ARTIFICIAL INTELLIGENCE AND GOVERNING THE LIFE CYCLE OF PERSONAL DATA

By: John Frank Weaver*

INTRODUCTION

[1] With other countries making efforts to regulate and govern artificial intelligence ("AI"), [1] it was only a matter of time before American legislators began similar efforts. In December 2017, a bipartisan group of U.S. senators and representatives introduced the Fundamentally Understanding the Usability and Realistic Evolution of Artificial Intelligence Act of 2017 (the "FUTURE of AI Act"). [2] The FUTURE of AI Act would create a committee to review a wide range of topics concerning AI and make recommendations for administrative and legislative strategies

* John Frank Weaver is an attorney with McLane Middleton, P.A. in Boston, Massachusetts and a member of the firm's Privacy and Data Security practice group, where part of his practice focuses on artificial intelligence and autonomous technology. He is the author of *Robots Are People Too*, which explores legal issues implicated by autonomous tech and AI, and a contributing writer to *Slate* magazine, where his articles focus on similar issues. He is a member of the board of editors of *The Journal of Robotics and Artificial Intelligence Law*, where he also writes the "Everything is Not *Terminator*" column, which discusses ongoing legal issues in AI.

[1] *See, e.g.*, Ott Ummelas, *Estonia plans to give robots legal recognition*, INDEP. (Oct. 14, 2017), http://www.independent.co.uk/news/business/news/estonia-robots-artificial-intelligence-ai-legal-recognition-law-disputes-government-plan-a7992071.html, https://perma.cc/E9NK-QZAG (last visited May 3, 2018); *see also The EU drafts laws of robotics*, CEBIT (Jan. 30, 2017), http://www.cebit.de/en/news-trends/news/the-eu-drafts-laws-of-robotics-824, https://perma.cc/TJ5T-7MYZ (last visited May 3, 2018).

[2] *See* Press Release, Office of Senator Maria Cantwell, *Cantwell, Bipartisan Colleagues Introduce Bill to Further Understand and Promote Development of Artificial Intelligence, Drive Economic Opportunity* (Dec. 12, 2017), https://www.cantwell.senate.gov/news/p ress-releases/cantwell-bipartisan-colleagues-introduce-bill-to-further-understand-and-promote-development-of-artificial-intelligence-drive-economic-opportunity.

to effectively promote, govern, and regulate AI.[3] Arguably the committee's most important task is to determine what to do with data used by AI.[4]

[2] Data is the lifeblood of AI.[5] Social media platforms like Facebook demonstrate this by using AI to adjust the content you see based on how you interact with Facebook.[6] The number of AI applications is growing, as is the need for data and the types of data required. Every time someone interacts with an AI-enabled personal assistants like Amazon's Alexa and Echo, that generates data the AI analyzes to improve how the devices interact with users and the applications offered.[7] Google's Project Magenta has produced AI programs that analyze vast amounts of data to create original art.[8] Narrative Science autonomously produces natural language

[3] *See id.*

[4] *See* FUTURE of Artificial Intelligence Act of 2017, S. 2217, 115th Cong., §§ 4(b)(1)(E), 4(b)(2)(I) (2017).

[5] *See* Robert Seamans, *Artificial Intelligence And Big Data: Good For Innovation?*, FORBES (Sept. 7, 2017), https://www.forbes.com/sites/washingtonbytes/2017/09/07/artificial-intelligence-and-big-data-good-for-innovation/#3bd540a94ddb, https://perma.cc/2AXY-5RHV (last visited May 3, 2018) ("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.").

[6] *See* Stacey Higginbotham, *Inside Facebook's Biggest Artificial Intelligence Project Ever*, FORTUNE (Apr. 13, 2016), http://fortune.com/facebook-machine-learning/, https://perma.cc/366H-MDP3 (last visited May 3, 2018) (Facebook has "created an internal platform to harness artificial intelligence so it can deliver exactly the content you want to see.").

[7] *See* George Anders, *Alexa, Understand Me*, MIT TECH. REV. (Aug. 9, 2017), https://www.technologyreview.com/s/608571/alexa-understand-me/, https://perma.cc/4FJ3-DLCW (last visited May 3, 2018) (noting that Echo devices with Alexa use "an artificial intelligence system built 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.").

[8] *See* Cade Metz, *How A.I. Is Creating Building Blocks to Reshape Music and Art*, N.Y. TIMES (Aug. 14, 2017), https://www.nytimes.com/2017/08/14/arts/design/google-how-ai-

articles and reports on sports, business, finance, and a number of other fields that produce large volumes of data that the company's AI programs can analyze.[9]

I. AI AND PERSONAL DATA

[3] There are few if any limits on the types of data AI analyzes. AI can consider impersonal data (*e.g.*, the Celtics won last night) just as easily as personal data (*e.g.*, you were at the Celtics game last night and ordered nachos and two beers).[10] However, AI's reliance on data becomes potentially problematic when the data is personal data, if for no other reason than there is no universal definition of personal data or its variants – personal information, personally identifiable information, etc.[11] In general, Americans limit personal data to data that can be used to identify an individual. In contrast, Europeans look at personal data much more broadly as any information about an individual. Compare these definitions from American laws:

---

creates-new-music-and-new-artists-project-magenta.html, https://perma.cc/KK3F-QPEL (last visited May 3, 2018) ("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.").

[9] *See* Patrick Seitz, *Narrative Science Turning Big Data Into Plain English*, INV. BUS. DAILY TECH. (Aug. 21, 2012), http://news.investors.com/technology/082112-622940-narrative-science-takes-data-analytics-to-next-level.htm?p=full", https://perma.cc/D3LY-VFTM (last visited May 3, 2018) (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.').

[10] *See generally* Erik Brynjolesson and Andrew McAfee, *The Business of Artificial Intelligence: What it can—and cannot—do for your organization*, HARV. BUS. REV. (Mar. 8, 2018, 10:39 AM), https://hbr.org/cover-story/2017/07/the-business-of-artificial-intelligence, https://perma.cc/MC4F-X68K (last visited May 3, 2018) (providing a general overview of how AI "learns" and operates).

[11] *Compare* MASS. ANN. LAWS ch. 93H, § 1 (LexisNexis 2018), *with* CAL. BUS. & PROF. CODE § 22577(a) (West 2018).

> ***Personally identifiable information***: individually identifiable information about an individual consumer collected online by an operator of a website located on the internet from that individual and maintained by the operator in an accessible form, including any of the following: an individual's first and last name, a home or other physical street address, an email address, a telephone number, a Social Security number, any other information that permits a specific individual to be contacted physically or online, and information concerning a user that the website or online service collects online from the user and maintains in personally identifiable form in combination with an identifier described above;[12] and
>
> ***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:
>
> (a) Social Security number;
>
> (b) driver's license number or state-issued identification card number; or
>
> (c) 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.[13]

against the definition used generally in the European Union:

> ***Personal data***: any information relating to an identified or identifiable natural person.[14]

These definitions are consistent with the different approaches to data and privacy in the European Union, where privacy and the protection of

[12] *See* CAL. BUS. & PROF. CODE § 22577(a) (West 2018).

[13] *See* MASS. ANN. LAWS ch. 93H, § 1 (LexisNexis 2018).

[14] *See* Council Directive 2016/679, art. 3, 2016 O.J. (L 119) 59 (EU) [hereinafter GDPR].

personal data is considered a fundamental right,[15] and the United States, where it is considered an interest balanced against others.[16] To a certain extent, American laws expand the limited breadth of the country's definition of personal data through subject-specific laws like the Health Insurance Portability and Accountability Act ("HIPAA"),[17] Children's Online Privacy Protection Act ("COPPA"),[18] and the Fair Credit Reporting Act Fair ("FCRAF").[19] However, the presence of those laws and their niche personal data definitions only highlight the limited scope of personal data under American law.

[4] As AI consumes more data, that limitation will become more pronounced. American data security laws are primarily concerned with identity theft (*i.e.*, third parties illegally obtaining enough information about you to realistically impersonate you in commercial or legal transactions and proceedings.)[20] While that is certainly a concern with AI, it is not the only concern. AI is able to analyze data that is about a specific individual and target advertising, communications, links, etc. designed to appeal to and convince that person.[21]

---

[15] *See* Charter of Fundamental Rights of the European Union, art. 8, 2012 O.J. (C 326) 397 [hereinafter EU Charter of Fundamental Rights].

[16] *See* Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the Unitd States and European Union*, 102 CAL. L. REV. 877, 880 (2014).

[17] *See* 42 U.S.C. § 1320d(4) (2012) (defining "health information"); *see also* 45 C.F.R. § 160.103 (2017) (defining "protected health information").

[18] *See* 15 U.S.C. § 6501(8) (2012) (defining "personal information" concerning parents and children).

[19] *See* 15 U.S.C. § 1681a(i) (2012) (defining "medical information").

[20] *See generally* Sasha Romanosky, Rahul Telang & Alessandro Acquisti, *Do Data Breach Disclosure Laws Reduce Identity Theft?*, 30 J. POL'Y ANALYSIS & MGMT. 256 (2011) (using panel data gathered from the Federal Trade Commission and other sources to examine the empirical effect of data breaches over an eight-year period).

[21] *See* Carole Cadwalladr, *Robert Mercer: The Big Data Billionaire Waging War on Mainstream Media*, THE GUARDIAN (Feb. 26, 2017),

That can be used for good purposes such as education, civic engagement, etc, but it can also be used to mislead, manipulate, and lie to individuals. One technologist has "cautioned that AI could set news consumption back roughly 100 years."[22] Another cautions that AI can be used to control human behavior.[23]

[5] With those dangers in mind, the definition of personal data cannot be limited to names, social security numbers, bank account numbers, etc., as American law currently limits that term. It must be expansive, consistent with the European Union's General Data Protection Regulation ("GDPR"), and include ***any*** information relating to a natural person, including, but not limited to, a name, an identification number, **location data**, online identifier or to one or more factors specific to the physical, physiological, **genetic**, mental, economic, cultural or social identity of that person.[24] For that reason, this article will, generally, rely on the GDPR definition of personal data, although the term and its variants from other statutes and regulations are also used.[25]

---

https://www.theguardian.com/politics/2017/feb/26/robert-mercer-breitbart-war-on-media-steve-bannon-donald-trump-nigel-farage, https://perma.cc/6RVM-Y9Y6 (last visited May 3, 2018).

[22] *See* Charlie Warzel, *He Predicted the 2016 Fake News Crisis. Now He's Worried About An Information Apocalypse*, BUZZFEED (Feb. 11, 2018), https://www.buzzfeed.com/charliewarzel/the-terrifying-future-of-fake-news?utm_term=.rnn7vzYQq#.lx7K63XL2, https://perma.cc/9TTQ-FJPU (last visited May 3, 2018).

