DePaul University
University Libraries

DePaul Law Review

Volume 69
Issue 2 *Winter 2019*

Article 16

Research Participants' Rights To Data Protection In The Era Of Open Science

Tara Sklar

Mabel Crescioni

RESEARCH PARTICIPANTS' RIGHTS TO DATA PROTECTION IN THE ERA OF OPEN SCIENCE

*Tara Sklar and Mabel Crescioni**

CONTENTS

Clinical trials are increasingly using sensors embedded in wearable devices due to their capabilities to generate real-world data. These devices are able to continuously monitor, record, and store physiological metrics in response to a given therapy, which is contributing to a redesign of clinical trials around the world. Traditional clinical trials are immensely expensive and limited in testing options, as they typically entail research participants coming to designated sites for measuring responses to an investigational treatment. This process creates a costly, time-intensive pathway from discovery to market and may not produce results that future patients wish to know, particularly around improvements in activities of daily living and overall quality of life. While wearable devices present potential benefits, including a reduction in expense

* Professor of Health Law, University of Arizona James E. Rogers College of Law and Mabel Crescioni, Professor of Practice, University of Arizona Colleges of Law and Public Health. The authors wish to thank the editors at DePaul Law Review for providing excellent feedback on this contribution to the Clifford Symposium on Tort Law and Social Policy. We are grateful for the thoughtful comments from Dov Fox, David Hyman, Stephan Landsman, Catherine Sharkey, Adam Zimmerman, and all the participants at the 2019 Clifford Symposium. This work also greatly benefitted from feedback provided by Marvin Slepian and participants at the 2019 Biomedical Engineering Roundtable on Law and Medical Devices at the National Academies of Sciences, Engineering, and Medicine and the 2019 Food and Drug Law Institute's Annual Conference.

and time for researchers as well as burden on research participants, there are data protection concerns around the magnitude of data that is generated by these devices. Participants may not be aware of the detailed, granular-level of data being collected from them, and researchers may be in violation of collecting 'unintended data'—that is, when the data collected does not pertain to the original research purpose. These seemingly opposing views, from individual data protection to sharing big data across populations as a common resource, would benefit from drawing on lessons learned in open science. Both data protection regulation and open science emphasize the need for transparency, access to data, security, and accountability. This Article focuses on the evolving role for research participants as they become increasingly engaged in clinical trials through participant-driven data collection, and how data protection regulation could further empower participants in the research process.

Introduction

Lawmakers in the European Union and California have enhanced protection of personal data with the passage of the General Data Protection Regulation (GDPR)[1] and the California Consumer Privacy Act (CCPA).[2] These laws coincide with an evolution in thinking about open access to data and the role of regulators in sharing data that could advance science and improve public health. An emerging issue between privacy concerns and the public interest is individual participant data and how clinical trials are increasingly collecting data directly from participants through mobile technologies, wearables, and other digital health devices. This shift to participant-driven data collection and acceptance of the real-word data they generate in clinical trials is encouraged by the 21st Century Cures Act,[3] with the expectation that they will accelerate the drug discovery and development process. This promise and ability to provide millions of data points on a wide-range of physiological functions is transforming research design and creating an unprecedented amount of continuous health monitoring data. The Food and Drug Administration (FDA) flagged the increased risk to privacy with this new technology but has yet to offer clear guidance.[4] Similarly, it is uncertain as to how the newly granted participants' rights over personal data under the GDPR and CCPA

1. Commission Regulation 2016/679 of April 27, 2016, General Data Protection Regulation O.J. (L 119) 1.

2. Cal. Civ. Code § 1798 (West 2020).

3. 21st Century Cures Act, Pub. L. No. 114-255, 130 Stat. 1033 (Dec. 13, 2016).

4. The FDA has not issued any formal guidance on the 21st Century Cures Act but has provided general information on the Act. *See* FDA.gov, *21st Century Cures Act*, https://www.fda

will be interpreted in a research setting. This developing technological and legal landscape holds serious implications for health research around the globe.

Clinical trials provide great benefits to society, for drug development, and to research participants. They produce extensive information about the safety and effectiveness of drugs and other medical products to advance scientific discovery,[5] and they create access to investigational therapies not yet on the market. As clinical trials increasingly adopt wearable devices, which have the ability to generate a magnitude of personal health data previously unimaginable, the protection of participants' rights over their data becomes a growing issue of concern. The benefits of responsibly sharing this wealth of data through data repositories, and ultimately in an open science information commons, further present an opportunity of unrealized potential as well as raise privacy concerns as de-identifying data becomes less viable.[6]

The overarching idea of the open science movement is that scientific knowledge should be publicly available.[7] In fact, many institutions that support this idea have adopted the word "commons" to describe this big data initiative of using health, medical, and genomic data across populations as a shared resource.[8] In addition, some scholars note the ethical and pragmatic importance of a participant-centric information commons, where efforts are made to empower participants in the research process by engaging them in a continuous decision-making role over use of their data.[9] Specifically, in a study led by Amy L. McGuire, the authors identified four critical attributes to support a participant-centric medical information commons (MIC) that align well with recent data protection regulations namely the GDPR and CCPA.[10] They are: transparency, access to data, security, and accountability.[11]

There are notable variations between the GDPR and CCPA, but both call for greater transparency and accountability from data con-

---

.gov/regulatory-information/selected-amendments-fdc-act/21st-century-cures-act (last updated Mar. 29, 2018).

5. *See, e.g.*, Michelle Mello et al., *Clinical Trial Participants' Views on the Risks and Benefits of Data Sharing*, 378 N.E. J. MED. 2202, 2203 (2018).

