To What Extent Does the EU General Data Protection Regulation (GDPR) Apply to Citizen Scientist-led Health Research with Mobile Devices?

(*Journal of Law, Medicine & Ethics*, Forthcoming)

Edward S. Dove[1] and Jiahong Chen[2]

[1] School of Law, University of Edinburgh, United Kingdom.

[2] Horizon Digital Economy Research, University of Nottingham, United Kingdom.

Edward S. Dove, Ph.D., is a Lecturer in Health Law and Regulation at the School of Law, University of Edinburgh. Jiahong Chen, Ph.D., is a Research Fellow in IT Law at Horizon Digital Economy Research, University of Nottingham.

Introduction

The EU's General Data Protection Regulation 2016/679 (GDPR),[1] which went into effect on May 25, 2018, governs the processing of personal data in Europe and promotes responsible data processing for a range of legitimate purposes.[2] The GDPR contains specific provisions for scientific research that involves processing of personal data.[3] These provisions clearly cover health research conducted by scientists at academic medical centers, pharmaceutical companies, universities, and other traditional institutions and organizations. However, it is unclear the extent to which these provisions, or indeed the GDPR as a whole, covers "citizen scientist"-led health research with mobile devices.

"Citizen science" and "citizen scientists" are loose terms that describe individuals undertaking scientific research who are independent and disconnected from any institutional affiliation.[4] The terms include patients and their family members who undertake scientific research through, among other platforms, consumer genetic testing, access to electronic health records, social media that link various individuals with similar health conditions, and use of powerful computer algorithms that can search through numerous and diverse sources of data.[5] Not surprisingly, citizen science is generally not funded by any government agency. Funding, if it exists at all, comes from private sources such as personal savings and crowdfunding.

Mobile devices, including smartphones and tablets, almost ubiquitously now include apps that collect health information, such as heart rate, blood pressure, blood sugar, and other measurements. At the same, using the internet to contact and communicate with large numbers of individuals, it has become increasingly common for various types of health research to incorporate mobile devices at the platform to collect and process personal data. Although citizen science-led health research with mobile devices holds some promise – some would argue this includes the democratization of science, increased possibility for serendipitous discovery (i.e. more "blue skies research"), and increased statistical power to generate findings (through brining more individuals together to share data) – it also raises some risks.[6] These include the possible lack of consent from participants in research projects, inadequate privacy and security protections for sensitive data exchanged remotely or on the internet, questionable expertise to undertake scientifically rigorous and publishable findings, and even worsening of health conditions caused by improperly drawn conclusions about prevention and treatment options.[7]

In this article, we look at the risks associated with privacy protections through the prism of the GDPR (see Box 1 for key definitions in the GDPR). Given that the GDPR is an "omnibus" piece of data protection legislation that is intended to cover all sorts of personal data processing, it is presumed to cover citizen scientist-led health research. As will be discussed, however, there are potential exceptions in the law that may permit citizen scientists to escape the GDPR's reach. In the following sections, and through a series of questions, we consider the possible application of the GDPR and potential implications for citizen science, specifically focusing on a relatively under-discussed provision called the "household exemption." Ultimately, we argue that the GDPR likely *does* cover citizen science-led health research with mobile devices, depending on the specific context and the territorial scope. However, the remaining open questions that result from our analysis lead us to call for a *lex specialis*, such as a Code of Conduct for Health Research, that would provide greater clarity and certainty regarding the processing of health data by for research purposes, including by these non-traditional researchers.

We begin our analysis by exploring the definition of personal data under the GDPR and whether the types of data processed in citizen science-led health research with mobile devices would fall under the definition.

Box 1. Key definitions in the GDPR.

Personal data: Any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

Data processing: Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction.

Data controller: A natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data processor: A natural or legal person, public authority, agency, or other body which processes personal data on behalf of the data controller.