[23] *See* CADWALLADR, *supra* note 21.

[24] *See supra* note 14, at Art. 4(1).

[25] At times, this article refers to personal data as used in specific statutes, regulations, etc., rather than the specific variant definition used in the relevant document. This is done for clarity, as using various personal data variations obscures the fact that these are all talking about different ranges of the same subject. Where context is not sufficient for the reader to discern the article's definition of personal data from the source material's term, I have used the document-specific term.

[6] That is not to say that Europe's treatment of personal data is perfect. By treating the protection of personal data as a fundamental right, the GDPR seems to lose sight of the fact that each individual has a property right in the personal data they generate. While they have the fundamental right not to make that data capturable, they also should be given the opportunity to condition the capture and use of their data on payment or other consideration.[26]

[7] Another potential issue in this broad definition of personal data is its breadth. It includes anything written about the data subject, not just data from the data subject.[27] Giving everyone the absolute right over their personal data, as defined here and in the GDPR, potentially permits them to edit unflattering things written about them. That is not the intent here, but AI permits the aggregation of all that content into easily analyzed forms in a way that we have not considered historically.

[8] This is similar to the use of a GPS tracking device in *United States v. Jones*, which considered police use of GPS without a proper warrant.[28] The Federal Bureau of Investigation and District of Columbia police suspected Antoine Jones of trafficking in narcotics and wanted to track his

[26] *See* Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2056-57 (2004). I do not subscribe entirely to the commodification of personal data as Schwartz describes it. Personal data loses some value without the subject individual providing input and guidance. As John Havens notes, "Data should not be treated as a commodity. People should be able to say 'These are the ways I want to share my data,' and companies should encourage users to personalize, or provide their own terms and conditions statements, for their data so it is more useful to everyone involved."; *see* Telephone Interview with John Havens, Executive Director, IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, in Philadelphia, Pa. (Mar. 21, 2017); *see generally* Jeff Desjardins, *How Much is Your Personal Data Worth?*, VISUAL CAPITALIST (Dec. 12, 2016) http://www.visualcapitalist.com/much-personal-data-worth/, https://perma.cc/TCG7-56EM (outlining various valuations of personal data captured and used).

[27] *See* Jeffrey Rosen, *The Right to Be Forgotten*, 64 STAN. L. REV. ONLINE 88, 90 (2012).

[28] *See* UNITED STATES V. JONES, 565 U.S. 400, 402 (2012).

movements.[29] Although the U.S. District Court of the District of Columbia issued a warrant permitting law enforcement to attach a GPS to Jones' car, the warrant stated that the GPS must be installed in the District of Columbia and within 10 days.[30] Law enforcement attached the GPS in Maryland on the 11th day.[31] In her concurring opinion, Justice Sonia Sotomayor considered what we believe to be private, wondering about

> "the existence of a reasonable societal expectation of privacy in the sum of one's public movements. I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."[32]

Although granting everyone the ability to control what others print about them is a flagrant violation of the First Amendment, it is worth considering whether people might reasonably expect that everything written about them in public will be aggregated in a manner that lets AI use that information to convince or manipulate them.

[9] It is also important to note that this article focuses almost exclusively on personal data that is held in a form accessible to AI programs, primarily hard drives and cloud servers, where data lives online or where massive data sets can be stored and analyzed most easily. Many of the existing rules and regulations consider personal data in other forms: paper, CDs, floppy disks, etc.[33] The considerations of rules and regulations are not discussed in great detail here.

---

[29] *See id.* at 400.

[30] *See id.*

[31] *See id.* at 403.

[32] *See id.* at 416.

[33] *See generally What do the HIPAA Privacy and Security Rules require of covered entities when they dispose of protected health information?*, U.S. DEP'T OF HEALTH &

A. Life Cycle of Personal Data

[10] Unlike the GDPR in the European Union, in the United States, there is no single, comprehensive federal law regulating the collection and use of personal data.[34] Instead, there is a hodgepodge of subject specific or state specific laws governing personal data.[35] Functionally, this means that there

HUM. SERVICES (Dec. 14, 2017), https://www.hhs.gov/hipaa/for-professionals/faq/575/what-does-hipaa-require-of-covered-entities-when-they-dispose-information/index.html, https://perma.cc/ZUL7-2FGL (last visited May 3, 2018) [hereinafter What do the HIPAA Privacy and Security Rules require?].

[34] *See* Ieuan Jolly, *Data Protection in the United States: Overview*, THOMSON REUTERS PRACTICAL L. (July 1, 2017), https://content.next.westlaw.com/6-502-0467?transitionType=Default&firstPage=true&bhcp=1&contextData=(sc.Default), https://perma.cc/82WD-QBRP (last visited May 3, 2018).

[35] State data breach statutes are a good example. *See* ALASKA STAT. § 45.48.010 *et seq.* (2018); *see* ARIZ. REV. STAT. § 18-545 (LexisNexis 2018); *see* CAL. CIV. CODE §§ 1798.29, 1798.82 (2018); *see* COLO. REV. STAT. § 6-1-716 (2018); *see* CONN. GEN STAT. §§ 36a-701b, 4e-70 (2017); *see* DEL. CODE ANN. tit. 6, § 12B-101 (2018); *see* FLA. STAT. ANN, §§ 501.171, 282.0041, 282.318 (LexisNexis 2018); *see* GA. CODE §§ 10-1-910, 10-1-911, 10-1-912 (2018), § 46-5-214 (2018); *see* HAW. REV. STAT. ANN. § 487N-1 (LexisNexis 2018); *see* IDAHO CODE §§ 28-51-104 to -107 (2018); *see* 815 ILL. COMP. STAT. ANN. § 530/5, §530/10, §530/12, §530/20, 530/25 (LexisNexis 2018); *see* IND. CODE ANN. § 4-1-11 *et seq*., § 24-4.9 *et seq.* (LexisNexis 2018); *see* IOWA CODE §§ 715C.1, 715C.2 (2018); *see* KAN. STAT. ANN. § 50-7a01 *et seq*. (2018); *see* KY. REV. STAT. ANN. § 365.732 (LexisNexis 2018); see KY. REV. STAT. ANN. §§ 61.931 to 61.934 (LexisNexis 2018); *see* LA. STAT.ANN. §§ 51:3071 (2018); *see* ME. REV. STAT. ANN. tit. 10, § 1346 *et seq.* (2018); *see* MD. CODE ANN., COM. LAW § 14-3501 (2018); *see* MD. CODE ANN., STATE GOV'T. §§ 10-1301 to 10-1308 (LexisNexis 2018); *see* MASS. ANN. LAWS ch. 93H, § 1 *et seq.* (LexisNexis 2018); *see* MICH. COMP. LAWS §§ 445.63, 445.72 (2018); *see* MINN. STAT. §§ 325E.61, 325E.64 (2018); *see* MISS. CODE ANN. § 75-24-29 (2018); *see* MO. REV. STAT. § 407.1500 (2018); *see* MONT. CODE ANN. §§ 2-6-1501 to 2-6-1503, § 30-14-1701 *et seq.*, § 33-19-321 (2018); *see* NEB. REV. STAT. ANN. § 87-801 *et seq*. (LexisNexis 2018); *see* NEV. REV. STAT. § 603A.010 *et seq.*, § 242.183 (LexisNexis 2018); *see* N.H. REV. STAT. ANN. § 359-C:19 *et seq.* (LexisNexis 2018); *see* N.J. STAT. ANN. § 56:8-161 *et seq.* (2018); *see* 2017 H.B. 15, CHAP. 36; *see* N.Y. GEN. BUS. LAW § 899-AA (Consol. 2018); *see* N.Y. STATE TECH. LAW 208 (Consol. 2018); *see* N.C. GEN. STAT §§ 75-61, 75-65 (2018); *see* N.D. CENT. CODE § 51-30-01 *et seq*. (2018); *see* OHIO REV. CODE ANN. §§ 1347.12, 1349.19, 1349.191, 1349.192 (LexisNexis 2018); *see*

is no single philosophy or strategy guiding American decisions about governing personal data. Although it can be useful to create silos of regulations governing specific types of data, like health information,[36] as AI becomes more common and accesses more personal data, it is increasingly important for there to be a national, comprehensive approach to protecting our personal data.

[11] The GDPR's approach is an improvement over America's in that it is a single regulation pursuing an overarching goal: ensuring that everyone is able to protect their personal data in the face of new and rapidly changing technologies.[37] In pursuing this goal, the GDPR focuses on granting new rights to individuals and creating new obligations for entities that process and control personal data.[38] However, in focusing on the data subjects, the GDPR does not recognize that personal data takes on a life of its own once it is created and captured.

[12] AI, relying on its analysis of personal data, can use personal data in surprising ways. For example, a person may understand and consent to his

---

OKLA. STAT. ANN. tit. 74, §§ 74-3113.1, 24-161 to -166 (LexisNexis 2018); *see* OREGON REV. STAT. §§ 646A.600 to 646A.628 (2018); *see* 73 PA. CONS. STAT. § 2301 *et seq.* (2018); *see* 11 R.I. GEN. LAWS § 11-49.3-1 *et seq*. (2018); *see* S.C. CODE ANN. § 39-1-90 (2018); *see* TENN. CODE ANN. §§ 47-18-2107, 8-4-119 (2018); *see* TEX. BUS. & COM. CODE ANN. §§ 521.002, 521.053 (2018); *see* UTAH CODE ANN. § 13-44-101 *et seq.* (LexisNexis 2018); *see* VT. STAT. ANN. tit. 9, §§ 2430, 2435 (2018); *see* WASH. REV. CODE ANN. §§ 19.255.010, 42.56.590 (2018); *see* W.VA. CODE ANN. § 46A-2A-101 *et seq.* (LexisNexis 2018); *see* WIS. STAT. § 134.98 (2018); *see* WYO. STAT. ANN. § 40-12-501 *et seq.* (2018); (collectively, the "State Data Breach Laws").

[36] *See* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936.

[37] *See* EU Charter of Fundamental Rights, *supra* note 15, at Art. 8; *see also* Beata A. Safari, Comment, *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* SAFARI, *supra* note 37, at 820-822.

or her data being used for direct marketing may not fully appreciate all the ways that AI can use personal data to market. Communications can be directed at the data that appear to come from friends.[39] Videos and sound clips featuring augmented images and voice recordings can be created.[40] News stories, real and fake, can be directed in order to convince that person of a particular idea or agenda.[41] For example, research scientists at Cambridge University's Psychometric Centre developed a program that can analyze "likes" on Facebook "to produce uncannily accurate results."[42] After 150 likes, the program can predict your personality better than your spouse; after 300 likes, it can understand you better than you understand yourself.[43]

[13] In a way, governing personal data by focusing only on the data subject is like governing children by only focusing on the parents: you miss all of the things the children do when the parents are not around. A law that governs the driving of minors by regulating the parents' behavior does not effectively regulate all of the children's behavior when they are driving without the parents in the car. Similarly, governing personal data by focusing the rights of the data subject does not effectively regulate all of the things that can be done with personal data once it is created and captured by a third part.