6. *Id.* at 2203.

7. *See* Mark Phillips & Bartha M. Knoppers, *Whose Commons? Data Protection as a Legal Limit of Open Science*, 47 J. L., MED. & ETHICS 106, 107 (2019).

8. *Id.*

9. *See, e.g.*, Amy L. McGuire et al., *Importance of Participant-Centricity and Trust for a Sustainable Medical Information Commons*, 47 J. L., MED. & ETHICS, 12, 13 (2019).

10. *Id.* at 17.

11. *Id.*

trollers (natural or legal persons, public authorities, agencies, or other bodies that process data related to a person) to improve the security of data and enhance individual rights over personal data.[12] The GDPR and CCPA curtail some of these individual rights if the data controller claims a research purpose for processing the data.[13] They also vary on which entities are covered, the definition of research, consent processes, safeguards to protect data, and sanctions. These variations create predictability problems for researchers conducting multi-site transnational clinical trials, as well as potential privacy risks for research participants in simply not knowing or fully understanding what they may be consenting to when they enter a clinical trial depending on their residency status (i.e., whether they are European Union residents, California residents, or residents of another country or U.S. state).[14]

These data protection efforts and others that are emerging in the United States and abroad, could benefit from incorporating strategies used in a participant-centric MIC, such as a dynamic consent process where participants and researchers have ongoing communication and enabling participant access to individual-level data. These strategies bring into harmony the goals of open science and data protection to promote free movement of personal data so long as there are efforts to secure data and recognize participants' rights.[15] Additional benefits with a participant-centric MIC approach include cultivating trust among research participants in the context of big data.[16] A system that emphasized trust could support diverse recruitment, better retention in clinical trials, and greater openness towards secondary use of personal data.

This Article is organized into four parts. Part I describes the benefits and privacy risks related to the use of wearable devices in clinical trials. Part II provides background information on GDPR and CCPA, and discusses their influence on state data privacy laws. Part III includes an analysis of participants' rights in relation to the research

12. *See* Phillips & Knoppers, *supra* note 7, at 107.

13. *See* Commission Regulation 2016/679, art. 89(2), 2016 O.J. (L119) 1, 84–85 (EU). The GDPR claims that there must be exemptions to some participants' rights in order to fulfil the purposes of scientific research. *See* CAL. CIV. CODE § 1798.105(d)(6) (West 2020). "Engage in public or peer-reviewed scientific, historical, or statistical research . . . deletion of the information is likely to render impossible or seriously impair the achievement of such research." *Id.*

14. The GDPR attempted to harmonize member states for greater consistency with data protection, but, under Article 9, member states are allowed flexibility to introduce further restrictions in the processing of sensitive data, such as health, biometric, and genetic data. Commission Regulation 2016/697, art. 9, 2016 O.J. (L119) 1, 38–39 (EU).

15. *See* Phillips & Knoppers, *supra* note 7, at 110.

16. *See* McGuire et al., *supra* note 9, at 17.

exemption under the GDPR and CCPA. Part IV proposes recommendations from the open science movement, specifically a participant-centric MIC to better align individual data protections with research participant engagement.[17]

I. Real-World Evidence and Wearables in Clinical Trials

Wearables are not new, but the introduction of commercial grade devices to clinical trials is a recent innovation that is starting to emerge.[18] Wearables have been rising in popularity around the world since 2006.[19] Estimates predict another surge in the next few years, which expect the wearable market to double to $27 billion market by 2022.[20] This growth reflects an increase in the general public's monitoring of overall health and wellness, as well as in research.

Wearables are defined as a small electronic device containing one or more sensors that are integrated into clothing or other accessories that can be worn on the body, such as on a wristband, belt, headband, adhesive patch, contact lens, or glasses. [21] Typical consumer-grade, activity-tracking wearables, such as the Apple Watch or Garmin Viovofit, come with a three-axis accelerometer to track movement in every direction and many have additional sensors, such as a gyroscope to measure orientation as well as an altimeter to determine feet hiked or stairs climbed.[22] These consumer-grade wearables can also be used to collect other biometric measures such as sleep, temperature, and heart rate.[23]

The more sensors a wearable has, the more accurate raw data it collects. Raw data is inputted into the device's algorithm and trans-

17. *See Global Open Access Portal: Open Science Movement*, UNESCO.org (2017), http://www.unesco.org/new/en/communication-and-information/portals-and-platforms/goap/open-science-movement/.

18. *See* Bill Byrom et al., *Selection of and Evidentiary Considerations for Wearable Devices and Their Measurements for Use in Regulatory Decision Making: Recommendations from the ePRO Consortium*, 21 Value in Health 6, 631–39 (2018). The authors discuss the potential of wearables to collect rich data and provide valuable insights, yet there is limited guidance on the acceptability of wearables in the clinical trials. Wearables are grouped into four categories from external (e.g., 3D camera monitoring movement), worn (devices worn on clothing or on body), implantable (inserted into body), and ingestible (swallowed by the user).

19. *See* Amy Westervelt, *Wearable Tech Helps You Live in the Moment*, Sci. Am. (May 29, 2014), https://www.scientificamerican.com/article/wearable-tech-helps-you-live-in-the-moment.

20. *See* Paul Lamkin, *Smart Wearables Market to Double By 2022: $27 Billion Industry Forecast*, Forbes (Oct. 23, 2018) https://www.forbes.com/sites/paullamkin/2018/10/23/smart-wearables-market-to-double-by-2022-27-billion-industry-forecast/#3583a50c2656.

