Why We Trust Dynamic Consent to Deliver on Privacy

Arianna Schuler Scott, Michael Goldsmith, Harriet Teare, Helena Webb, Sadie Creese

Why We Trust Dynamic Consent to Deliver on Privacy.

Arianna Schuler Scott[1] [0000-0001-6565-8266], Michael Goldsmith[1], Harriet Teare[2], Helena Webb[1] and Sadie Creese[1].

[1] Department of Computer Science, University of Oxford, Oxford, UK
[2] Centre for Health, Law and Emerging Technologies, University of Oxford, Oxford, UK
arianna.schulerscott@cs.ox.ac.uk

Abstract. Dynamic consent has been discussed in theory as a way to show user preferences being taken into account when data is accessed and shared for research purposes. The mechanism is grounded in principles of revocation and engagement – participants may withdraw or edit their permissions at any time, and they receive feedback on the project they are contributing to if they have chosen to do so. The level of granular control offered by dynamic consent means that individuals have informational control over what they are sharing with the study, and to what extent that data can be used further. Rather than attempt to redefine privacy, this paper takes the position that data controllers have certain obligations to protect a data subject's information and must show trustworthy behaviour to encourage research participation. Our model of privacy is grounded in normative, transaction-based requirements. We argue that dynamic consent is a mechanism that offers data controllers a way to evidence compliance with individual privacy preferences, and data subjects with control as and when they require it. The key difference between dynamic consent and a "rich" database consisting of a dataset with the ability for a subject to revoke access is human engagement, or relations of trust. We must re-think how consent is implemented from the top-down (policy-based) and bottom up (technical architecture) to develop useful privacy controls.

Keywords: dynamic consent, privacy, trustworthiness, engagement, revocation.

1 Introduction

Giving consent for a research study to make use of personal information is widely considered to be a personal and individual choice. Historically, consent procedures were meant to prevent physical harm to participants caused by unethical medical research [1]. The degree to which the choice to participate is a free one, given societal obligations and personal motivation varies depending on the study and context in which it is being done [2] but it is generally accepted that researchers are trusted to have ethical oversight of their work and are required to be able to prove that human participants elected to take part. Societal expectations around research such as to advance thinking in expert areas, provide solutions and contribute to the betterment of society, create individual expectations which contribute to an individual's motivation to take part. They generally wish to contribute and choose what their information is used for, opting

to delegate implementation to those with relevant expertise – namely, researchers [3]. There has been work done to explore the concept of "trustworthiness" where experts must demonstrate behaviour/s that justify this inherent trust in research to invite and encourage participation.

This shift towards two-way, transactional knowledge development draws parallels with some of the conceptual development around privacy, especially in medical research. In "Rethinking Informed Consent in Bioethics" [4] the authors discuss privacy as normative, grounded in how information is communicated rather than what is communicated. General privacy rules fall short, they argue, because these rules are too vague. Trying to define "data acquisition" in general as a privacy violation is too broad as there are legitimate reasons for wanting to gather data. Instead, the authors focus on narrower definitions where the means of acquisition are problematic rather than the kind of data being collected - acquiring information through intrusive or impermissible action results in violation. Technology increases the amount of information that can be put together about an individual, and be used for good or ill. Rather than simply trying to increase general trust levels, O'Neill argues that it is the placement of trust (or mistrust) that is key [5]. For individuals to place trust, institutions must show trustworthiness, or consent decisions will be made based on the lack of it. Being specific about what an individual consents to, allows controllers to be more specific as to what constitutes a violation.

This paper makes the claim that a dynamic form of consent goes some way to meeting the requirements put forward by a normative, transactional privacy model. We do not make the claim that informed consent can be used as a way for an individual to control information as this dives into a conversation that we will later address, on contemporary positions as to why current implementations of consent cannot be used to protect data (for an excellent discussion on this, see [6]). Data holds value and we discuss data protection obligations held by those who collect, store, control, use and share personal data in a research context. The term "personal information" includes: data gathered directly from someone such as name and medical history, the meaning drawn from these attributes, and inferences that can be made as part of the wider research process. Such an overwhelming amount of information can be difficult to access, to parse and to make informed decisions about and while accounts differ as to whether individuals want that level of control, institutions ultimately have legal obligations and business interests (such as not being fined) to consider.

