. It seems likely that other attorneys general will pursue similar investigations, but as of this writing, Attorney General Healey is the only AG who has announced an investigation. As a result, I focus largely on her efforts in Massachusetts.

10. It is an open question as to whether Cambridge Analytica actually falls within Massachusetts' jurisdiction. I am assuming that is the case and so do not address that issue here. Also, because this article focuses on state law, I only discuss the 2012 U.S. Federal Trade Commission Decision and Order affecting Facebook as an example of a consumer protection action that states could use as a model. *See In the Matter of Facebook, Inc.*, Docket No. C-4365, Decision and Order, U.S. Federal Trade Commission, *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf ("2012 FTC Decision").

11. *See* Robert Seamans, "Artificial Intelligence And Big Data: Good For Innovation?," *Forbes,* September 7, 2017, *available at* https://www.forbes.com/sites/washingtonbytes/2017/09/07/artificial-intelligence-and-big-data-good-for-innovation/#5019a104ddb0 ("The most dramatic advances in AI are coming from a data-intensive technique known as machine learning. Machine learning requires lots of data to create, test and 'train' the AI.").

12. Cade Metz, "How A.I. Is Creating Building Blocks to Reshape Music and Art," *New York Times,* August 14, 2017, *available at* https://www.nytimes.com/2017/08/14/arts/design/google-how-ai-creates-new-music-and-new-artists-project-magenta.html ("The project is part of a growing effort to generate art through a set of A.I. techniques.... Called deep neural networks, these complex mathematical systems allow machines to learn specific behavior by analyzing vast amounts of data.").

13. Patrick Seitz, "Narrative Science Turning Big Data Into Plain English," *Investors.com,* August 21, 2012, http://news.investors.com/technology/082112-622940-narrative-science-takes-data-analytics-to-next-level.htm?p=full ("The possibilities are limitless for turning data into plain English articles. Government data like employment, trade and other economic statistics can be turned into readable reports 'super quick' and at 'outrageous scale.'").

14. George Anders, "Alexa, Understand Me," *MIT Technology Review,* August 9, 2017, *available at* https://www.technologyreview.com/s/608571/alexa-understand-me/ (noting that Echo devices with Alexa use "an artificial intelligence system building upon, and constantly learning from, human data ... The more time Alexa spends with its users, the more data it collects to learn from, and the smarter it gets.").

15. It should be noted that although there are federal laws governing some specific types of personal data (Health Insurance Portability and Accountability Act, Children's Online Privacy Protection Act, Fair Credit Reporting Act Fair, etc.),

there is no federal law governing personal data or personal information broadly. Massachusetts, in addition to being the state where Attorney General Healey is beginning an investigation, is recognized as having one of the toughest, if not the toughest, data privacy requirements in the United States. Kevin D. Lyles, Maricio F. Paez, & Alfred Cheng, *Massachusetts Law Raises the Bar for Data Security,* Jones Day, February 2010, http://www.jonesday.com/massachusetts_law_raises.

[16] Council Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, 2016 O.J. (L119) 1, Art. 4(1) ("GDPR").

[17] Mass. Gen. Laws ch. 93H, § 1 (2018). Similar definitions exist in 47 other states. *See* Alaska Stat. § 45.48.010 *et seq.* (2018); Ariz. Rev. Stat. § 18-545 (2018); Ark. Code §§ 4-110-101 *et seq.* (2018); Cal. Civ. Code §§ 1798.29, 1798.82 (2018); Colo. Rev. Stat. § 6-1-716 (2018); Conn. Gen Stat. §§ 36a-701b, 4e-70 (2018); Del. Code tit. 6, § 12B-101 *et seq.* (2018); Fla. Stat. §§ 501.171, 282.0041, 282.318(2)(i) (2018); Ga. Code §§ 10-1-910, -911, -912 (2018); § 46-5-214 (2018); Haw. Rev. Stat. § 487N-1 *et seq.* (2018); Idaho Stat. §§ 28-51-104 to -107 (2018); 815 ILCS §§ 530/1 to 530/25 (2018); Ind. Code §§ 4-1-11 *et seq.,* 24-4.9 *et seq.* (2018); Iowa Code §§ 715C.1, 715C.2 (2018); Kan. Stat. § 50-7a01 *et seq.* (2018); KRS § 365.732 (2018), KRS §§ 61.931 to 61.934 (2018); La. Rev. Stat. §§ 51:3071 *et seq.* (2018); Me. Rev. Stat. tit. 10 § 1346 *et seq.* (2018); Md. Code Com. Law §§ 14-3501 *et seq.* (2018); Md. State Govt. Code §§ 10-1301 to -1308 (2018); Mo. Rev. Stat. § 407.1500 (2018); Mont. Code §§ 2-6-1501 to -1503, 30-14-1701 *et seq.,* 33-19-321 (2018); Neb. Rev. Stat. §§ 87-801 *et seq.* (2018); Nev. Rev. Stat. §§ 603A.010 *et seq.,* 242.183 (2018); N.H. Rev. Stat. §§ 359-C:19 *et seq.* (2018); N.J. Stat. § 56:8-161 *et seq.* (2018); 2017 H.B. 15, Chap. 36; N.Y. Gen. Bus. Law § 899-AA (2018); N.Y. State Tech. Law 208 (2018); N.C. Gen. Stat. §§ 75-61, 75-65 (2018); N.D. Cent. Code §§ 51-30-01 *et seq.* (2018); Ohio Rev. Code §§ 1347.12, 1349.19, 1349.191, 1349.192 (2018); Okla. Stat. §§ 74-3113.1, 24-161 to -166 (2018); Oregon Rev. Stat. §§ 646A.600 to .628 (2018); 73 Pa. Stat. §§ 2301 *et seq.* (2018); R.I. Gen. Laws §§ 11-49.3-1 *et seq.* (2018); S.C. Code § 39-1-90 (2018); Tenn. Code §§ 47-18-2107, 8-4-119 (2018); Tex. Bus. & Com. Code §§ 521.002, 521.053 (2018); Utah Code §§ 13-44-101 *et seq.* (2018); Vt. Stat. tit. 9 §§ 2430, 2435 (2018); Wash. Rev. Code §§ 19.255.010, 42.56.590 (2018); W.V. Code §§ 46A-2A-101 *et seq.* (2018); Wis. Stat. § 134.98 (2018); Wyo. Stat. §§ 40-12-501 *et seq.* (2018) (collectively, the "State Data Breach Laws").