21. *See* Byrom et al., *supra* note 18, at 631.

22. Caroline Saunders, *Balancing Innovation and Regulation: Why the FDA should adopt a More Dynamic Risk-Based System for Wearables*, 58 Jurimetrics 83, 91 (2017).

23. *See id.*

lated into user-friendly statistics on the device. Data stored on the wearables can be uploaded using a Bluetooth connection to a mobile device, such as smartphones, tablets, or laptops and then is transmitted to a server that holds a larger data set that is part of the clinical trial. "Data may be collected in real time, scheduled intervals, or be proximity-based."[24] Wearables in clinical trials range from consumer devices—to clinical grade wearables—such as those developed by Empatica—that are able to measure more specific health conditions, including the onset of a seizure.[25]

Currently, about fifteen percent of clinical trials incorporate wearable devices, but in a study conducted by Intel, Kaiser Associates estimates that by 2025 seventy percent of clinical trials will incorporate this type of sensor technology.[26] Wearables can support the collection of real-world data, which the 21st Century Cures Act defines as "data regarding the usage, or the potential benefits or risks, of a drug derived from sources other than traditional clinical trials."[27] A recent study on the increasing adoption of wearables in clinical trials emphasized how real-world data collected from wearables can directly address limitations in traditionally designed clinical studies.[28] Specifically, there are fewer in-person tests, which reduces not only time and costs, but also the burden on research participants. The study stated:

> While, in the past, more measurements would have directly increased the burden [on research participants], the use of wearable medical devices can be worn for a prolonged period [and] offer data without the need for the subject to be bothered over and over again.[29]

Clinical trials are typically designed to focus on a reduction of symptoms, rather than to measure whether the drug or device makes the participant's life more liveable.[30] For example, a common test in a clinical trial is a walking test from one point to another over a set distance. In contrast, measures in a natural environment tracked by wearables can report walking, stair climbing, and other daily move-

24. Christophe Mombers, Kathleen Legako & Annette Gilchrist, *Identifying Medical Wearables and Sensor Technologies that Deliver Data on Clinical Endpoints*, 81 BR. J. CLIN. PHARMACOL. 196, 197 (2015).

25. *See, e.g.*, *id.* at 196. For example, a company called Empatica develops wearables to monitor seizures, which can help manage Epilepsy and other medical conditions.

26. *See* Denise Myshko, *Wearables in Clinical Trials*, PHARMAVOICE (Mar. 2019), https://www.pharmavoice.com/article/2019-03-wearables/.

27. *See* 21st Century Cures Act, Pub. L. No. 114-255, 130 Stat. 1033 (Dec. 13, 2016).

28. *See* Mombers, Legako & Gilchrist, *supra* note 24, at 198.

29. *Id*. at 198.

30. *Id*. at 196.

ments over a twenty-four-hour window for a long period of time, stretching over weeks or months. This form of data provides researchers and the participants with practical information (e.g., how is the participant's performance with '*x*' activity at different times of the day compared over days and weeks?). This type of real-world data collected from wearables can be analyzed to produce real-world evidence and be used to provide insights into how the treatment is effecting participants' activities of daily living and, ultimately, their quality of life.

The FDA and others have acknowledged a gap between traditional clinical trials and the evidence needed to support a drug's optimal use in a natural, real-world environment.[31] Clinical trials, as they are traditionally designed, suffer from major shortcomings including length of time, expense, and high failure rate.[32] National Institutes of Health Director, Francis Collins, summarized the poor performance as the average length of time takes thirteen years from target discovery to regulatory approval, the failure rate exceeds ninety-five percent, and the cost per successful drug is over $1 billion, after adjusting for previous failures.[33] Furthermore, their design and protocol may artificially inflate treatment adherence with research staff and coordination that is heavily involved in the delivery of care.[34]

Given the high-cost and low success rate present in clinical trials and the advantages available with wearable technology, it is not surprising that the Clinical Trials Transformation Initiative (CTTI) issued a report in 2018. The report strongly endorsed the use of wearables in clinical trials.[35] CTTI is a patient-centered public-partnership whose primary aim is "to develop and drive adoption of practices that will increase the quality and efficiency of clinical trials."[36] In the 2018 report, CTTI highlighted the abilities of wearables to reduce barriers to

31. *See generally* Mombers, Legako & Gilchrist, *supra* note 24, at 196.

32. Francis S. Collins, *Reengineering Translational Science: The Time is Right*, 3 SCI. TRANSL. MED. 90, 1 (2011).

33. *See, e.g.*, Elizabeth Hall-Lipsy, Leila Barraza & Christopher Robertson, *Practice-Based Research Networks and The Mandate for Real-World Evidence*, 44 AM. J. L. & MED. 219, 221 (2018).

34. *Id*.

35. *CTTI Recommendations: Advancing the Use of Mobile Technologies for Data Capture & Improved Clinical Trials*, CLINICAL TRIALS TRANSFORMATION INITIATIVE (CTTI) (2018), https://www.ctti-clinicaltrials.org/files/mobile-devices-recommendations.pdf [hereinafter CTTI 2018].