[14] Instead, personal data governance should focus on the life cycle of personal data and address each stage individually.[44] Personal data, as

[39] *See* Warzel, *supra* note 22.

[40] *See id.*

[41] *See* Cadwalladr, *supra* note 21.

[42] *See id.*

[43] *See id.*

[44] *See* Richard Kissel, et al., *Guidelines for Media Sanitization*, NAT'L INST. OF STANDARDS AND TECH., U.S.DEPT. OF COM. 17-18, 50 (Dec. 2014) http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf, https://perma.cc/3P6C-QLK8 (last visited May 3, 2018).

collected and used today, has a three-phase life cycle, from the perspective of the people whose data is collected:[45]

> 1. Capture: Data capture is a broad term that refers to any process of collecting information that can be manipulated by a computer program,[46] including personal information that someone affirmatively enters into a website, app, or computer is data collection, as well as the aggregated observable online behavior tracked by sites like Facebook, Amazon, and Google.[47]
> 2. Usage and Maintenance: Once personal data is captured, the third party entity that captured the data retains the it for some period of time. This phase occupies the majority of any personal data's life cycle. Everything that a third party does with personal data (except destroy it) is included in this phase: store, sell, analyze, etc.[48]

---

[45] *See* Malcolm Chisholm, *7 phases of data life cycle*, BLOOMBERG (July 14, 2015) https://www.bloomberg.com/professional/blog/7-phases-of-a-data-life-cycle/, https://perma.cc/3RD5-4D7R (last visited May 3, 2018). (Chisholm divides the life cycle of data, or "Life History," which he suggests may be more appropriate, into 7 phases: Capture, Maintenance, Synthesis, Usage, Publication, Archival, and Purging. However, Chisholm is writing from the perspective of data management professionals. From the perspective of consumers whose data is collected, this number can be reduced to 3, as explained above.)

[46] *See Data Capture,* CAMBRIDGE ADV. LEARNER'S DICTIONARY & THESAURUS, https://dictionary.cambridge.org/us/dictionary/english/data-capture, https://perma.cc/VXC4-43S4 (last visited Mar. 9, 2018); *see also Data Capture,* COLLINS ENGLISH DICTIONARY, https://www.collinsdictionary.com/us/dictionary/english/data-capture, https://perma.cc/NN9A-WZTF (last visited Mar. 9, 2018); *see also* OXFORD LIVING DICTIONARIES, https://en.oxforddictionaries.com/definition/data_capture, https://perma.cc/E69R-FERP (last visited Mar. 9, 2018).

[47] *See* Lina M. Khan, *Amazon's Antitrust Paradox*, 126 YALE L.J. 710, 773-774 (2017); *see also* James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137, 1187-1190 (2009).

[48] *See* CHISHOLM, *supra* note 45.

3. Destruction: This phase is simply the destruction, termination, or purging of data.[49] It does not include when data is disclosed due to a breach; that is included in Usage and Maintenance.

By classifying each phase of personal data's life cycle, we can identify the distinct data governance needs of each phase.[50] By creating phase-specific rules and requirements, we can more effectively protect the privacy interests and property interests each person has in their personal data.

[15] The purpose of this article is to explore the potential regulatory system that could comprehensively govern each phase in way that effectively addresses personal data used by AI so that there is a logical consistency to the regulatory system as a whole. Each of the following three sections reviews one of the three phases listed above. In doing so, each section first considers what actually occurs in each phase, discussing what data capturers, data users, and data destroyers do with the data. Next, each section considers, though not exhaustively, relevant European and American laws that currently apply during the relevant phase. Finally, using the existing laws already discussed, the last part of each section lays out how personal data, data subjects, data capturers, data users, and data destroyers should be governed from a personal data life cycle perspective.

II. DATA CAPTURE

A. How is Data Captured*?*

[16] At the risk of leading this section with an overly obvious statement, it is safe to say that the legal standards surrounding the capture of personal data in America are entirely different from those in the European Union.[51]

[49] *See* George L. Paul & Robert F. Copple, *Dealing with Data*, 14 BUS. L. TODAY 35 (2005) (noting that as part of the life cycle of data all data not required to be retained by law or business purposes should be destroyed).

[50] *See* CHISHOLM, *supra* note 45.

[51] *Compare* GDPR, *supra* note 14, at Art. 6(1)(a) (requiring the consent of a data subject before the data can be used), *with* CAL. BUS. & PROF. CODE § 22575(a) (West 2018)

However, the methods of data capture are essentially the same in both jurisdictions:

1. Data entry: Data about a data subject that is created purposefully by the data subject, including data from application forms and surveys, and collected by a third party.[52]

2. Data reception: Data that third parties capture means other direct entry by the data subject, including (a) through devices or programs that observe the behavior of human beings using those devices or programs, including clicking habits on social media, shopping or browsing patterns online, etc.,[53] and (b) analysis of content and data prepared by parties other than the data subject, including newspapers, public records, social media entries, etc.[54]

Surveys in America suggest that Americans pay more attention to and are more concerned about personal data that is captured via data entry.[55] We are much more likely to believe that personal information like social security numbers and medical history, which are frequently manually entered into a form, is "very sensitive" compared to internet search history or purchasing habits.[56] This is, of course, consistent with the American concern for identify theft.

(requiring that the operator of a commercial website that collects personally identifiable information post its privacy policy on the website, but does not require consent).

[52] *See* Peter A. Tatian, *Designing a Data Entry and Verification System*, INT'L FOOD POL'Y RES. INST. 26 (1992).

[53] *See* CHISHOLM, *supra* note 45.

[54] *See* ROSEN, *supra* note 27, at 90.

[55] *See* Lee Rainie, *The State of Privacy in Post-Snowden America*, PEW RESEARCH CENTER (Sept. 21, 2016), http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/, https://perma.cc/4KBX-MHFP (last visited May 3, 2018).

[56] *See id.* (According to the survey results reported, 90% of American adults believe their social security number is very sensitive and 55% believe the state of their health is very sensitive, however only 24% believe their internet searches are very sensitive and only 8% believe their purchasing habits are very sensitive).

[17] Although I would not dispute that social security numbers are sensitive information that should be kept private and confidential, as discussed above, AI is able to use personal information about our patterns and habits captured through data reception that potentially makes that data just as sensitive.57 Certainly it makes that data valuable.

[18] We should keep that in mind when considering the standards that should govern the capture of personal data because the rules that control data capture will also affect how the capturers maintain and use personal data. And before considering the preferred standards, we should review quickly some of the existing data capture standards.

B. Relevant Current Legal Standards Governing Data Capture

1. GDPR in the EU

[19] In Europe, the GDPR requires that at the time of capture, data capturers provide data subjects with the relevant information regarding how that individual's personal data will be used.[58] Before capturing data, the capturing party must obtain the consent of the data subject, or there must be some other lawful basis.[59] Consent is defined as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement" to the collection and use of his or her personal data.[60] It is

[57] *See* Andrew W. Bagley & Justin Brown, *Limited Consumer Privacy Protections Against the Layers of Big Data*, 31 SANTA CLARA COMPUT. & HIGH TECH. L.J. 483, 488-489 (2015).

[58] *See* GDPR, *supra* note 14, at ch. 3, sec. 2, art. 13-14.

[59] *See id.* at ch. 2, art. 6(1). In addition to consent, Article 6(1) provides other lawful bases, including: contractual necessity, compliance with legal obligations, vital interests, public interest, and legitimate interests. EU Member States are permitted to introduce additional lawful bases, per Article 6(2).

[60] *See id.* at art. 4(11).

helpful to unpack two terms from that definition: "freely given" and "informed."

[20] The GDPR looks at three factors when considering whether consent is freely given: (1) whether the data individual has genuine, free choice in deciding whether to give consent; (2) whether the individual is unable to refuse consent; and (3) whether the performance of a contract is conditioned on the individual's consent is not necessary for the performance of that contract.[61] If the entity capturing the data exercises any compulsion or undue pressure on an individual, the consent will not be valid.[62]

[21] To be properly informed, an individual must have sufficient information to properly understand what he or she us consenting to.[63] The nature of what will be done with the personal data should be explained in an intelligible and easily accessible form, using clear and plain language that does not contain unfair terms.[64]

CalOPPA requires the operators of websites or online services that collect personal data (as defined in the statute) about individuals living in California to "conspicuously post" their privacy policy.[65] The privacy policy must do the following:

---

[61] *See id.* at ch. 2, art. 7(4); *see also* Stacy A. Tovino, *The HIPAA Privacy Rule and the EU GDPR: Illustrative Comparisons*, 47 SETON HALL L. REV. 973, 986-87 (2017).

[62] *See* Detlev Gabel & Tim Hickman, *Chapter 8: Consent – Unlocking the EU General Data Protection Regulation*, WHITE & CASE (July 22, 2016) https://www.whitecase.com/publications/article/chapter-8-consent-unlocking-eu-general-data-protection-regulation, https://perma.cc/AK4L-YFQ8.

[63] *See id.*

[64] *See* GDPR, *supra* note 14, at ch. 2, art. 7(2).

[65] *See* CAL. BUS. & PROF. CODE §22575(a) (2018). As CalOPPA is a state law, it only applies to businesses that impact California residents. However, given the size of California and the relatively easy criteria to satisfy, many companies comply with CalOPPA in all states, not just in California.

> 1. Identify the categories of personal data that the operator collects through the website or online service about individual consumers who use or visit its commercial website or online service and the categories of third-party persons or entities with whom the operator may share that personal data.
> 2. If the operator maintains a process for an individual consumer who uses or visits its commercial website or online service to review and request changes to any of his or her personal data that is collected through the website or online service, provide a description of that process.
> 3. Describe the process by which the operator notifies consumers who use or visit its commercial website or online service of material changes to the operator's privacy policy for that website or online service.
> 4. Identify its effective date.
> a. Disclose how the operator responds to web browser "do not track" signals or other mechanisms that provide consumers the ability to exercise choice regarding the collection of personal data about an individual consumer's online activities over time and across third-party websites or online services, if the operator engages in that collection.
> b. Disclose whether other parties may collect personal data about an individual consumer's online activities over time and across different websites when a consumer uses the operator's website or service.
> c. An operator may satisfy the requirement of (5) above by providing a clear and conspicuous hyperlink in the operator's privacy policy to an online location containing a description, including the effects, of any program or protocol the operator follows that offers the consumer that choice.[66]

Note that the requirements listed above merely define what information has to be revealed about the personal data collected. CalOPPA does not give consumers to right to deny the operators of websites and online services the right to use their personal data altogether. Further, although operators have

[66] *See* CAL. BUS. & PROF. CODE §22575(b) (2018).

to disclose the information identified in the statute, but the statute does not actually place any limits on what operators can do with personal data.