Definition of personal data

Among the several categories of data specified in the GDPR are categories defined by their identifiability of individuals. Here, three categories of data exist: personal, anonymous, and pseudonymous. Health data, as long as they are associated with an identified or identifiable individual, constitute personal data, and are therefore subject to the GDPR.[8] Under Article 4(15), data concerning health is defined as "personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status." In the GDPR Recitals (i.e. the context-providing paragraphs that appear before the Articles), it is clarified that "Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject."[9]

Conversely, anonymous data do not concern an identified or identifiable individual and are therefore not subject to the GDPR. As Recital 26 states:

> The principles of data protection should […] not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

Should citizen scientists collect anonymous data, they need not comply with the GDPR. It is, however, not always straightforward to ascertain whether a set of health data are fully anonymous. If the data subject can be re-identified by "means likely reasonably to be used either by the controller or by any other person"[10] then the data concerned would remain personal data. There have been various studies showing how seemingly perfectly anonymized health data can be re-identified with additional information that is publicly available.[11]

Finally, pseudonymous data are personal data that have been processed in such a way that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.[12] Since pseudonymous data remain personal data under the GDPR, the GDPR applies even where the data in question has gone through pseudonymization.[13] However, pseudonymization may help demonstrate compliance with requirements under the GDPR, such as making the secondary use of personal data compatible with the primary purpose,[14] as well data protection by design[15] and robust security measures,[16] particularly in the context of scientific research.[17]

In our view, health data collected through mobile devices is highly unlikely to qualify as anonymous data, as they are usually associated with a specific device, which de facto renders the individual identifiable, even without such details as the individual's name or specific whereabouts. This position is supported by Recital 30, which states:

> Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.

Thus, health data collected through mobile devices, including those that are pseudonymized, are most likely to fall within the definition of "personal data" and "data concerning health" under the GDPR.

Territorial scope and the household exemption

We must next consider the territorial scope of the GDPR, which has expanded the reach of European data protection law compared to the previous 1995 Data Protection Directive. Under Article 3, the GDPR applies to the processing of personal data in the context of the activities of an establishment (e.g. office or site) of a controller or a processor in the EU, regardless of whether the processing takes place in the EU or not. Hence, if a citizen scientist is conducting their research in the EU and

personal data are processed as part of that research, the GDPR will apply. The GDPR also applies to the processing of personal data of data subjects who are in the EU by a controller or processor not established in the EU, where the processing activities are related to:

- the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the EU; or
- the monitoring of their behavior as far as their behavior takes place within the EU.

So, where health research is being conducted through a mobile or wearable device with users situated in the EU, even when the citizen scientist is situated outside the EU, in our view, the GDPR would apply, as the scientist is arguably monitoring the users of mobile devices, or even providing a service (namely, research involving the users, with results that are likely fed back to the user in real time).

A more interesting question to consider in the citizen science context, though, is the GDPR's so-called "household exemption." Under Article 2(2)(c), the GDPR states: "This Regulation does not apply to the processing of personal data: […] by a natural person in the course of a purely personal or household activity." To put this in context, it may not be necessary for a mobile device to transmit any data beyond the confines of one's device. If data processing only takes place on the device itself and no personal data are transmitted beyond the device to some third-party entity or processor, the GDPR would seem to not apply. This is known as the household (or domestic) exemption and explained in Recital 18 of the GDPR:

> This Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. Personal or household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities.

As two EU data protection law scholars comment:

> This notion [purely personal or household activity] should be interpreted based on the general social opinion and includes personal data that is being processed for leisure activities, hobbies, vacation or entertainment purposes, for the use of a social network or data that is part of a personal collection of addresses, birthdays or other important dates, such as anniversaries.[18]

The Court of Justice of the European Union (CJEU) has clarified the scope of the household exemption in a few cases, which, though handed down during the time of the previous 1995 Data Protection Directive, should remain valid law given the unchanged wording of the household exemption from the Directive to the GDPR.