36. Clinical Trials Transformation Initiative, *Strategic Plan*, CLINICAL TRIALS TRANSFORMATION INITIATIVE (CTTI) (May 2016), https://www.ctti-clinicaltrials.org/who-we-are/strategic-plan.

clinical trial recruitment, lower costs, and increase research participant engagement.[37]

The science behind wearables continues to advance due to the popular demand for public use and use in clinical research.[38] For example, a growing range of physiological functions, including brain activity, muscle tension, hydration levels, blood pressure, temperature, stress, and blood chemistry can be regularly collected and stored.[39] Data from wearables also contains physical information about each research participant, including their exact location with dates and time stamps. If taken together, then this data could be used to reach conclusions about a research participants' whereabouts on any given day and time as well as physical and emotional states. Vice President of Clinical Data at Veeva, Richard Young, sums up the data progression: "Ten years ago, there were a *million data points* in a big Phase III study . . . . Today, we are talking about collecting *millions of data points per patient per day*."[40]

The data collected from wearables offers an abundance of information that may go beyond, or be unrelated to, the data needed in a particular study for which it is being collected and processed. This is where unintended data issues surface as well related privacy concerns. Essentially, unintended data is personal data that may not be relevant to a stated research purpose and is collected by virtue of the transmission process. The regular uploading of personal data that includes continuous health monitoring over extended periods of time may provide more depth and detail than research participants may be aware of or would have consented to and presents privacy risks that are in need of further examination. Some privacy advocates claim access to this kind of unintended data violates notions of fairness and integrity in the scientific process; and refer to this access as "the biggest civil rights issue of our time."[41]

The privacy concerns regarding the use of wearables in clinical trials are echoed in data sharing. Some privacy scholars fear that even with pseudonymization, anonymization, and other protective measures

37. *See* CTTI 2018, *supra* note 35.

38. Paul Lamkin, *Smart Wearables Market to Double By 2022: $27 Billion Industry Forecast*, FORBES (Oct. 23, 2018), https://www.forbes.com/sites/paullamkin/2018/10/23/smart-wearables-market-to-double-by-2022-27-billion-industry-forecast/#3583a50c2656.

39. *See* McGuire et al., *supra* note 9.

40. *See* Myshko, *supra* note 26 (emphasis added).

41. Omer Tene & Jules Polonetsky, *Beyond IRBs: Ethical Guidelines for Data Research*, 72 WASH. & LEE L. REV. 458, 459 (2016) (citing Alistair Croll, *Big Data is Our Generation's Civil Rights Issue, and We Don't Know It*, O'REILLY RADAR (Aug. 2, 2012), http://radar.oreilly.com/2012/08/big-data-is-our-generations-civil-rights-issue-and-we-dont-know-it.html).

used to de-identify personal data, there may still be a risk to re-identify individuals, which could have a chilling effect on participation in clinical trials.[42] International organizations, such as the Biometrics Institute,[43] are finding privacy concerns lead to a similar reluctance with wearable use and suggest global standards and guidelines for wearables that support responsible and ethical use of personal data.[44] In a survey presented at a recent Biometrics Institute Conference, seventy-nine percent of participants indicated that privacy concerns were the most significant roadblock for wider adoption of wearable technology.[45]

Wearable use in clinical trials is projected to dramatically increase over the upcoming years.[46] The potential advantages to reduce barriers, lower costs, and accelerate the regulatory approval process could offer substantial public health benefits.[47] In addition, wearables play a key role in enabling large-scale, participant-driven data collection where research participants are responsible for reporting data through their personal devices. This shift in clinical trial design could expand research participant engagement in several ways, ranging from overall quality improvement to patient safety.

The utilization of wearable technology incorporates feedback for individual preferences, their physical reactions and satisfaction levels with the treatment over time and with certain daily activities (e.g., climbing stairs, walking, and sleeping).[48] This type of feedback model aligns with the concept of continuous quality improvement—systematically measuring and iteratively improving customer or patient satisfaction—in which quality improvement is defined and measured from the patient perspective.[49] In a clinical trial, collection of dense physio-

42. *See* Mello et al., *supra* note 5, at 2203; GDPR Article 4 defines pseudonymization as "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information." Commission Regulation 2016/697, art. 4, 2016 O.J. (L119) 1, 33 (EU).

43. Biometrics Institute, https://www.biometricsinstitute.org/ (last visited Jan. 22, 2020).

44. *See, e.g.*, Chris Burt, *Biometrics Institute Announces Initiatives to Support Ethical and Responsible Biometrics Use*, BIOMETRIC UPDATE.COM (Jan. 29, 2019), https://www.biometricupdate.com/201901/biometrics-institute-announces-initiatives-to-support-ethical-and-responsible-biometrics-use.

45. *See* Unisys Corporation, *Unisys Survey Finds Wearable Technology to Revolutionize Biometrics; Privacy Issues Yet to Be Addressed*, PR NEWSWIRE (Aug. 23, 2016), https://www.prnewswire.com/news-releases/unisys-survey-finds-wearable-technology-to-revolutionize-biometrics-privacy-issues-yet-to-be-addressed-300316454.html.

46. *See generally* Myshko, *supra* note 26.

47. *See* CTTI 2018, *supra* note 35.

48. *See generally* Byrom et al., *supra* note 18.

49. *See, e.g.*, Eleanor D. Kinney et. al., *Quality Improvement in Community-Based, Long-Term Care: Theory and Reality*, 20 AM. J. L. & MED. 59, 73 (1994); *see also* Rachel Zuraw &

logical data may identify early safety issues, as well as inform dose adjustments and frequencies.[50] Research participants could add their voice to the data collected by wearables and help identify potential safety issues and dosing preferences; even difficulties with medication adherence could support safety goals and participants' retention in the clinical trial.