[22] Subject-matter specific regulations and legislation, at least at the data capture stage, have adopted both the GDPR method of obtaining consent before and the CalOPPA method of requiring only notice before collection. For example, like CalOPPA, HIPAA also requires notice of privacy practices for "protected health information."[67] The notice must include:

> 1. A description of the types of uses and disclosures that the covered entity is permitted to make for treatment, payment, and health care operations;
> 2. A description of each of the other purposes for which the covered entity is permitted or required to use or disclose protected health information without the individual's written authorization;
> 3. If a use or disclosure listed in the notice is prohibited or materially limited by other applicable law, the description must reflect the more stringent law;
> 4. For each purpose listed in the notice, the description must include sufficient detail to place the individual on notice as to the uses and disclosures that are permitted or required by law; and
> 5. A description of the types of uses and disclosures that require authorization, a statement that other uses and disclosures not described in the notice will be made only with the individual's written authorization, and a statement that the individual may revoke an authorization.[68]

HIPAA also has regulations governing when an individual's authorization is required or when an individual must be offered the opportunity to agree or object.[69] However, unlike the GDPR, such consent or opportunities to

[67] *See* 45 C.F.R. § 164.520(a) (2018).

[68] *See* 45 C.F.R. § 164.520(b)(1)(ii) (2018).

[69] *See* 45 C.F.R. § 164.508 (2018); *see also* 45 C.F.R. § 164.512 (2018).

object are not required before the personal information is captured, but later in the use and maintenance phase.[70]

[23] In contrast, COPPA specifically requires both data capturers to provide notice and obtain "verifiable parental consent" before any collection of personal data from children, including consent to any material change in the collection practices.[71] The operator must make reasonable efforts to ensure that a parent of a child receives direct notice of the operator's practices regarding the capture of children's personal data.[72] The notice must state that the operator of any website or online service will not capture a child's personal data without the parent's consent, the personal data the operator intends to collect from the child should the parent provide consent, and that if the parent does not provide consent within a reasonable period of time from the date of the notice, the operator will delete the parent's online contact information from its records.[73] The "operator must also give the parent the option to consent to the collection and use of the child's personal information without consenting to the disclosure of his or her personal information to third parties."[74]

C. How Should Data Capture Be Governed in the Life Cycle of Personal Date?

[24] One of the important aspects of considering and governing personal data as a life cycle is that data capture does not exist in a vacuum. Personal

[70] *See id.* To some extent, this reflects the fact the personal data collected – "protected health information" – is necessary for the medical professionals to perform their jobs in hospitals and health clinics, as opposed to the personal data collected by commercial websites, which, at best, is necessary to sell widgets better.

[71] *See* 16 C.F.R. § 312.4(a) (2018). *See also* 16 C.F.R. § 312.5(a) (2018).

[72] *See* 16 C.F.R. § 312.4(b) (2018).

[73] *See* 16 C.F.R. § 312.4(c) (2018).

[74] *See* 16 C.F.R. § 312.5(a)(2) (2018).

data is rarely captured with no purpose; website operators and other capturing entities use that data. This point will become even more important as AI makes personal data more valuable and useful. Although few regulations consider the ultimate destruction of data, that is the endpoint that a life cycle theory aims for. That is the perspective we need to take when considering how data capture should be governed in the life cycle of personal data.

[25] With that in mind, the notice provisions that existing regulations in the United States and Europe are a good place to start. All data capturers should provide direct notice to inform individuals:

1. Who is capturing their personal data;
2. What data will be captured;
3. How the capturer will use the personal data;
4. What techniques the capturer uses to ensure that the personal data is secure;
5. What other entities may purchase the personal data from the capturer;
6. How individuals can easily consent, refuse consent, or condition consent to such data capturing; and
7. How individuals can revoke or change the conditions placed on their consent after initially giving consent.[75]

Ideally, any notice that complies with these requirements will communicate to individuals three fundamental principles that will govern for the lives of their personal data: (1) data capturers must practice full transparency in how they capture and use data; (2) individuals are able to exercise full control over their personal data, revising it when they deem necessary and dictating whether it can be captured and used and what conditions apply to that capture and use; and (3) any personal data captured will be secure.[76]

[75] *See* 16 C.F.R. § 312.4(b) (2018); *see also* GDPR, *supra* note 14, at 61; *see also* CAL. BUS. & PROF. CODE § 22575 (2018).

[76] *See* GINA STEVENS, CONG. RESEARCH SERV., R41756, PRIVACY PROTECTIONS FOR PERSONAL INFORMATION ONLINE 7-5700 (2011).

[26] Once individuals are properly notified, data capturers must obtain individuals' specific consent to capture and use their personal data. The form should resemble the pre-capture consent required by the GDPR as well as the authorization required by HIPAA for the disclosure or use of personal data that is not specifically listed in the regulations.[77] That is, the consent must be unambiguously given, in writing, and via a form that is easy to read and understand.[78] Individuals must have a meaningful opportunity to deny consent and to make that consent conditional subject to the capturer complying with a data subject's terms, *i.e.*, there can be no form of compulsion to give consent.[79]

[27] The idea of conditional consent as used in this article is not immediately present in either American or European regulation of personal data. If personal data exists as a property right, owners of certain personal data – *i.e.*, the personal data they generate themselves through internet browsing, phone app usage, etc. – should be able to license its use subject to specific terms and conditions.[80] This has a couple of benefits. First, it permits online commerce to continue its reliance on personal data. This is a point that American policymakers emphasize – and worry about – when considering a "privacy bill of rights" and improved protections for personal data.[81] Second, it provides tangible benefits to individuals. Data capturers can offer or bid to track my personal data.[82] Do you want to capture data

[77] *See* 45 C.F.R. § 164.501 (2018); 45 C.F.R. § 164.506 (2018); 45 C.F.R. § 164.508 (2018); 45 C.F.R. § 164.510 (2018); GDPR, *supra* note 14, at 23.
[78] *See* 45 C.F.R. § 164.508 (2018); GDPR, *supra* note 14, at Rec. 32.

[79] *See* GDPR, *supra* note 14, at Rec. 32

[80] *See* Interview with John Havens, *supra* note 26.

[81] *See* STEVENS, *supra* note 76, at 2-3. *See also* U.S. DEP'T OF COMMERCE INTERNET TASK FORCE, COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK (2010), https://www.ntia.doc.gov/files/ntia/publications/iptf_privacy_greenpaper_12162010.pdf, https://perma.cc/P96F-VVTH (pointing out that privacy protections are crucial to maintaining consumer trust).

[82] *See* Interview with John Havens, *supra* note 26.

regarding my breakfast purchasing and consumption habits? I want discounts to the stores where I buy breakfast, or I want a free cup of coffee once a week.[83]

[28] The conditions an individual places on the use of personal data are subject to change during the life cycle of that data, and the initial notice should clearly state how an individual can do that. However, any changes made to those conditions after data capture occur in the data maintenance and usage phase.

III. DATA USAGE AND MAINTENANCE

A. What activities are included in data usage and maintenance?

[29] As discussed briefly above, data usage and maintenance encompasses most of personal data's life cycle. This phase includes: assigning or creating values for the data inputs;[84] applying data as information to improve the functions of the business operations of the data capturer;[85] targeted advertising;[86] conveying the data to third parties;[87]

[83] I hate coffee strongly enough that I feel compelled to note that in a footnote, but I admit it is irrelevant to the hypothetical above.

[84] *See* CHISHOLM, *supra* note 45.

[85] *See* Chris Petty, *Treating Information as an Asset*, SMARTER WITH GARTNER (Nov. 30, 2017), https://www.gartner.com/smarterwithgartner/treating-information-as-an-asset/, https://perma.cc/764R-J2DJ (last visited May 3, 2018); *see also* Jathan Sadowski, *Companies are Making Money From Our Personal Data – But at What Cost?*, THE GUARDIAN (Aug. 31, 2016, 9:00 AM), https://www.theguardian.com/technology/2016/aug/31/personal-data-corporate-use-google-amazon, https://perma.cc/7DMZ-QVPS (last visited May 3, 2018).

[86] *See* Catherine Clifford, *How Google, Apple, Facebook and Others Use Your Personal Data*, ENTREPRENEUR (June 28, 2013), https://www.entrepreneur.com/article/227248, https://perma.cc/M8W2-AW7A (last visited May 3, 2018).

[87] *See id.* (referencing Baynote infographic chart to illustrate how larger tech companies distribute and use data for third party connections and exchanges).

using personal data to improve website autocomplete functions;[88] using personal data to better identify media and articles users will enjoy;[89] targeting specific prices at specific consumers;[90] storing the data;[91] disclosing the data;[92] predicting and controlling human behavior;[93] and manipulating, organizing, or disseminating the data in any way.[94] It is an extensive list, and one that will only get longer as AI is used to analyze, manipulate, and monetize personal data even further.

[30] The monetization of personal data is arguably the primary reason the use and maintenance phase continues to expand. There is inherent value in the data itself, as data capturers are able to use it to improve their

---

[88] *See* Your Data: We want you to understand what data we collect and use, GOOGLE PRIVACY, https://privacy.google.com/your-data.html?modal_active=your-data-proof-overlay&article_id=c1-p-search-autocomplete-2, https://perma.cc/D9CF-GUAR (last visited May 3, 2018) (click on the "Your Data" subheading, scroll down to "How data improves Google searches", click middle box top row for "How Google autocompletes your searches").

[89] *See* Your Data: We want you to understand what data we collect and use, GOOGLE PRIVACY, https://privacy.google.com/your-data.html?modal_active=your-data-proof-overlay&article_id=c1-p-now-personalized-6, https://perma.cc/4AZ2-QERS (last visited May 3, 2018) (click on "How Google search helps you find your own information").

[90] *See* Katie Pedersen, Greg Sadler, & Virginia Smart, *How Companies Use Personal Data to Charge Different People Different Prices for the Same Product*, CBCNEWS (Nov. 24, 2017, 5:00 AM), http://www.cbc.ca/news/business/marketplace-online-prices-profiles-1.4414240, https://perma.cc/LPD3-XHYJ (last visited May 3, 2018).

[91] *See* CHISHOLM, *supra* note 45 (discussing phase of data archiving and storage).

[92] *See* State Data Breach Laws, *supra* note 35 (collectively citing all State laws on data disclosure).