In the case of *Bodil Lindqvist v Åklagarkammaren i Jönköping* (Case C-101/01), the CJEU was asked to consider, among other questions, whether uploading personal data, including health data, onto an internet website by an individual can be regarded as outside the scope of 1995 Data Protection Directive on the ground that it is covered by one of the exceptions in Article 3(2), namely the household exemption. The CJEU ruled that posting data online about colleagues amounts to processing of personal data and cannot be exempted on the basis of personal or household

activities, as the details are "accessible to and indefinite number of people" on the internet. According to the Court:

> That [household] exception must therefore be interpreted as relating *only* to activities which are carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people.[19]

This reasoning was elaborated in the subsequent case of *František Ryneš v Úřad pro ochranu osobních údajů* (Case C-212/13), concerning the domestic use of a closed-circuit television camera (CCTV) around the front door of a family home, which happened also to capture partially images from a public street. Here, the CJEU was asked to consider, among other questions, whether the operation of a camera system installed on a family home for the purposes of the protection of the property, health, and life of the owners be regarded as outside the scope of the 1995 Data Protection Directive on the ground that it is covered by the household exemption, even though such a system also monitors, in part, a public space. Again, the CJEU maintained a narrow interpretation of what "personal or household activity" means:

> Since the provisions of Directive 95/46, in so far as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy, must necessarily be interpreted in the light of the fundamental rights set out in the Charter […], the exception provided for in the second indent of Article 3(2) of that directive *must be narrowly construed*.
>
> The fact the Article 3(2) […] falls to be narrowly constructed has its basis also in the very wording of the provision, under which the directive does not cover the processing of data where the activity in the course of which that processing is carried out is a "purely" personal or household activity, that is to say, not simply a personal or household activity.
>
> To the extent that video surveillance such as that at issue in the main proceedings covers, *even partially*, a public space and is accordingly directed outwards from the private setting of the person processing the data in that manner, it cannot be regarded as an activity which is a purely "personal or household" activity for the purposes of the second indent of Article 3(2) of Directive 95/46.[20]

However, the CJEU also pointed out that the applicability of data protection law does not mean that such activities (i.e. CCTV around one's home) are disallowed, as there are certain mechanisms provided by law whereby data controllers may possibly justify the collection and use of personal data through those activities.[21]

The more recent judgment of *Tietosuojavaltuutettu v Jehovan todistajat* (Case C-25/17) upholds the criteria set out in the previous cases. In this case, the CJEU considered whether the collection of personal data by members of the Jehovah's Witness Community constituted a purely personal or household activity within the meaning of Article 3(2) of Directive 95/46. Here, the facts concerned collecting personal data through door-to-door preaching of households. The CJEU held that:

> …an activity cannot be regarded as being purely personal or domestic where its purpose is to make the data collected accessible to an unrestricted number of people or where that activity extends, even partially, to a public space and is

> accordingly directed outwards from the private setting of the person processing the data in that manner […].
>
> …door-to-door preaching, in the course of the which personal data are collected […] is, by its very nature, intended to spread the faith of the Jehovah's Witness Community among people who […] do not belong to the faith of the members who engage in preaching. Therefore, that activity is directed outwards from the private setting of the members who engage in preaching.[22]

What we gather from these three cases is that the household exemption, both under the old Data Protection Directive and now the GDPR, is narrowly construed. Namely, only those activities which are *purely* personal or within a household may be exempt from the reach of the law. The GDPR has provided two examples of such activities: 1) correspondence and the holding of addresses (e.g. writing emails and maintaining an address book), or 2) social networking and online activity undertaken within the context of such activities (e.g. Facebook chat and postings within one's social network). It is also made clear that any connection to a commercial or professional activity would preclude the activity in question from being purely personal or household.[23]

The use of personal data for health research by citizen scientists is clearly not covered by the two examples provided by the GDPR, but it does not necessarily involve any commercial or professional interest, either. This means that the nature of such research activities and whether they can benefit from the household exemption are at least open to question. Provided that mobile devices monitor the health conditions only of the citizen scientists themselves and/or family members, and provided that such data are accessible only *within* the family and not transmitted to a third party or external device or processor (as otherwise the use of data will essentially break out into the "public space" and thus lose its "purely personal or household" nature), it would be plausible to argue for the exemption for such activities. As a Council of Europe handbook on data protection law observes, context matters in determining whether the household exemption applies:

> Citizens' access to the internet and the possibility to use e-commerce platforms, social networks and blogging sites to share personal information about themselves and other individuals make it increasingly difficult to separate personal from non-personal processing. Whether activities are purely personal or household depends on the circumstances. Activities that have professional or commercial aspects cannot fall under the household exemption.[24]