There are benefits associated with the use of wearables in clinical trials that could greatly improve the traditional clinical trial design from producing real-world data, reducing costs, and supporting greater engagement with research participants. However, these benefits need to be considered in conjunction with the ability of wearables to generate vast amounts of unintended data that research participants may not be aware they are providing. Given the escalating use of wearables in clinical trials and rapidly developing sensor capabilities that will increasingly be able to collect a greater granularity in physiological functions, there are privacy risks that should be urgently addressed in the evolving regulations, namely GDPR and CCPA.

II. Data Protection Rights

The GDPR and CCPA reflect a worldwide trend towards greater accountability to protect personal data, while simultaneously balancing support for research and the responsible sharing of clinical data. The GDPR, which went into effect in May of 2018, is working to reconcile these goals and resolve uncertainty with further guidance from the European Commission and other agencies.[51] The CCPA took effect in January of 2020, solely for California residents, but continues to be considered by other states and federally for future regulation.[52] The advances in wearables and other sensor technologies could further impact current and future data protection regulations in ways not fully fathomed. All these factors suggest that there is an opportunity to refine how the GDPR, CCPA, and other data privacy laws regulate research so that it is compatible with the goals of research participant engagement and open science.

The GDPR and CCPA define personal data and participants' rights to processing of personal data with notable differences. The GDPR

Tara Sklar, Digital Health Privacy and Age: Quality and Safety Improvement in Long-Term Care, Ind. Health L. Rev. (forthcoming 2020).

50. *See* Elena S. Izmailova et al., *Wearable Devices in Clinical Trials: Hype and Hypothesis*, 104 Clin. Pharmacol. Ther. 42, 43 (2018).

51. Commission Regulation 2016/679 of April 27, 2016, General Data Protection Regulation O.J. (L 119) 1.

52. Cal. Civ. Code § 1798 (West 2020).

considers personal data as "any information relating to an identified or identifiable natural person, directly or indirectly."[53] This can encompass addresses, license plate numbers, social security numbers, blood type, bank account information, and a person's online identifiers, such as Internet Protocol addresses as well as one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.[54] The CCPA defines personal data as "any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked directly or indirectly, with a particular consumer or household."[55] Both the GDPR and the CCPA are concerned with protecting information that could be directly or indirectly linked to identify a natural person.[56]

A. General Data Protection Regulation

The GDPR was passed by the European Union in 2016 and went into effect in May of 2018 across thirty-one countries, with implications for any entity that processes data from an EU resident.[57] Although the GDPR is an EU regulation, it applies to *all* organizations (businesses, non-profits, and government entities) that collect, process, or hold data collected from users in the European Union, regardless of where the controllers or processors are based.[58] Entities are subject to the GDPR if their activities involve processing of personal data of an individual located in the European Union, which can range from a U.S. citizen temporarily in the European Union with a wearable device to multi-site transnational clinical trials, or a data center on another continent storing data collected from persons in the European Union.

---

53. *See* Commission Regulation 2016/697, art. 4(1), 2016 O.J. (L119) 1, 33 (EU).

54. *See id.*

55. *See* CAL. CIV. CODE § 1798.140 (West 2020).

56. See Table 1 for a side-by-side comparison of participants' rights granted under the GDPR and CCPA.

57. There are twenty-eight EU member states and thirty-one states that are part of the European Economic Area. There are additional countries that the EU Commission recognizes as providing an adequate level of data under its "adequacy" status in Article 45 of the GDPR. Commission Regulation 2016/697, art. 45, 2016 O.J. (L119) 1, 61 (EU). *See also* European Commission, Adequacy of the Protection of Personal Data in Non-EU Countries, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en.

58. *See id.*

The GDPR overhauls the ways in which organizations collect, use, and share personal data.[59] In a research setting, the GDPR aims to support digital technology (including wearables) by reducing barriers to process personal data for a research purpose, while maintaining ethical obligations regarding consent and protection of research participants. The GDPR also attempts to address "shortcomings" of the previous EU data privacy law that was passed in 1995, Data Protection Directive (DPD).[60] Examples include the creation of notification policies for participants and authorities when there is a data breach and the strengthening of rules for data minimization.[61]

The GDPR has seven key principles for processing of personal data: "Lawfulness, fairness and transparency[;] purpose limitation[;] data minimization[;] accuracy[;] storage limitation[;] integrity and confidentiality (security)[; and] accountability."[62] The principles relating to purpose limitation and data minimization are the most pertinent to the question of how to regulate unintended data generated by wearables in clinical trials. Overall, even if the data collection and processing is done in a research setting, the GDPR aims for organizations to limit the scope to: (1) A person's data may only be collected for a specific purpose; (2) The person must be informed of and consent to the purpose for which their data is collected; (3) Only as much data as is necessary to achieve that purpose should be collected; (4) The collected data must be deleted at the request of the person from whom it was collected, or when it is no longer needed for the purpose for which it was collected.[63] In short, GDPR asks all organizations to understand what data they are collecting, why they are collecting it, and to establish mechanisms to manage that data.

B. California Consumer Privacy Act

The CCPA was signed by Governor Jerry Brown on June 28, 2018 and went into effect on January 1, 2020.[64] Although not as extensive in scope as the GDPR, it is arguably the strongest U.S. consumer privacy

59. *See, e.g.*, Edward S. Dove, *The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era*, 46 J. L., MED., & ETHICS 1013, 1014 (2018).

60. *See* Directive 95/46, 1995 O.J. (L 281) 1, 31 (EC).

61. *See, e.g.*, Politou, Eugenia, Efthimios Alepis & Constantinos Patsakis, *Forgetting Personal Data and Revoking Consent Under the GDPR: Challenges and Proposed Solutions*, 4 J. OF CYBERSECURITY 1, 4 (2018).