2 Literature

Consent is a mechanism for protecting an individual's rights within research [7] and consent decisions must have the potential to change over time, simply because people are prone to changing their minds. A dynamic choice is more representative. There are areas of concern regarding informed consent: people's choices can be coerced, especially where there is a power imbalance, (online for example, where they may be forced to agree to data-sharing in order to access a service) and they often do now know the options available to them (due to obscure privacy policies and an overwhelming amount of information being presented). Even if these problems did not exist then the issue

remains as to how much control data subjects actually exercise. This can be unclear due to differences between business and user requirements that often cannot be bridged [8]. Solutions exist - promoting informed consent has been shown to reduce decisional conflict and increase perceived knowledge and understanding [9], and focusing on "genuine" (rather than wholly informed consent) where individual control over permissible actions for a data controller to take, and the amount of information received from that controller [10] are the priority.

There are two significant cases where trust collapsed due to poor consent management and engagement with the public in a medical context: the scandal at Alder Hey Children's Hospital and the case of NHS England's Care.data project. Alder Hey Children's hospital did not ask parents of deceased children whether their child's organs could be used for research purposes before collecting tissue. Interestingly, it was not that the organs were used that constituted a violation, it was that parents were not asked beforehand. While medical professionals may have been guided throughout their training and careers to protect patients from hard news or difficult decisions, this case signals a shift from paternalism to more inclusive practice. While post-mortems may be carried out without parents' consent, hundreds of organs were kept for years after death which meant unfettered access to samples that were unethically procured. On the recommendations of an independent enquiry, The Human Tissue Act was established in 2004 to mandate how organs were to be used for research purposes, and an oversight committee was established: the Human Tissue Authority [11].

Care.data was not so retrospective, the project simply broke down. England's National Health Service (NHS England) wanted to implement a national database for medical records that crossed primary and secondary care. Despite the obvious benefits centralizing this kind of information might result in, the overall rollout strategy did not prioritise communication with the Great British Public. The scheme was opt-out by default which made people feel as if the decision had already been made for them, and there were no doctors or public-facing experts who could field questions or convince the public that the initiative was in any way trustworthy. Public trust in NHS England plummeted and a project that could have provided valuable services to many people was dropped. The national data guardian produced a report after the fact where she suggested that a more thought-out communication strategy and dynamic consent/opt-out procedure may have resulted in a more receptive response [12], [13].

2.1 Dynamic Consent

The "dynamics" of dynamic consent consist of: enabling individuals to give and revoke consent to the use of their samples, centralizing all transactions and interactions, allowing individuals to be approached for different projects or their feedback on emergent ethical considerations, and letting consent preferences be modified over time [18].

Dynamic consent, built on the principles of revocation and engagement, was created to address problems with one-time, broad consent. The most significant issue with broad consent is that it is not informed, due to only asking the participant once for their consent and delegating future decisions to an unseen "expert". Developed to build trust and improve participant recruitment and participation over time [14], dynamic consent

builds on work done by the Ensuring Consent and Revocation (EnCoRe) project that aimed "to make giving consent as reliable and easy as turning on a tap, and revoking that consent as reliable and easy as turning it off again" [15].

Allowing people to revoke consent for data-use is one of the two underlying concepts of this model. Engaging in communication around data-use is the other. Arguments against dynamic consent decry the expense generated having to design revocation and engagement into research practice at an early stage. Granted, it may be the case that new procedures may need to be adopted, or the relationship between researcher and participant reconsidered [16] but dynamic consent improves trust in how electronic records are used because control is passed to the participant. If information has been shared without authorisation or sold then trust is lost, and when this happens then data is less likely to be shared [17] and research relies on data.