[93] *See* CADWALLADR, *supra* note 21, (referencing Prof. Jonathan Rust's concerns with use of personal data to manipulate or change behaviors unbeknowest to user).

[94] *See* GDPR, *supra* note 14, at Art. 4(2).

marketing, sales, and user experiences.[95] Increasingly, though, data brokers – entities whose sole business is collecting and reselling personal data – represent a growing business with revenues in the hundreds of millions of dollars and have begun to garner attention from the Federal Trade Commission.[96] To the extent that they capture or acquire personal data, they also need to be governed by the requirements discussed below for the use and maintenance phase. As with data capture requirements, the existing legal requirements for the storage, disclosure, and use of personal data inform the standards that should govern the use and maintenance phase in the life cycle of personal data.

B. Relevant Legal Requirements Currently Governing the Use and Maintenance of Personal Data

1. GDPR in the EU

[31] The GDPR emphasizes data security, although it does not provide many specific details. During the use and maintenance phase, personal data must be maintained and used in such a way that ensures appropriate security of the data, including protection against accidental loss, unauthorized use, unlawful use, destruction, and damage.[97] Depending on the nature of the relevant party's use of the personal data, the necessary security measures

[95] *See* Danielle J. Garber, *COPPA: Protecting Children's Personal Information on the Internet*, 10 J.L. & POL'Y 129, 140-45 (2001); Sadowski, *supra* note 91.

[96] *See* FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 23 (May 2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf, https://perma.cc/P9QZ-WG6U (last visited May 3, 2018). *See also* Press Release, Federal Trade Commission, FTC to Study Data Broker Industry's Collection and Use of Consumer Data (Dec. 18, 2012), https://www.ftc.gov/news-events/press-releases/2012/12/ftc-study-data-broker-industrys-collection-use-consumer-data, https://perma.cc/D24A-ST2R (last visited May 3, 2018).

[97] *See* GDPR, *supra* note 14, at paras. 29, 71, 156; Art. 5(1)(f), 24(1), 25(1)-(2), 28, 32, 39.

could include encryption of the personal data, on-going reviews of security measures; redundancy and back-up facilities, and regular security testing.[98] Industry associations are encouraged to establish codes of conduct to govern the use and maintenance of personal data in their fields in such a way that complies with the GDPR. If the relevant data protection authority ("DPA") approves a code of conduct, adherence to that code can be evidence of complying with the GDPR.[99]

[32] Conveyances of personal data to entities in countries outside the EU are prohibited unless the European Commission determines that the relevant country ensures an adequate level of data protection.[100] The factors that affect that determination include: the rule of law and legal protections for human rights and fundamental freedoms; access to transferred data by public authorities; the existence and effective functioning of DPAs; and international commitments and other obligations in relation to the protection of personal data.[101]

[33] In the event of a data breach, the party that possesses the personal data must report the breach to the relevant DPA without undue delay and in no case more than 72 hours after becoming aware of it. The notice must include:

> 1. A description of the nature of the personal data breach, including the categories and approximate number of individuals affected and the categories and approximate number of personal data records concerned;
> 2. The name and contact information of the data protection officer ("DPO") at the party who is the point of contact;
> 3. The likely consequences of the personal data breach; and

[98] *See id.* at para. 83; Art. 32.

[99] *See id.* at paras. 77, 81, 98-99; Art. 24(3), 28(5), 35(8), 40(1)-(2), 46(2)(e), 57(1), 83(2)(j).

[100] *See id.* at paras. 101-116; Art. 44, 45(1).

[101] *See id.* at paras. 103-07; Art. 44, 45.

> 4. Any measures taken or proposed by the party to address the breach, including, where appropriate, measures to mitigate the possible adverse effects of the breach.[102]

The party does not have to inform the DPA if the data breach is unlikely to result in any harm to the affected individuals.[103]

[34] Additionally, the party must notify the individuals affected by the data breach. That notice should include (2)-(4) above.[104] However, the party is not required to send the notice if :

> 1. The party has implemented appropriate technical and organizational protection measures, and that those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to accept it, such as encryption;
> 2. The party has taken subsequent measures which ensure that the high risk to the rights and freedoms of the affected individuals is no longer likely to materialize; or
> 3. The notification requires disproportionate effort, in which case the party must issue a public notice of the breach.[105]

[35] Individuals are entitled to other notices from data users upon request. Individuals have the right to obtain confirmation as to the purposes their data are being used for, the entities to whom personal data is disclosed, and the existence of automated-decision making, *i.e.*, AI-based decisions, that rely on their data.[106] Individuals also have a "right to an explanation,"

[102] *See* GDPR, *supra* note 14, at Art. 33(3).

[103] *See id.* at Art. 33(1).

[104] *See id.* at Art. 33(2)-(4).

[105] *See id.* at Art. 34(3).

[106] *See id.* at Art. 15(1).

meaning that upon request data users are required to inform them whether "automated decision-making, including profiling" is involved in using their personal data and provide them with "meaningful information about the logic involved" with that use.[107] The GDPR also grants individuals the right not to be subject to a decision "evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or significantly affects him or her" without any human intervention.[108] Data subjects should be able to express their points of view regarding the use of their personal data.[109] Data using entities must permit data subjects to correct personal data they have identified as incorrect.[110]

[36] Note that, for the most part, the requirements governing the use and maintenance of personal data do not address the types of uses, only what security measures are necessary. The GDPR appears to rely on industry associations and organizations to include those requirements in their codes of conduct, to whatever extent they choose.[111] It is an open topic whether some uses of personal data should be prohibited or limited. As some

[107] *See* GDPR, *supra* note 14, at Art. 13(2)(f). *See also* Bryce Goodman & Seth Flaxman, *European Union Regulations On Algorithmic Decision-Making and a "Right to Explanation"*, Presented at the 2016 ICML Workshop on Human Interpretability in Machine Learning (Aug. 31, 2016) at 6, https://arxiv.org/abs/1606.08813, https://perma.cc/MHG5-T5TH (last visited May 3, 2018); John Frank Weaver, *Artificial Intelligence Owes You an Explanation*, SLATE, (May 8, 2017, 7:15 AM), http://www.slate.com/articles/technology/future_tense/2017/05/why_artificial_intelligences_should_have_to_explain_their_actions.html, https://perma.cc/VR49-C8JW (last visited May 3, 2018).

[108] *See* GDPR, *supra* note 14, at para. 71.

[109] *See id.*

[110] *See id.* at Art. 16.

[111] *See id.* at Art. 40(2) (noting that industry associations and other bodies representing business interests may prepare or amend codes of conduct to address "the legitimate interests pursued… in specific contexts," which could be relied on to prohibit certain uses of personal data in certain contexts).

researchers have noted, at least one of the uses of personal data, "predict[ing] and potentially control[ling] human behavior," is "incredibly dangerous… incredibly scary."[112] You could argue that use qualifies as a decision that is "based solely on automated processing" and "significantly affects him or her," which is prohibited by the GDPR.[113] However, you can just as easily argue that this type of use is consistent with current marketing practices and is not prohibited by the GDPR. In light of the notice and consent required by the GDPR, it appears that in trying to protect personal data, the GDPR relies almost exclusively on data subjects objecting to data capture and use when so desired, rather than focusing on what the personal data does after capture.

IV. THE UNITED STATES

[37] There is no federal law comparable to the GDPR governing the use and maintenance of all personal data in the United States. Where state and federal governments have promulgated rules and regulations governing the use and maintenance of personal data, they have taken an approach similar to Europe's.[114] Security is the priority. Specific uses are not necessarily prohibited or conditioned. With regard to a few specific types of personal data, third parties must obtain the data subject's consent before using it for many purposes.[115]

[38] Currently, there are 15 states that have specific statutes and/or regulations requiring data security measures.[116] As noted in the Introduction,

[112] *See* CADWALLADR, *supra* note 21.

[113] *See* GDPR, *supra* note 14, at Art. 22(1).

[114] *See e.g.*, ARK. CODE ANN. §§ 4-110-104(b) (2017) (exemplifying a state statute that, like the CDPR, stresses security of personal data).

[115] *See* GABEL & HICKMAN, *supra* note 62.

[116] Those states are Arkansas (ARK. CODE ANN. § 4-110-104(b) (2017)); California (CAL. CIV. CODE §§ 1798.81, 1798.81.5 (2018)); Connecticut (CONN. GEN. STAT. § 42-471 (2017)); Florida (FLA. STAT. ANN. § 501.171(2) (2017)); Indiana (IND. CODE ANN. § 24-

these statutes apply by their terms to only a limited type of personal data, typically some combination of name, social security number, driver's license number, credit card number, bank account number, etc.[117] The security standards established in these state laws vary greatly.

Most states have only specified that covered parties "take reasonable measures to protect and secure" the relevant data,[118] "implement and maintain reasonable procedures… to protect and safeguard from unlawful use or disclosure" the relevant data,[119] "implement and maintain reasonable procedures and practices appropriate to the nature of the information, and exercise reasonable care to protect the personal information,"[120] etc. Massachusetts, however, has provided much more detailed requirements governing how to protect the relevant personal data. These requirements include designating specific employees to maintain security programs;[121] requiring that service providers implement security measures,[122] 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.[123]

4.9-3-3.5 (2018)); Kansas (KAN. STAT. ANN. § 50-6,139b (2018)); Maryland (MD. CODE ANN., COM. LAW §§ 14-3501 to 14-3503 (2018)); Massachusetts (MASS. ANN. LAWS ch. 93H § 2(a) (2018)); Minnesota (MINN. STAT. § 325M.05 (2017)); Nevada (NEV. REV. STAT. ANN. §§ 603A.210, 603A.215(2) (2017)); New Mexico (H.B. 15, 53rd Leg., 1st Sess. (N.M. 2017)); Oregon (OR. REV. STAT. § 646A.622 (2017)); Rhode Island (11 R.I. GEN. LAWS § 11-49.3-2 (2017)); Texas (TEX. BUS. & COM. CODE ANN. § 521.052 (2017)); Utah (UTAH CODE ANN. §§ 13-44-101, -201, 301 (2017)).

[117] *See, e.g.*, CONN. GEN. STAT. § 42-471(c) (2017); FLA. STAT. ANN. § 501.171(1)(g) (2017); IND. CODE § 24-4.9-2-10 (2018); MASS. ANN. LAWS ch. 17, §17.02 (2018).

[118] *See* FLA. STAT. § 501.171(2) (2014).

[119] *See* IND. CODE § 24-4.9-3-3.5(c) (2017).

[120] *See* KAN. STAT. ANN. § 50-6,139b(b)(1) (2016).

[121] *See* 201 MASS. CODE REGS. §17.03(2)(a) (LexisNexis 2010).