In the case of "self-experimenters," i.e. individuals who gather personal data about their own health and biometric measurements and then voluntarily attempt to experiment in some way to alter their health, it seems likely this activity would fall within the household exemption, provided these self-experimenters used or disclosed their own data or findings to only a small number of individuals (e.g. a small social network of fellow self-experimenters). As the Council of Europe handbook states: "An individual who keeps his or her correspondence, a personal diary describing incidents with friends and colleagues *and health records of family members*, may be exempt from data protection rules, as these activities could be purely personal or merely household activities."[25] But as the same handbook goes on to note: "…another factor that must be taken into account is whether personal data are made available to a large number of persons, obviously external to the private sphere of the individual."[26] We know, based on the case law discussed above, that the household exemption will not extend to the publication of personal data to an unlimited number of recipients on the internet, as opposed to say, a small social network that is available to members only. In this scenario, the household exemption will therefore likely apply where individuals have performed an

experiment and in the course of doing so (including before and after the experimentation), process personal data and disseminate it to a small number of persons. However, were the "self-experimenter" to disseminate their personal data to large number of persons; post personal data about other individuals; commercialize the findings in some way, such as selling results or holding him- or herself out for hire for guinea-pig testing; or otherwise undertake self-experimentations as a full-time activity, then it seems more likely that the household exemption would disapply.

It should also be pointed out that that just because the self-experimenter is the data subject, or one of the data subjects, does not mean that they cannot be a (joint) data controller at the same time. At the time of the 1995 Data Protection Directive, there were discussions about social media users as data controllers jointly with the platform.[27] Although much of the legal uncertainty in this context has been dispelled by GDPR Recital 18 ("[p]ersonal or household activities could include […] social networking […]"), there is no doctrinal reason why a data subject cannot be a data controller at the same time. In fact, the idea of "data subjects as data controllers" has recently been subject to further debates amid a number of CJEU cases,[28] but further research is needed to clarify such a possibility in a setting of citizen science.

Considering the CJEU's consistently narrow interpretation of the household exemption in existing case law, other forms of citizen scientist-led research are unlikely to be exempted if they are challenged in legal proceedings. For example, collecting and analyzing behavioral data from smartphones, even only within a group of citizen scientists or a limited number of pilot users, can hardly be exempted as purely personal or domestic. This interpretation is in line with the Court's reasoning that allowing such activities to fall outside the scope of data protection law would place individuals under serious data protection risks if the citizen scientists do not use such data with reasonable care.

Thus, in our view, while the GDPR has not expressly precluded the possibility of relying on the household exemption, it would be difficult for citizen scientists to make such a case for their health research that processes health data using mobile devices beyond their own or their family members'.

Lawful bases for processing personal data

Having considered that the GDPR likely applies to most forms of citizen-scientist led health research with mobile devices (assuming either the citizen scientist and/or the users are based in the EU), we must now turn to consider which lawful bases might be appropriate to process personal data. It is a principle under EU data protection law that processing of personal data is generally prohibited unless it is based on one of the legal grounds explicitly afforded by law. This is particularly the case for certain special categories of data (i.e. "sensitive data"), including health-related data, which is the data type most likely to apply in this specific context.[29] It should be noted that a number of legal bases applicable to personal data of general nature ("non-sensitive data"), such as "performance of a contract" or "legitimate interests" of the data controller,[30] cannot sufficiently legitimize the collection and use of sensitive data. Since health data are undoubtedly sensitive data, this section of our article will only look into the legal grounds applicable to sensitive data.

In the context of mobile device-driven health research carried out by citizen scientists, the following legal bases for processing sensitive data can be considered:

- vital interests;
- provision of health and social care;

- public health;
- explicit consent; and
- scientific research purposes.

We assess the strength of each of these lawful bases below.