[18] European Union, *Charter of Fundamental Rights of the European Union,* 26 October 2012, 2012/C 326/02, Art. 8 ("EU Charter of Fundamental Rights").

[19] Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union,* 1-2 Cal. L. Rev. 877, 880 (2014).

[20] GDPR, Rec.61, Art. 13-14.

[21] *Id.,* Rec. 40, Art. 6(1).

[22] *Id.,* Rec. 45, 65, Art. 7(3).

[23] *Id.,* Art. 17(1). One of the mitigating factors is exercising the right to freedom of expression, which is intended to prevent an individual from requiring the deletion of all articles and social media posts that express critical opinions about him or her.

[24] "Personally identifiable information" in the California Online Privacy Protection Act ("CalOPPA") is broader than Massachusetts' "personal information" in that it includes "information concerning a user that the website or online service collects online from the user and maintains in personally identifiable form in combination with identifying information" (*e.g.,* name with physical address, email address, social security number, etc.). Cal. Bus. & Prof. Code § 22577(a) (2018). This definition would likely include information necessary for laser phishing, which is intended to target specific individuals, but not necessarily the other forms of deceptive AI described in this article, as they are designed to deceive larger audiences.

[25] Cal. Bus. & Prof. Code § 22575(a) (2018). CalOPPA applies to so many individuals, *i.e.,* every consumer residing in California, that in the absence of a federal statute, many entities operating online follow its requirements both as a legal requirement and as a best practice.

[26] The 2012 FTC Decision made Facebook another rare exception, as it requires Facebook to obtain an individual's consent before sharing personal data—not just personal information—with third parties if doing so exceeds the individual's privacy settings. *See* 2012 FTC Decision, *supra* note 10.

[27] At least 48 states total. *See* State Data Breach Laws, *supra* note 17.

[28] Those states are Arkansas (Ark. Code §§ 4-110-104(b) (2018)), California (Cal Civ. Code §§ 1798.81, 1798.81.5 (2018)); Connecticut (Conn. Gen. Stat. § 42-471 (2018)); Florida (Fla. Stat. § 501.171(2) (2018)); Indiana (Ind. Code § 24-4.9-3-3.5 (2018)); Kansas (K.S. § 50-6,139b (2018)); Maryland (Md. Code Com Law §§ 14-3501 to -3503 (2018)); Massachusetts (Mass. Gen. Laws Ch. 93H § 2(a) (2018)); Minnesota (Minn. Stat. § 325M.05 (2018)); Nevada (Nev. Rev. Stat. §§ 603A.210, 603A.215(2) (2018)); New Mexico (2017 H.B. 15, Chap. 36); Oregon (Or. Rev. Stat § 646A.622 (2018)); Rhode Island (R.I. Gen. Laws § 11-49.3-2 (2018)); Texas (Tex. Bus. & Com. Code § 521.052 (2018)); Utah (Utah Code §§ 13-44-101, -201, 301 (2018)).

[29] Fla. Stat. § 501.171(2) (2018).

[30] Ind. Code § 24-4.9-3-3.5(c) (2018).

[31] K.S. § 50-6,139b(b)(1) (2018).

[32] 201 Mass. Code Regs. § 17.03(2)(a) (2018).

[33] 201 Mass. Code Regs. § 17.03(2)(f)(2) (2018).

[34] 201 Mass. Code Regs. § 17.04 (2018).

[35] *In the Matter of Facebook, Inc.*, Docket No. C-4365, Complaint, U.S. Federal Trade Commission, *available at* https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookcmpt.pdf.

[36] 2012 FTC Decision, *supra* note 10. As of this writing, it is very possible that Facebook has violated this order and will be subject to FTC fines.

[37] *See* EU Charter of Fundamental Rights, *supra* note 18, at Art. 8; Beata A. Safari, *Intangible Privacy Rights: How Europe's GDPR Will Set a New Global Standard for Personal Privacy Data Protection,* 47 Seton Hall L. Rev. 809, 820-822 (2017).

[38] *See* John Frank Weaver, *Artificial Intelligence and Governing the Life Cycle of Personal Data,* Rich. J. L. & Tech. (forthcoming).