[122] *See* 201 MASS. CODE REGS. §17.03(2)(f)(2) (LexisNexis 2010).

[123] *See* 201 MASS. CODE REGS. §17.04 (1)-(3) (LexisNexis 2010).

[39] Federal statutes governing the use and maintenance of subject-specific personal data have also prioritized security. For example, HIPAA's "Security Rule" specifies a series of administrative, physical, and technical security procedures for covered entities to use to assure the confidentiality integrity and availability of the relevant personal data.[124]

[40] Administrative safeguards include designating a security official who is responsible for developing and implementing security policies and procedures[125] and performing periodic assessments of how well the covered entity's security policies and procedures meet HIPAA requirements.[126] Physical safeguards include limiting access to a covered entity's facilities while ensuring that authorized access is allowed[127] and implementing policies and procedures to specify proper use of and access to workstations and electronic media.[128] Technical safeguards include implementing technical policies and procedures that allow only authorized persons to access electronic personal data[129] and using hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use personal data.[130]

---

[124] *See Summary of the HIPAA Security Rule*, U.S.DEP'T OF HEALTH AND HUMAN SERV., https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html, https://perma.cc/X3KN-ZBST (last visited Mar. 1, 2018).

[125] *See* 45 C.F.R. § 164.308(a)(2) (2018).

[126] *See* 45 C.F.R. § 164.308(a)(8) (2018).

[127] *See* 45 C.F.R. § 164.310(a) (2018).

[128] *See* 45 C.F.R. §§ 164.310(b)-(c) (2018).

[129] *See* 45 C.F.R.. § 164.312(a) (2018).

[130] *See* 45 C.F.R. § 164.312(b) (2018).

[41] In addition to addressing security strategies and mechanisms, American laws also address notices to individuals whose personal data is in the use and maintenance phase.[131] In the event of a security breach, almost all states require entities that use and maintain personal data (as defined in each state's statute) provide notice to individuals whose data may be compromised.[132]

[42] California requires that covered entities notify individuals whose personal data has been sold to one or more third parties for direct marketing purposes, with such notice to include the names of the relevant third parties and the disclosed personal data, but only upon the request of the individual.[133] The statute uses the term "personal information" and the list of data that is included within that definition is broader than other states' statutes governing personal information and includes data that is valuable in the context of AI, such as products purchased.[134]

[43] As mentioned in above in Section II(b)(2), HIPAA requires consent in certain situations before the covered entity can disclose personal data during the use and maintenance phase. Generally speaking, there are three rules:[135]

1. Covered entities may use and disclose the relevant personal data with no prior permission from the data subject for that individual's treatment, payment, and health care operations, activities, and certain public benefit activities.[136]

[131] *See generally* State Statutes, *supra* note 35.

[132] *See id*.

[133] *See* CAL. CIV. CODE § 1798.83 (2018).

[134] *See id.* at § 1798.83(e)(6).

[135] *See* TOVINO, *supra* note 61, at 980-983 (a thorough discussion of these rules).

[136] *See* 45 C.F.R. §§ 164.501, 164.506(c)(1), 164.512(a)-(l) (2018).

Covered entities may conduct five sets of personal data uses and disclosures once the data subject has been notified and has either agreed or not objected to the use and disclosure.[137]

> 2. Those five sets of personal data uses and disclosures include: (a) certain uses and disclosures of directory information, such as name, location, general condition, and religious affiliation;[138] (b) certain uses and disclosures that would allow other persons to be involved in a patient's care or payment for care;[139] (c) certain uses and disclosures that would help notify, or assist in the notification of, family members, personal representatives, and other persons responsible for the care of the individual's location, general condition, or death;[140] (d) certain uses and disclosures for disaster relief purposes; [141] and (e) certain disclosures to family members and other persons who were involved in the individual's care or payment for healthcare prior to the individual's death.[142]
>
> 3. Covered entities must obtain prior authorization, either written or oral, from the relevant individual before using or disclosing that person's personal data in any situation that does not satisfy the first two rules.[143]

These rules are interesting because they assign a preferred status to some personal data disclosures by covered entities (patient treatment, family notification, etc.) versus others, which makes sense in the health care context.

---

[137] *See generally* 45 C.F.R. §164.510 (2018).

[138] *See* 45 C.F.R. §§ 164.510(a)(i)(A)-(D) (2018).

[139] *See* 45 C.F.R. § 164.510(b)(1)(i) (2018).

[140] *See* 45 C.F.R. § 164.510(b)(1)(ii) (2018).

[141] *See* 45 C.F.R. § 164.510(b)(4) (2018).

[142] *See* 45 C.F.R. § 164.510(b)(5) (2018).

[143] *See* 45 C.F.R. § 164.510 (2018).

[44] American laws and regulations governing the use and maintenance of personal data are similar to the GDPR in that they do not prohibit covered entities from using captured personal data for particular purposes.[144] Individuals are given some protections in the form of required data security, are entitled to certain notices in the event of a breach or (in California) if they ask about disclosure of personal data to third parties, and (in some scenarios) must grant their consent before their personal data can be disclosed.[145]

A. How Should the Use and Maintenance of Personal Data be Governed in the Life Cycle of Personal Data?

[45] Governing the use and maintenance phase of personal data's life cycle requires first looking at what was done in the previous phase of the life cycle, data capture.[146] Before a party captures any personal data, it often must send direct notice and obtain consent.[147] The direct notice must be sent to the relevant individuals, identifying the personal data to be captured, how the data will be used, the other entities that may purchase the data, how the data will be secured, and how the individuals can consent, revoke consent, and condition consent.[148] Regulations governing the use and maintenance phase in the life cycle must build from those requirements in anticipation of the final phase, destruction.

---

[144] *See generally* 45 C.F.R. § 164.306 (2018).

[145] *See* CAL. CIV. CODE §§ 1798.83(a)(1)-(2) (2018); *see also* 107 CODE OF MASS. REGS. § 2.04(1) (2018).

[146] *See* CHISHOLM, *supra* note 45.

[147] *See generally Data Protection – What the Regulations Say*, AUDIENCE DATA SHARING, https://www.audiencedatasharing.org/legal-information, https://perma.cc/6WG8-L3HF (last visited Mar. 9, 2018).

[148] *See* 16 C.F.R. § 312.4(b), *supra* note 81 (discussing the notice provisions that currently exist in the United States and Europe).

[46] Consistent with the GDPR and American laws, security must be emphasized during this phase. Regulations and legislation based on personal data's life cycle should require specific administrative, physical, and technical protocols[149] that are flexible enough to reflect differences in industries and changing standards.[150] In particular, it is important that data users are required to conduct regular reviews and audits of their security measures and hire specific personnel that are responsible and trained for data security.[151]

[47] Data users must send notices to individuals when their data has been compromised in a security breach.[152] Those notices should include:

1. A description of the nature of the personal data breach, including the categories and approximate number of individuals affected and the categories and approximate number of personal data records concerned;
2. The name and contact information of the person within the entity that will oversee the response and mitigation efforts;
3. The likely consequences of the personal data breach; and
4. Any measures taken or proposed by the party to address the breach, including, measures to mitigate the possible adverse effects of the breach.[153]

The notices should be direct notices, not merely public announcements.

[48] Because individuals have the right to both (a) revoke their consent to the capture of their personal data and to specific uses for their personal data, and (b) change the conditions that data users must comply with in order to use their personal data, it is necessary for entities that have been

[149] *See generally* 45 C.F.R. §§ 164.308, 164.310, 164.312.

[150] *See generally* 201 MASS. CODE REGS. § 17.01 (2018); *see also* GDPR, *supra* note 14, at paras. 29, 71, 83, 156, arts. 5(1)(f), 24(1), 25(1)-(2), 28, 32, 39.

[151] *See* 201 MASS. CODE REGS. §17.03(2)(a); *see also* GDPR, *supra* note 14, at art. 32.

[152] *See generally* State Statutes, *supra* note 35.

[153] *See* GDPR, *supra* note 14, at paras. 73, 85-88, art. 33.

authorized to collect and use individuals' personal date to send annual notices to those individuals identifying:

> 1. Who continues to capture their personal data;
> 2. When the relevant consent was first given;
> 3. All data that has been captured;
> 4. How the data subject can edit and reprioritize the data the entity is using;
> 5. What data the entity is authorized to capture going forward;
> 6. How the capturer uses the personal data;
> 7. What techniques the capturer uses to ensure that the personal data is secure;
> 8. What other entities have purchased the personal data from the capturer in the last year and are expected to purchase the data in the coming year;
> 9. Any existing conditions placed on the capture and use of the personal data; and
> 10. How individuals can revoke their consent or change the conditions placed on their consent.[154]

In addition to the annual notice, individuals should have the right to request a statement from relevant entities that will contain the information listed above. Similarly, if data subjects change their consent and/or conditions and terms of use, they should receive an updated notice from the relevant entity. When a data user sells or transfers an individual's personal data, it should be the responsibility of that entity to ensure that the acquiring third party sends similar notices to the data subject.[155]

[49] The right to establish terms and conditions for the use of personal data should also include the right to change how data capturers prioritize and use personal data as well as the right to correct personal data that is inaccurate.[156] How many people have clicked on a link that looked amusing

[154] *See* 16 C.F.R. § 312.4(b) (2018); *see generally* GDPR, *supra* note 11, at para. 61, art. 13-14, 16-17; *see also* CAL. CIV. CODE § 1798.83 (2018).

[155] *See generally* GDPR, *supra* note 14, at para. 81, art. 28(1)-(3), 29.

[156] *See id.* at art. 16.

or that only vaguely interested them, only for that link to be the source of advertisements in their newsfeed or internet searches for the next three months? That clicked link is personal data that data users are relying on to sell advertising in a way that benefits neither the advertisers (who are marketing to an uninterested audience member) nor the individual (who did not have a commercial interest in the link to begin with). Allowing individuals to customize their personal data will make that data more useful to parties that use the data and to individuals who ideally will seek to profit from their property rights in their data. AI and AI programmers will have no problem incorporating individuals' preferences into the algorithms analyzing personal data. AI programs that do that will produce better results.[157]

[50] Whether or not certain uses of personal data should be prohibited or more strictly regulated than others is an open question. The use of personal data by AI to make decisions that have legal consequences for the relevant individuals is one area where the GDPR suggests an outright ban, as individual have the right not to be subject to "a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her", subject to certain limitations.[158] Researchers that have developed methods of using AI to analyze personal data to design advertisements and strategies to "convince" individuals have called for this use to be regulated.[159] "The danger of not having regulation around the sort of data you can get from Facebook and elsewhere is clear…It's how you brainwash someone," notes Jonathan Rust, the director of the Psychometrics Centre at the University of Cambridge.[160]

---

[157] *See* Interview with John Havens, *supra* note 26.