62. *Guide to the General Data Protection Regulation*, INFORMATION COMMISSIONER'S OFFICE https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/ (last visited Jan. 22, 2020).

63. *See id.*

64. CAL. CIV. CODE § 1798 (West 2020).

law to date and an outcome of the GDPR's influence. The CCPA provides California residents with a legal framework to protect their personal data. Its applicability is limited to large businesses with $25 million or more in gross revenues, processing data of 50,000 consumers, and fifty percent of revenue from data sales.[65] The CCPA creates new rights that make current privacy notices and their more generalized statements obsolete. For instance, under the right to data access, consumers (i.e., participants) can request from a business the categories of personal information, and the specific pieces of personal information, that the business has collected about the specific consumer.[66] The business must then notify consumers of this fact.[67] Meanwhile under the right to deletion, consumers can request that a business delete any of their personal information that the business holds, and the business's online privacy notice must include notification of this right.[68]

The CCPA also requires, upon receipt of a verifiable consumer request, that a business collecting personal information about the consumer disclose the following:[69]

1. Categories of personal information collected about the consumer.
2. Categories of sources from which personal information is collected.
3. Business or commercial purposes for collecting or selling the personal information.
4. Categories of third parties with which the personal information is shared; and
5. Specific pieces of personal information collected about that consumer.

65. *See* § 1798.140(c).
66. *See* § 1798.100.
67. § 1798.100.
68. § 1798.105.
69. § 1798.115.

TABLE 1: Participants' Rights Granted Under the CCPA and GDPR

	CCPA	GDPR
Rights Granted	1. Right to disclosure 2. Right to deletion 3. Right to data access 4. Right to opt-out 5. Right to non-discrimination	1. Right to be informed 2. Right to access 3. Right to rectification 4. Right to erasure 5. Right to restrict processing 6. Right to data portability 7. Right to object 8. Rights in relation to automated individual decision making, profiling

C. GDPR and CCPA Influence on State Data Privacy Laws

A controversial issue on which the GDPR and CCPA diverge is opt-out/opt-in consent, and this is also hotly contested in state data privacy laws. The CCPA uses the right to opt-out, which enables consumers to, at any time, opt out of a business's sale of a consumer's personal information to third parties.[70] Furthermore, any businesses that may sell personal information to third parties are required to provide notice of potential sale and of a consumer's right to opt-out.[71] The GDPR mandates an opt-in approach, which means that individuals must provide affirmative consent for their data to be processed, meaning it must be "freely given, specific, informed and unambiguous."[72] The trend in the United States regarding state data privacy laws follows the CCPA model and allows individuals to opt-out of certain uses, namely the selling of their personal data to a third party.[73]

Critics of the GDPR claim that the opt-in approach would stymie competition, since consumers might only opt-in to more established companies' websites and online services.[74] They also doubt whether it

70. CAL. CIV. CODE § 1798.120 (West 2020).

71. § 1798.120.

72. Commission Regulation 2016/697, art. 4(11), 2016 O.J. (L119) 1, 34 (EU). Article seven of the GDPR further discusses the conditions of consent. *See id.* at art. 7, 37.

73. CAL. CIV. CODE § 1798.115(d).

74. Caroline Spiezio, *Privacy Notices, Opt-In Clauses Debated as US Regulators Shape Federal Privacy Law*, CORPORATE COUNSEL (Mar. 12, 2019), https://www.law.com/corpcounsel/2019/03/

enhances individuals' privacy.[75] In contrast, advocates for the opt-in approach note that most people do not adjust the default settings and have concerns that it is not possible to meaningfully opt-out.[76] This opt-in preference is largely shared by those who support a participant-centric MIC. Studies show that research participants prefer opt-in consent, and some experts claim that opt-out consent can be exploitative, erode trust, and come off as sneaky.[77]

The GDPR and CCPA also sharply diverge on sanctions for non-compliance. The GDPR provides a tiered approach where organizations can be fined up to four percent of annual global turnover or €20 million, whichever is greater, for breaches of data protection principles or data participants' rights.[78] An organization can be fined €10 million or two percent of annual global turnover, whichever is greater, for data security breaches, not informing data participants about a breach, or poor record keeping.[79] In contrast, the CCPA fines organizations in breach up to $2,500 per violation for negligent violations and up to $7,500 per violation for intentional violations.[80]

This wide disparity in sanctions between the GDPR and CCPA have implications for an organization's level of effort to secure data, and the future direction of state data privacy laws. If sanctions are minimal, then data security may not receive the resources necessary to make it a top priority. Related concerns regarding accountability, enforcement, and recourse for victims of data misuse or privacy breaches are all important considerations in refining the GDPR, CCPA, as well as the current and proposed state data privacy laws.

Interestingly, Senators Amy Klobuchar (D-MN) and Lisa Murkowski (R-AK) recently proposed the Protecting Personal Health Data Act,[81] a bi-partisan federal data privacy law that incorporated principles directly from the GDPR. Namely, the Bill would allow individuals to delete and amend their health data as well as access individual copies.[82] This proposed legislation is particularly notable in the con-

---

12/privacy-notices-opt-in-clauses-debated-as-us-regulators-shape-federal-privacy-law/?slreturn=20190230102041.

75. *Id.*

76. *Id.*

77. *See* McGuire et al., *supra* note 9, at 16.

78. *See* Dove, *supra* note 59, at 1013.

79. *Id*. at 1015.

80. *See* CAL. CIV. CODE §§ 1798.150, 1798.155(c) (West 2020). The CCPA creates the "Consumer Privacy Fund" within the General Fund of the State Treasury.