Vital interests. Under Article 9(2)(c), sensitive personal data may be processed if it is "necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent." Despite the possibly valid argument that certain citizen science health research projects may concern the vital interests of individuals, especially those involving the development of treatment or medication for rare diseases, it is unlikely this legal ground can be invoked to justify the processing of health data. For one thing, Article 9(2)(c) sets out a strict condition that this is applicable only when "the data subject is physically or legally incapable of giving consent." For another thing, the "vital" test requires an exceptional level of urgency, such as "monitoring epidemics and their spread or in situations of humanitarian emergencies" (Recital 46) or threats to "physical integrity or life" (Recital 112). In the absences of these elements, vital interests of the data subject or another personal are generally inapplicable as a legal ground.

Provision of health and social care. Under Article 9(2)(h), sensitive personal data may be processed if it is:

> …necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3 [in Article 9].

Paragraph 3 speaks to a person being subject to an obligation of secrecy under EU or Member State law or rules established by national competent bodies. While research carried out by citizen scientists may benefit from the provision of health and social care, this does not mean that the use of sensitive data is automatically justified. The conditions laid down by Article 9(2)(h) are rather stringent, requiring: a) a legal basis either provided by EU or Member State law, or by a health service contract; and b) such processing being subject to an obligation of secrecy as stipulated by law or regulation. Without such safeguards, the reliance on this provision would not be valid.

Public health. Under Article 9(2)(i), sensitive personal data may be processed if it is:

> …necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.

For the same reasons as above, public health is also unlikely to be a suitable lawful basis in the citizen science context. The applicability of the public health lawful basis depends on an existing legal basis provided by EU or Member State law, as well as the safeguards of legally stipulated professional (or other) secrecy.

Explicit consent. Under Article 9(2)(a), sensitive personal data may be processed if "the data subject has given explicit consent to the processing of those personal data for one or more specified

purposes, except where Union or Member State law provide that the prohibition [of processing sensitive data] may not be lifted by the data subject." At first glance, explicit consent seems to be the safest, if not the only, choice for citizen scientists with regard to mobile device-driven health research carried out using sensitive personal data. However, it should be noted that there are further complications regarding this ground. First, the provision specifically allows Member States to restrict the types of processing of sensitive data to which data subjects may consent. Second, Article 9(4) also allows Member States to introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.[31] Thus, while citizen scientists may be in a good position to obtain the explicit consent from users of mobile devices and who wish to participate in a research project, they must be mindful of national laws that may restrict either consent or processing of health-related data.

Scientific research. Finally, under Article 9(2)(i), sensitive personal data may be processed if it is

> …necessary for […] scientific […] research purposes […] in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

This is also a more promising lawful basis. However, it requires a basis in EU or Member State law. These laws may further stipulate that health research have research ethics committee approval.[32] This can pose a problem to citizen scientists, as unlike institutional researchers, they may lack a support structure that enables them to apply for and obtain research ethics approval, as well as helping them determine which ethics committee(s) to apply to for assessment and approval.

Thus, most of the legal grounds provided by Article 9(1) are difficult to apply to the case of citizen scientist-led health research. The scientific research purpose provision at Article 9(2)(i) may be a possible route, but it would require authorization under EU or Member State law and may not be very helpful in the international research context where personal data are exported from the EU to third countries, such as the United States. The most practical basis would therefore seem to be the explicit consent basis at Article 9(2)(a), but due to the potential fragmentation of law across Member States (despite the GDPR's desire to harmonize data protection law across Europe), even robustly obtained consent may suffer a high risk of legal uncertainty.[33]

However, not all hope is lost. We now proceed to explore a provision in the GDPR which may prove to be a boon for citizen scientists and others wishing to undertake health research.

Compatible use

While collecting sensitive data for health research purposes can be a complex legal process in the EU, once the data have been lawfully collected for a primary purpose – which does not have to be related to health research – it should be much more straightforward for citizen scientists to *reuse* such data for research purposes. This is because GDPR Article 5(1)(b) – which states the data protection principle of purpose limitation – expressly recognizes the compatibility of scientific research as a secondary purpose, as long as the conditions set out in Article 89(1) are met.[34] This means that even if personal data were collected for a different purpose, further processing of such data by the same data controller (i.e. citizen scientist) for research purposes will be considered compatible,[35] and therefore will not require a separate legal basis.[36] Accordingly, for citizen scientists to rely on this principle to reuse pre-collected health data, three conditions must be fulfilled:

1. The data concerned must have been lawfully collected in the first place.
2. The processing must and must only serve the sole purpose of research. The GDPR acknowledges a broad definition of "scientific research,"[37] including privately funded research, and there is no compelling reason to not accept citizen scientist-led research as a valid form of "scientific research."
3. Such processing must be in line with the requirements laid down by Article 89(1), in particular with appropriate safeguards to ensure compliance with the principle of data minimization.[38] It should be noted that, unlike Article 9(2)(i) analyzed above, neither Article 5(1)(b) nor Article 89(1) requires EU or Member State law to provide a legal basis. It follows then that where citizen scientists (as opposed to institutional researchers) have difficulty relying on Article 9(2)(i), they should be able to process already lawfully collected data for the *secondary purpose* of scientific research.

In this regard, research activities carried out by citizen scientists are to some extent privileged under the GDPR, especially with regard to reusing lawfully collected data. Compared to institutional scientists, however, primary collection and use of health data with mobile devices remain legally challenging for citizen scientists.

Conclusion and policy implications

In this article, we explored whether the GDPR applies to citizen scientist-led health research with mobile devices. The analysis above shows that, depending on the territorial scope, citizen scientist-led health research with mobile devices *is* likely to be covered by the GDPR. The GDPR's household exemption is unlikely to apply unless the activities are *solely* "personal or household," which would mean using mobile devices that process data only within the confines of the individual or their family members, and no personal data are transferred to third parties. Consequently, for citizen scientists to process health data collected by mobile devices, they would likely need to obtain explicit consent from data subjects, rely on the scientific research provision, or rely on the authorization provided under the purpose limitation principle with regard to scientific research.

Despite the special provisions governing the use of personal data in the area of scientific research, the GDPR largely remains a one-size-fits-all, omnibus legal instrument. This provides benefit in terms of greater overall legal certainty for various stakeholders – including data subjects – but as a drawback, it may not offer sufficient granularity to deal adequately with the highly heterogeneous real-life scenarios in different contexts. In the case of health research, the GDPR does not differentiate institutional researchers and independent researchers (we are agonistic as to whether it should), although it leaves some room for Member State laws to step in and lay down more specific rules – and this is arguably a negative as it goes against the concerted drive for harmonization of data protection law.

As a result, citizen scientists may find the GDPR both too strict and too lax. On the one hand, obtaining a legal basis under Article 9(2) other than explicit consent may be a challenge. On the other hand, once a data controller has lawfully collected sensitive data for a different purpose, they can reuse such data for the loosely defined purpose of "scientific research," which could be exploited by not just citizen scientists, but also pharmaceutical companies.

The implication for policymakers, whether in Europe or elsewhere, is that in the area of health research, there may be a need for a *lex specialis* to handle the issue regarding the processing of health data for research purposes (including by non-traditional researchers), which involves both a sophisticated coverage of distinct circumstances and the complicated balance among various

interests. To this end, we are encouraged by the work undertaken by the Biobanking and BioMolecular resources Research Infrastructure-European Research Infrastructure Consortium (BBMRI-ERIC), a European-based distributed research infrastructure, which is currently developing a "Code of Conduct for Health Research," in line with GDPR Article 40.[39] Such efforts may mark an opportunity to develop a set of standards to provide greater clarity and certainty regarding the legal obligations of citizen scientists to protect the privacy interests of those whose data they process using mobile devices for health research purposes.

Acknowledgements

Special thanks to the organizers of the "Addressing ELSI Issues in Unregulated Health Research Using Mobile Devices Working Group Meeting #3," held in October 2018 in Atlanta, Georgia, at which a version of this article was presented. Jiahong Chen is supported by the EPSRC grant "From Human Data to Personal Experience" (EP/M02315X/1).