[158] *See* GDPR, *supra* note 14, at art. 22.

[159] *See* CADWALLADR, *supra* note 21.

[160] *See id.*

[51] Technologists like Aviv Ovadya, the chief technologist for the University of Michigan's Center for Social Media Responsibility, worry about artificial intelligence-assisted misinformation campaigns will lead to "toxic misinformation." He is concerned that "We are so screwed it's beyond what most of us can imagine."[161] Bad actors could use AI analysis of personal data to make it "appear as if anything happened, regardless of whether or not it did."[162] One example is laser phishing, which relies on AI to scan your personal data to craft fake but believable messages from people you know.[163] With tools like these, it is legitimately possible to make individuals believe just about anything, convincing them to act against their own interests in new and dangerous ways.

[52] With regard to uses like manipulative convincing or toxic misinformation, the ultimate question is not one concerning the life cycle of the personal data that these AI programs rely on, but a public policy question. Do we want third parties to use our personal data – our likes, dislikes, shopping habits, internet histories, online comments, etc. – to push particular agendas, be they commercial or political, that we might not be aware of? Maybe outright prohibition is appropriate, or maybe legislatures should consider other methods of discouraging those uses, such as imposing a fiduciary duty on every entity that has personal data and seeking criminal prosecution when that duty is violated.[164]

---

[161] *See* WARZEL, *supra* note 22.

[162] *See id.*

[163] *See id.* (prohibiting laser phishing or introducing tighter consent laws for personal data would not fully address tactics like laser phishing, as they can frequently operate using publically available personal information).

[164] *See* John Frank Weaver, *Should AI Makers Be Legally Responsible for Emotionally Manipulating Customers?*, SLATE (Jan. 20, 2014, 11:31 AM), http://www.slate.com/blogs/future_tense/2014/01/20/should_ai_makers_be_legally_responsible_for_emotionally_manipulating_customers.html, https://perma.cc/K27Z-NS25 (last visited May 3, 2018).

[53] As the use and maintenance phase of personal data's life cycle occupies most of the life cycle, it is critical to consider how this phase bridges the first, data capture, and the last, data destruction. The notices, consents, terms, and conditions that individuals attached to their personal data at data capture and updated during the use and maintenance phase must be consistent so that individuals are able to track their personal data, manage it appropriately, and effectively trade their property rights in that data.[165] Establishing this life cycle mentality is particularly important as AI becomes more dominant during the use and maintenance phase. Having a consistent system for personal data will help individuals make sense of the ways in which their personal data is used and make informed choices about their personal data.

V. DESTRUCTION OF PERSONAL DATA

A. What is data destruction?

[54] Destruction of personal data in this article refers to both (i) "sanitizing" data as used by the federal government, meaning rendering access to relevant personal data infeasible,[166] and (ii) the "erasure" or disposal of personal data, meaning the secure removal of that data in a readable or decipherable form from the records of the relevant entity in such a way so as not to permit unauthorized disclosure of the data.[167]

---

[165] *See* Sagara Gunathunga, *How to Design GDPR Compliant Consent*, MEDIUM (Sep. 16, 2017), https://medium.com/@sagarag/how-to-design-gdpr-compliant-consent-b5d6cf28d0c5, https://perma.cc/DR25-UXYZ (last visited May 3, 2018).

[166] *See* Guidelines for Media Sanitization, *supra* note 44, at 44.

[167] *See* GDPR, *supra* note 14, art. 17; *see also* What do the HIPAA Privacy and Security Rules require?, *supra* note 33; *see also* Data Disposal Laws, NATIONAL CONFERENCE OF STATE LEGISLATURES (Dec. 1, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx, https://perma.cc/XRG5-HKGK (last visited Mar. 7, 2018).

[55] Although some legislation and regulations provide comprehensive requirements for the destruction of personal data in all forms – paper records, bags, bottles, alternative media, etc.[168] – the narrow scope of this article is personal data in electronic records, and so destruction is limited to personal data in that type of storage.

B. What Are the Current Legal Requirements Governing the Destruction of Personal Data?

1. Erasure of Personal Data Under the GDPR in the EU

[56] The GDPR contains the much celebrated "right to be forgotten,"[169] which grants individuals the right to obtain from a data controlling entity the erasure of their personal data without undue delay where one of the following grounds applies:

> 1. The personal data are no longer necessary for their purposes;
> 2. The requesting individuals withdraw their consent to the capture and use of their personal data and there are no other legal grounds for the continued use of that data;
> 3. The individuals object for relevant reasons established in the GDPR;
> 4. The personal data have been unlawfully captured or used;

[168] *See* Kissel, *supra* note 44, at 25; *see also* What do the HIPAA Privacy and Security Rules require?, *supra* note 33; *see also* 45 C.F.R. § 164.310(d)(2)(i) (2018).

[169] *See* Eric Posner, *We All Have the Right to Be Forgotten*, SLATE (May 14, 2014, 4:37 PM), http://www.slate.com/articles/news_and_politics/view_from_chicago/2014/05/the_european_right_to_be_forgotten_is_just_what_the_internet_needs.html, https://perma.cc/W8NX-8494 (last visited May 3, 2018); *see also* Jeffrey Toobin, *The Solace of Oblivion*, THE NEW YORKER (Sept. 29, 2014), https://www.newyorker.com/magazine/2014/09/29/solace-oblivion, https://perma.cc/3EP8-QJFM (last visited May 3, 2018); *e.g.*, Farhad Manjoo, *'Right to Be Forgotten' Online Could Spread*, THE NEW YORK TIMES (Aug. 5, 2015), https://www.nytimes.com/2015/08/06/technology/personaltech/right-to-be-forgotten-online-is-poised-to-spread.html, https://perma.cc/8MKE-PUQ4 (last visited May 3, 2018).

> 5. The personal data have to be erased for compliance with one or more legal obligations; or
> 6. The personal data have been collected in relation to the offer of information society services referred to in the GDPR.[170]

Data controlling entities do not have to comply with an erasure request to the extent that continued use and maintenance of the personal data is necessary for:

> 1. Exercising the right of freedom of expression and information;
> 2. Compliance with a legal obligation;
> 3. The performance of a task carried on in the public interest or in the exercise of official authority vested in the relevant entity;
> 4. Reasons of public interest in the area of public health, as established in the GDPR;
> 5. Archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes if erasure is likely to render impossible or seriously impact the achievement of the relevant objective; or
> 6. The establishment of legal claims.[171]

[57] Although the GDPR does not establish specific mandatory time frames for the erasure of personal data, data controlling entities are required to store such data for no longer than is necessary for the purposes for which the personal data are captured and used.[172] It is possible that industry-specific codes of conduct could establish more specific deadlines for the mandatory erasure of personal data.[173]

[58] Using the appropriate technical or organizational measures, data erasure must be performed in a secure fashion that ensures appropriate

---

[170] *See* GDPR, *supra* note 14, art. 17(1).

[171] *See id.* at art. 17(3).

[172] *See id.* at para. 39; *see also id.*, art. 5(1)(e).

[173] *See id.* at art. 24(3), 28(5), 35(8), 40(1)-(2), 46(2)(e), 57(1)(m), 57(1)(p), 57(1)(o), 83(2)(j); *see also id.*, rec. 77, 81, 98, 99; *see also* Tovino, *supra* note 61, at 991.

security of those data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage.[174]

2. Disposal and Destruction of Personal Data in the United States

[59] At least 32 states have laws governing the destruction of personal data that provide general guidelines for that destruction.[175] Typical language includes:

---

[174] *See* GDPR, *supra* note 14, at paras. 29, 71, 156; *see also id.* at art. 5(1)(f), 24(1), 25(1)-(2), 28(1), 32(1)-(2), 39(1)(b); *see also* Detlev Gabel & Tim Hickman, *Chapter 6: Data Protection Principles – Unlocking the EU General Data Protection Regulation*, WHITE & CASE (July 22, 2016), https://www.whitecase.com/publications/article/chapter-6-data-protection-principles-unlocking-eu-general-data-protection, https://perma.cc/BVG4-HMFP (last visited May 3, 2018).

[175] *See* ALASKA STAT. §§ 45.48.500-590 (2018) (Alaska); *see also* ARIZ. REV. STAT. § 44-7601 (2018) (Arizona); *see also* ARK. CODE §§ 4-110-103-104 (2018) (Arkansas); *see also* CAL. CIV. CODE §§ 1798.81, 1798.81.5, 1798.84 (2018) (California); *see also* COLO. REV. STAT. § 6-1-713 (2018) (Colorado); *see also* CONN. GEN. STAT. § 42-471 (2018) (Connecticut); *see also* DEL. CODE tit. 6 §§ 5001C-5004C (2018) (Delaware); *see also* DEL. CODE tit. 19 § 736 (2018) (Delaware); *see also* FLA. STAT. § 501.171(8) (2018) (Florida); *see also* GA. CODE § 10-15-2 (2018) (Georgia); *see also* HAW. REV. STAT. §§ 487R-1-3 (2018) (Hawaii); *see also* 20 ILCS 450/20 (2018) (Illinois); *see also 815* ILCS 530/30 (2018) (Illiois); *see also* 815 ILCS 530/40 (2018) (Illinois); *see also* IND. CODE § 24-4-14-8 (2018) (Indiana); *see also* IND. CODE § 24-4.9-3-3.5(c) (2018) (Indiana); *see also* KAN. STAT. §§ 50-7a01-03 (2018) (Kansas); *see also* KAN. STAT. §50-6, 139b(2) (2018) (Kansas); *see also* KY. REV. STAT. § 365.725 (2018) (Kentucky); *see also* MASS. GEN. LAWS ch. 93I, § 2 (2018) (Massachusetts); *see also* MD. STATE GOVT. CODE §§ 10-1301-1303 (2018) (Maryland); *see also* MICH. COMP. LAWS § 445.72a (2018) (Michigan); *see also* MONT. CODE ANN. § 30-14-1703 (2018) (Montana); *see also* NEV. REV. STAT. § 603A.200 (2018) (Nevada); *see also* N.J. STAT. §§ 56:8-161-162 (2018) (New Jersey); *see also* 2017 H.B. 15, Chap. 36 (New Mexico; signed by governor but not as of yet codified); *see also* N.Y. GEN. BUS. LAW § 399-H (2018) (New York); *see also* N.C. GEN. STAT. § 75-64 (2018) (North Carolina); *see also* ORE. REV. STAT. § 646A.622 (2018) (Oregon); *see also* R.I. GEN. LAWS § 6-52-2 (2018) (Rhode Island); *see also* S.C. CODE § 30-2-310 (2018); *see also* S.C. CODE § 37-20-190 (2018) (South Carolina); *see also* TENN. CODE § 39-14-150(g) (2018) (Tennessee); *see also* TEX. BUS. & COM. CODE § 72.004 (2018) (Texas); *see also* TEX. BUS. & COM. CODE § 521.052 (2018) (Texas); *see also* UTAH CODE § 13-44-201 (2018) (Utah); *see also* 9 VT. STAT. § 2445 (2018)

- "electronic media… containing personal information shall be destroyed or erased so that personal information cannot practically be read or reconstructed;"[176]
- "When disposing of records that contain personal information, a business and a governmental agency shall take all reasonable measures necessary to protect against unauthorized access to or use of the records;"[177]
- "When a business disposes of a business record that contains personal identifying information of a customer of the business, the business shall modify, by… erasing, or other means, the personal identifying information so as to make the information unreadable or undecipherable;"[178] and
- "No person, business, firm, partnership, association, or corporation, not including the state or its political subdivisions, shall dispose of a record containing personal identifying information unless the person, business, firm, partnership, association, or corporation, or other person under contract with the business, firm, partnership, association, or corporation does any of the following… destroys the personal identifying information contained in the record; or modifies the record to make the personal identifying information unreadable; or takes actions consistent with commonly accepted industry practices that it reasonably believes will ensure that no unauthorized person will have access to the personal identifying information contained in the record."[179]

(Vermont); *see also* WASH. REV. CODE § 19.215.020 (2018) (Washington); *see also* WISC. STAT. § 134.97 (2018) (Wisconsin).