81. *See* Protecting Personal Health Data Act, S. 1842, 116th Cong. (2019), https://www.congress.gov/bill/116th-congress/senate-bill/1842?q=%7B%22search%22%3A%5B%22personal+data+health%22%5D%7D&s=1&r=1.

82. *Id.*

text of this Article for its goal to directly address the category of personal health data collected by wearables and related technologies. If enacted, Health and Human Services would, in conjunction with other regulatory stakeholders, promulgate regulations that would strengthen privacy and security protections for personal health data; apply uniform standards for consent as well as appropriate exceptions; include minimum security standards; and require limits on collection, use, and disclosure of data to only those directly relevant and necessary to accomplish a specific purpose.[83] Not surprisingly, California is considering a similar bill, Information Privacy: Digital Health Feedback Systems,[84] concerning this type of health data. This proposed legislation would expand California's health privacy law to include any information from a digital health feedback system, which is broadly defined to include sensors, devices, and internet platforms that receive personal health data.[85]

III. Research Exemption and Related Safeguards

Legislators passed the GDPR and CCPA to strengthen privacy and data protection, while allowing an exemption for research. They differ both in how they define research and in how they apply a research exemption, which allows for some research participants' rights to be curtailed—specifically, the rights to erase or delete personal data and restrict processing.[86] For example, organizations may not be required to comply with participants' requests to erase their data from the clinical trial as that right is "likely to render impossible or seriously impair the achievement of the specific purpose."[87] Retention is a challenge for clinical trials, in general, and allowing participants to entirely erase their data could jeopardize the quality of the data and significance of the research findings. Researchers may also avoid restrictions under this exemption and conduct *further* processing of sensitive categories of data if they can show a "compatible purpose" with the data

83. *Id.*

84. Information Privacy: Digital Health Feedback Systems, A.B. 384, Reg. Sess. (Cal. 2019).

85. *Id.*

86. *See* GDPR's art. 17(3)(d) so-called right to be forgotten does not apply if processing is for research purposes as defined under art. 89(1). *Compare* Commission Regulation 2016/679, art. 17(3)(d), 2016 O.J. (L119) 1, 44 (EU) *with* Commission Regulation 2016/679, art. 89, 2016 O.J. (L119) 1, 84–85 (EU). *See also* Cal. Civ. Code § 1798.105 (West 2020).

87. *See* Commission Regulation 2016/679, art. 89(2), 2016 O.J. (L119) 1, 84–85 (EU). The GDPR claims that there must be exemptions to some participants' rights in order to full the purposes of scientific research. *See also* Cal. Civ. Code § 1798.105(d)(6). "Engage in public or peer-reviewed scientific, historical, or statistical research . . . when the businesses' deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent." *Id.*

that was initially collected.[88] This Part discusses the differences between the GDPR and CCPA in a research context, including approaches to consent, exemption, and safeguards for research participants' data.

The GDPR offers more flexibility than its predecessor, the DPD, by providing greater latitude in creating new exemptions for researchers to process personal data. This broad research exemption reflects its mandate to facilitate a digital single market across EU member states.[89] As such, the GDPR provides a far-reaching definition of research where it encompasses "technological development and demonstration, fundamental research, applied research, and privately funded research."[90] This results in a wide umbrella of "research" activities that could be included under the research exemption. The CCPA, by contrast, has a limited scope in how it defines research. Specifically, research only refers to federally sponsored research.[91] It is unclear if privately funded research could also claim a research exemption and override certain participants' rights.

Since this is an evolving area of determining how to regulate vast amounts of personal data in clinical trials, it is unclear how to align participants' rights with informed consent without placing an undue burden on researchers, particularly for sponsors that run transnational clinical trials. Consistent with its aim to promote harmonization across the European Union, the GDPR attempts to satisfy the ethical obligation for consent in such a way that it would minimize the burden for data processing in an international research context.[92] The GDPR requires informed consent and that researchers treat participants in a fair and transparent way by providing information about what their data will be used for, who will process it, and how it will be stored.[93]

The CCPA follows the revised Common Rule, which is the Basic HHS Policy for Protection of Human Research Subjects, which requires broad consent.[94] If researchers are able to obtain broad consent for the storage, maintenance, and secondary research use of identifiable biospecimens and data, then any subsequent uses of the individ-

88. Commission Regulation 2016/679, art. 9(2)(j) & 6(4) & Recital 50, 2016 O.J. (L119) 1, 39 & 37 & 9–10 (EU).

89. *See* Gabe Maldoff, *How GDPR Changes the Rules for Research,* International Association of Privacy Professionals, IAPP.ORG (Apr. 19, 2016), https://iapp.org/news/a/how-gdpr-changes-the-rules-for-research/.

90. *See* Commission Regulation 2016/679, Recital 159, 2016 O.J. (L119) 1, 30 (EU).

91. CAL. CIV. CODE § 1798.145(c)(1)(C) (West 2020).

92. *See* Maldoff, *supra* note 89.

93. *See* Commission Regulation 2016/679, art. 7, 2016 O.J. (L119) 1, 37 (EU).