References

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [hereinafter GDPR].
2. See generally Dove, E.S., "The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era," Journal of Law, Medicine & Ethics 46, no. 4 (2018): 1013-1030.
3. Such as GDPR, Arts. 5(1)(b) & (e), 9(2)(j), 14(5)(b), 17(3)(d) and 21(6).
4. Guerrini, C. J. et al., "Citizen Science, Public Policy," Science 361, no. 6398 (2018): 134-136.
5. Rothstein, M. A., Wilbanks, J. T., and Brothers, K. B., "Citizen Science on Your Smartphone: An ELSI Research Agenda: Currents in Contemporary Bioethics," Journal of Law, Medicine & Ethics 43, no. 4 (2015): 897-903.
6. Den Broeder, L. et al., "Citizen Science for Public Health," Health Promotion International 33, no. 3 (2016): 505-514.
7. Hoffman, S., "Citizen Science: The Law and Ethics of Public Access to Medical Big Data," Berkeley Technology Law Journal 30, no. 3 (2015): 1741-1805.
8. GDPR, Recital 35.
9. *Id*.
10. GDPR, Recital 26. See also *Patrick Breyer v Bundesrepublik Deutschland* (CJEU, Case C-582/14), paras. 42-48.
11. Culnane, C., Rubinstein, B. I., and Teague, V., "Health Data in an Open World," *arXiv preprint* (2017), *available at* <https://arxiv.org/abs/1712.05627>; Rocher, L., Hendrickx, J. M., and de Montjoye, Y. A., "Estimating the Success of Re-identifications in Incomplete Datasets Using Generative Models," Nature Communications 10, no. 1 (2019): 3069 (1-9).
12. GDPR, Art. 4(5).
13. GDPR, Recital 28.
14. GDPR, Art. 6(4).
15. GDPR, Art. 25(1).
16. GDPR, Art. 32(1).

17. GDPR, Art. 89(1): "Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards […] Those measures may include pseudonymisation […]."
18. Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer, 2017), p. 16.
19. *Bodil Lindqvist v Åklagarkammaren i Jönköping* (CJEU, Case C-101/01) para. 47 (emphasis added).
20. *František Ryneš v Úřad pro ochranu osobních údajů* (CJEU, Case C-212/13) paras. 29-30, 33 (emphasis added).
21. *Ryneš*, para. 34.
22. *Tietosuojavaltuutettu v Jehovan todistajat* (CJEU, Case C-25/17), paras. 42, 44-45.
23. GDPR, Recital 18.
24. European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law: 2018 edition* (FRA and CoE, 2018), p. 103.
25. *Id*, p. 102.
26. *Id*, p. 103.
27. Wong, R., "Social Networking: Anybody is a Data Controller," (2008) *available at* <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1271668>; Van Alsenoy, B. et al., "Social Networks and Web 2.0: Are Users Also Bound by Data Protection Regulations?" Identity in the Information Society 2, no. 1 (2009): 65-79.
28. Edwards, L., "Data Subjects as Data Controllers: A Fashion(able) Concept?" (2019) *available at* <https://policyreview.info/articles/news/data-subjects-data-controllers-fashionable-concept/1400>.
29. GDPR, Art. 9(1).
30. GDPR, Art. 6(1).
31. GDPR, Art. 9(4).
32. See e.g. the UK's Data Protection Act 2018 ss. 19(3) and 19(4)(a). The DPA 2018 requires that processing of personal data that is necessary for scientific research purposes that relates to measures or decisions with respect to a *particular* data subject is forbidden unless it is "approved medical research," by which is meant medical research carried out by a person who has approval to carry out that research from a recognized research ethics committee.
33. Timmers, M. et al., "Will the EU Data Protection Regulation 2016/679 Inhibit Critical Care Research?" Medical Law Review 27, no. 1 (2018): 59-78.
34. GDPR, Art. 5(1)(b): "[…] further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes […]."
35. Pormeister, K., "Genetic Data and the Research Exemption: Is the GDPR Going Too Far?" International Data Privacy Law 7, no. 2 (2017): 137-146; Shabani, M., and Borry, P., "Rules for Processing Genetic Data for Research Purposes in View of the New EU General Data Protection Regulation," European Journal of Human Genetics 26, no. 2 (2018): 149-156.
36. GDPR, Recital 50.
37. GDPR, Recital 159.
38. GDPR, Art. 89(1): "[…] Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. […]"
39. See Code of Conduct for Health Research, *available at* <http://code-of-conduct-for-health-research.eu>.