[176] *See* MASS. ANN. LAWS ch. 93I, §2(b) (LexisNexis 2018).

[177] *See* ALASKA STAT. § 45.48.500(a) (2017).

[178] *See* TEX. BUS. & COM. CODE Ann. § 72.004(b) (West 2017).

[179] *See* N.Y. GEN. BUS. LAW § 399(h)(2) (LexisNexis 2018).

Some states, like Massachusetts, also affirmatively note that entities may retain third party vendors to dispose of personal data, but require that those vendors comply with the statutory requirements.[180]

[60] HIPAA provides disposal requirements with somewhat more detailed descriptions, at least with regard to the processes used. Under HIPAA, data using entities are required to "[i]mplement policies and procedures to address the final disposition of electronic protected health information."[181] Other publications by the United States Department of Health and Human Services ("HHS") provide further guidance, although much of it assumes the destruction of the electronic storage device itself, which is likely impossible or impractical where the personal data is saved to cloud servers or hard drives for access by AI programs.[182] Where HHS addresses destruction methods that are likely to be AI-friendly, it refers to clearing techniques, *i.e.*, using software or hardware products to overwrite media with non-sensitive data.[183]

[180] *See* MASS. ANN. LAWS ch. 93, § 2(b) (LexisNexis 2018).

[181] *See* 45 C.F.R § 164.310(d)(2)(i) (2018).

[182] *See* Department of Health & Human Services, *Security Standards: Physical Safeguards*, 2 HIPPA SECURITY SERIES, Paper 3, 1 (last updated Mar. 2007), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/physsafeguards.pdf, https://perma.cc/6YPG-MVHP (last visited May 3, 2018); *see also* Guidelines for Media Sanitization, *supra* note 44, at ii, iv (the National Institute of Standards and Technology in the United States Commerce Department ("NIST") also published the Guidelines for Media Sanitization, a detailed guide to destroying personal data that provides instructions tailored for many electronic storage devices. NIST is responsible for developing information security standards and guidelines for most federal information systems, but the Guidelines for Media Sanitization specifically states that nongovernmental organizations may adopt its guidelines on a voluntary basis).

[183] *See* What do the HIPAA Privacy and Security Rules require?, *supra* note 33 (referring nongovernmental entities to the Guidelines for Media Sanitization, *supra* note 44 (for "practical information on how to handle sanitization" of personal data "through the information life cycle").

[61] As with the GDPR, American data destruction laws and regulations do not establish mandatory timelines for the destruction of personal data. State data destruction laws do not address the topic.[184] HIPAA does not address mandatory data destruction, but it also does not attempt to alter the existing federal and state medical record retention rules, which require that records containing personal data *not be destroyed* for certain periods of time.[185] For example, the federal Medicare Conditions of Participation require that Medicare-participating hospitals maintain medical records for five years.[186] Many state medical practice acts require physicians licensed in those states to maintain their own medical records for set periods, such as seven years.[187] Additionally, unlike the GDPR, the right to be forgotten does not exist in American law, at least not for adults.[188]

C. How Should the Destruction of Personal Data be Governed in the Life Cycle of Personal Data?

[62] Based on the requirements during the first two life cycle phases and the principles contained in European and American laws governing personal data destruction, there should be two primary obligations in this phase: mandatory destruction and destruction upon request. The first concept is largely ignored in both laws, though the GDPR both hints at it and leaves open the possibility that an industry's code of conduct could create a required timeline for the destruction of personal data.[189] The

[184] *See* State Data Destruction Laws, *supra* note 179.

[185] *See* TOVINO, *supra* note 61, at 991.

[186] *See* 42 C.F.R § 482.24(b)(1) (2018).

[187] *See*, *e.g.*, 22 TEX. ADMIN. CODE § 165.1(b)(1) (2018).

[188] *See* John W. Dowdell, *An American Right to Be Forgotten*, 52 TULSA L. REV. 311, 333, 338 (2017) (stating California became the first state to adopt the right to be forgotten for minors in 2015) (citing CAL. BUS. & PROF. CODE § § 22580-22581 (2015)).

[189] *See* GDPR, *supra* note 14, paras. 39, 77, 81, 98-99, arts. 5(1)(e), 24(3), 28(5), 35(8), 40(1)-(2), 46(2)(e), 57(1)(m), (o)-(p), 83(2)(j).

second concept is firmly established in the GDPR as the right to be forgotten, but is largely absent from American law.[190]

[63] Mandatory termination in this article refers to a regulatory or statutory deadline, such as five or seven years after consent, when data users are required to destroy the personal data they have collected from an individual, subject to a few conditions.[191] The first is that the destruction deadline is waivable by the data subject after appropriate notice, which will reset the mandatory destruction timeline. Prior to the data capture phase, a data capturer should obtain the consent of each individual whose data it wants to capture and send direct notice to those individuals, which explains what personal data it will capture, what that data will be used for, etc. During the use and maintenance phase, annual notices should be sent to each individual, updating that information, noting the entities that have purchased each data subject's personal data, reminding data subjects how they can update their personal information and conditions, etc. During the destruction phase, a data user should send direct notice to individuals when the mandatory destruction date for their personal data is approaching. The notice should state:

1. Who is proposing to destroy the data;
2. The date(s) when consent was given and the date of the proposed destruction;
3. All the data that has been captured, used, and maintained;
4. The data that will be excluded from mandatory destruction for public policy reasons, as discussed below;
5. The deadline for the data subject to object to the destruction of data in order to reset the mandatory timeline;
6. Clear instructions explaining how to respond to the notice;
7. How the captured data has been used;
8. What data the data user will continue to capture and how it will be used in the event the timeline is reset;
9. What techniques the data capturer is using to secure the data;

---

[190] *See id.* at art. 22; *see also* BUS. & PROF. CODE § § 22580-22581.

[191] *See* 45 C.F.R § 482.24(b)(1); *see also* 22 TEX. ADMIN. CODE § 165.1(b)(1).

10. What other entities have purchased the data since consent was first given;
11. What benefits or services, if any, the individuals will lose due to the destruction of the data;
12. Any existing conditions placed on the capture and use of the personal data; and
13. In the event the destruction is waived, how individuals can change (a) the conditions placed on the capture and use of their data going forward, and (b) their personal data if it is inaccurate or improperly analyzed.[192]

Upon an individual's response, the data user will take the requested actions, *e.g.*, reset the timeline, change the conditions of use, update the personal information, etc. If there is no response, the personal data are destroyed on the date indicated in the notice.

[64] The other conditions that would prevent the mandatory destruction of personal data are public policy reasons. For example, public policy might dictate that medical records should be retained beyond the mandatory destruction date, as suggested by the federal and state laws governing medical records retention. Other reasons include:

1. Exercising the right of freedom of speech;[193]
2. Compliance with a legal obligation;
3. The performance of a task carried on in the public interest or in the exercise of official authority vested in the relevant entity;
4. Archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes if erasure is likely to render impossible or seriously impact the achievement of the relevant objective; or
5. The establishment of legal claims.[194]

[192] *See* GDPR, *supra* note 14, paras. 39, 73, 85-88, art. 5(1)(e), 33.

[193] *See* DOWDELL, *supra* note 188, at 334-335; *see generally* ROSEN, *supra* note 27 at 88-92 (describing the implications of the right to be forgotten on the right of freedom of speech).

[194] *See* GDPR, *supra* note 14, art. 17(3).

Personal data that qualify under one or more of these restrictions would not be destroyed at the destruction deadline, and the destroying entity should identify that data in the destruction notice.

[65] With regard to destruction of personal data upon request, data users should be required to comply with those requests, unless doing so would be contrary to one or more of the public policy reasons listed above.

VI. CONCLUSION

[66] AI makes personal data more valuable and will continue to do so as AI applications become increasingly sophisticated analysts of personal data. AI programs can find patterns or preferences that the data subject did not realize were there and then use those discoveries to target advertising, news, and compelling opinion pieces to that person, either because the analysis indicates that media will interest the person or because the analysis indicates the media will convince that person of a separate idea or objective. The process and end result of that AI analysis gives personal data a life of its own, separate from the data subject. Because it is a separate subject, to properly govern personal data, laws and regulations should be written to address personal data's life cycle with an eye toward the data subject's interests, not just to address the data subject's interest.

[67] That means acknowledging that the personal data has a life of its own. The data subject must consciously decide to create this new entity and must be kept up to date about it. Before data is even captured during the capture phase, data subjects must give consent and receive notice about the data capture. As each data subject has a property right in the personal data he or she generates, data capturers can only use that data subject to any terms and conditions the data subject places on the capture and use of the personal data. Similarly, data users must send annual notice to data subjects about their personal data, to keep them up to date on its use and development, reminding the data subjects that they can further condition or deny consent based on the current status of their personal data. Finally, a waivable mandatory destruction date limits the separate life of personal data, but permits the data subject to waive the mandatory destruction if that person

so chooses. Similarly, data subjects have the right to begin the destruction phase in the life cycle sooner upon request.

[68] AI creates a host of new problems and opportunities. It is incumbent on legislators, regulator, and policy makers to realize that personal data is the fuel that powers AI. To properly regulate AI, we have to properly regulate personal data over its entire life cycle. Hopefully, the FUTURE of AI Act will form a committee that advocates for that.