94. *See* 45 C.F.R. § 46.104 (d)(7) (2018).

ual's identifiable biospecimens and data consistent with the initial broad consent would not require additional consent.[95] The CCPA defines research in such a narrow way that if an organization meets the research definition, then it seems straightforward to apply the research exemption. The GDPR is less clear in whether specific or broad consent is required, even if a research exemption applies.[96]

The research exemption is subject to safeguards under the GDPR and CCPA. The GDPR includes several safeguards, with the principles of data minimization, purpose limitation, and "data protection by design" as the most applicable to this issue of unintended data largely collected from wearables.[97] The principle of data minimization states that only data, which is "adequate, relevant, and limited to what is necessary in relation to purposes for which data is being processed" should be collected, stored, and used.[98] The purpose limitation requires that data should not be processed for any other purpose and should not be held after the data storage expires.[99] This type of data protection by design requires researchers to put in place "technical and organizational measures" to ensure that they process only the personal data necessary for the research purposes.[100]

The CCPA provides a similar safeguard, which is, "permit access only to the minimum necessary personal information needed for the research project."[101] There is a lack of clear guidance in how to reconcile the research exemption with its related safeguards when it comes to unintended data. The implications of this could be whether the research exemption will override participants' rights for processing unintended data, meaning data that may not be necessary for carrying out the stated research purpose. A further complication for predictability goals is that EU member states can require additional safeguards for any exemptions granted for research purposes.[102]

IV. Research Participants' Data and Open Science

International collaboration in the research space is supported through responsibly sharing clinical trial data, which has been critical

95. *Id*.

96. *See* Phillips & Knoppers, *supra* note 7, at 109.

97. Commission Regulation 2016/679, art. 5, 2016 O.J. (L119) 1, 35–36 (EU).

98. *See id.*, art. 5(1)(c), 35.

99. *Id.*, art. 5(1)(b), 35.

100. *See id.*, art. 5, 35–36.

101. *See* Cal. Civ. Code § 1798.24(t)(2)(B) (West 2020).

102. *See* Commission Regulation 2016/679, art. 9(2)(j), 2016 O.J. (L119) 1, 39 (EU).

to improve drug development and regulatory processes.[103] Much emphasis has been placed by regulatory agencies on the importance of data sharing, especially for its ability to shed light on concerns of inaccurate, biased, and insufficient reports that would be nearly impossible to resolve without access to underlying trial data.[104] Additionally, scientific discovery could advance with access to this data and potentially identify issues that were missed, understudied, or buried. As wearables become increasingly used in clinical trials, sharing data from these devices will become more widespread and could exponentially improve medical knowledge, particularly once challenges around data translation are addressed.

There are a number of strategies that relate to an open science initiative of responsibly sharing clinical trial data through a participant-centric MIC and that also align with data protection principles. This Part describes three strategies that adhere to the goals of the GDPR and CCPA and have the potential to expand research participant engagement in clinical trials. The strategies are dynamic consent, participant access to individual-level data, and a robust system of accountability.

Dynamic consent is not required under the GDPR or CCPA but could provide some needed clarity as well as support for research and innovation goals. Dynamic consent is primarily designed to facilitate two-way, ongoing communication between the researcher and research participant.[105] It utilizes a communication platform that allows researchers to follow up with participants over time, which, given the real-time capabilities of using wearables in research, could be a tremendous advantage for early identification of potential safety issues or adjustments for dosing amounts and frequencies. This approach could improve retention as researchers can be more responsive if participants are thinking of dropping out of a trial due to a change in their condition or adverse response to the treatment. Also, dynamic consent could alleviate data protection concerns regarding whether research participants fully comprehend the level of detail and depth that is collected about them through wearables' continuous health monitoring. Lastly, dynamic consent supports follow-up studies where researchers are more likely to stay in contact with participants that may have moved locations or reengage them if they have lost interest.

---

103. *See* Martha Brumfield, *The Critical Path Institute: Transforming Competitors into Collaborators*, 13 NATURE REVS. DRUG DISCOVERY 785 (2014).

104. *Id*.

105. *See* Mary A. Majumder et al., *The Role of Participants in a Medical Information Commons*, 47 J. L., MED. & ETHICS 51, 53 (2019).

Access to individual-level data is a feature that can be addressed during the design process and is also part of the participants' rights to personal data protection. In addition, this feature promotes transparency and trust between researchers and research participants, as well as empowerment for the participant by allowing them to become more engaged in the research process.[106] A robust system of accountability closely aligns with the goals of data protection—requiring sanctions and outline enforcement mechanisms. There are benefits to harmonizing an accountability system so that researchers can comply without conflicting requirements across jurisdictions. Additionally, research participants could understand their rights and redress options available to them if there is a data breach or misuse of data that is not dependent on their particular location.

There is tremendous opportunity to inform the evolving GDPR, CCPA, state data privacy laws, and potential federal data privacy laws with these types of strategies, which could also expand research participant engagement. Incorporating these strategies could address some of the confusion regarding the safeguards for data protection under the GDPR. For example, dynamic consent would ensure that research participants' preferences and concerns are part of whether they consider minimal data collection related to the research purpose. Researchers should consider the ethical and practical benefits in adopting these types of strategies, which range from better meeting the needs of those receiving the treatment to complying with data protection principles and reducing costs associated with attrition.

Conclusion

The GDPR and CCPA affirmatively recognize research participants' greater control over personal data. However, it is unclear how these types of data protection regulations will balance privacy with research, especially in regard to applying the research exemption to data that arguably does not meet the data minimization safeguards required under the GDPR and CCPA. The current regulations represent a step forward in the global trend to enhance participants' rights, particularly when there are potential privacy risks with the increasing use of wearables and related technologies. Amendments to the GDPR, CCPA, and state data privacy laws are actively taking place, and new data protection regulations are being proposed. Now is

106. *See* McGuire et al., *supra* note 9, at 17.

the time to introduce approaches that align the goals of data protection with open science and bring a needed level of continuous participant engagement into the research process.