2.2 Trustworthiness

People can show trust in an institution despite a lack of trustworthy behaviour (such as transparency [18]) that they claim should be the norm. We make this point because it is pertinent that people do not have the option to behave in the way they would like to due to a lack of institutional support. Further discussion on institutional expectation lies outside the scope of this paper.

We make the distinction here between trustworthiness (shown by a data controller) and trust (given by a data subject). The fact that people are willing to entrust their data to researchers in the absence of trustworthy practice, as shown in the Alder Hey example, is significant because it strengthens the idea of a social contract between science and society. Data is derived from the public, so it must benefit them [19]. This social contract means that scientific improvement must meet the needs of the public [20], needs which can be collected and formalised using dynamic consent [21].

Privacy gives people the opportunity to negotiate how others access or use their information, and the attitude towards these "others" is influenced by the level of trust in them. There is a level of trust in research institutions that is strong enough for individuals to feel comfortable delegating decisions about unknown, broad uses of their personal data. As long as data is handled correctly, consent is revocable and studies are ethically approved [22] then broad consent is acceptable. Trust is fundamental for broad consent to be an option. Researchers are assumed to be trustworthy or have trustworthy infrastructure in place such as ethics review boards, so research participants can trust them with their consent decisions.

2.3 Privacy

Privacy is often associated with notions of self-identity [23] and individuals have been shown to want control over personal information and the decisions they make pertaining to that data [24]. There has been interesting discussion framing privacy as the freedom of an individual to make decisions that let them shape who they are [25]. In this case, the author's criticism of many privacy discussions is that while information controls are often discussed, more attention needs to be given to underlying philosophical

and ethical foundations, as well as the information itself that's being controlled. In terms of research data-use, asking "which data are being used, and for what purposes" might begin to address this.

While discussing information under control, a significant area of research to mention is the development of contextual integrity, where information flows provide privacy (my doctor sends medical information to another consultant) and their breakdown constitutes a violation (my doctor sends medical information to a non-medical party) [26]. This normative stance on privacy has directly influenced the approach this paper has taken towards data-use.

3 Results

In this section we present a privacy model that compares acceptable and unacceptable scenarios given normative privacy modelling around data-sharing for research use, and an initial specification for dynamic consent as it might be implemented as part of a research project. This is novel in that we do not have any way to measure whether or not an implementation of dynamic consent is achieving what the literature positions it to do. What we find is that the unacceptable scenarios could be mitigated by incorporating dynamic consent into the research process at the design stage.

For example, just knowing what individual preferences are in terms of who data can be shared with could be used as a filter when exporting data or creating reports that are to be shared, as the EnCoRe project was able to demonstrate. We suggest that the following serve as indicators of conceptual evidence for the use of dynamic consent by data controllers as a privacy mechanism.

3.1 Privacy Model

The key sources used to build the comparisons in table 1 were the General Data Protection Regulation (GDPR) [27] and Onora O'Neill's "Rethinking Informed Consent in Bioethics" [4]. The former provides obligations that data controllers must meet, while the latter provided a normative approach to what privacy violations could look like and how those might be avoided through developing a consent process that asks an individual for their preferences when they are recruited and allows them to change their mind.

In the case where an individual is asked about sharing their data with a third party for example, these preferences must have some level of granularity as this overarching question can be broken down further. Options may include sharing data with a third party for research use, sharing data with a third party for any purpose, and "ask me before you share my data with a third party for any reason".

In table 1, while the placement of most statements will appear obvious, the fourth row may appear untenable to some readers. "Data is shared with explicit consent to do so" is placed under "Unacceptable" because the point of this system is not to overload the data subject with every single request for their data.

Table 1. Normative privacy in the context of research.

Acceptable	Unacceptable
Data is processed for the purposes stated with consent (of any kind) to share data for stated purposes.	Data is processed for the purposes stated without consent (of any kind) to share data for stated purposes.
Data is processed for unstated research purposes, with consent to only share for research purposes.	Data is processed for unstated research purposes, without consent to share for other research purposes.
Data is processed for commercial purposes, with consent to share for commercial purposes.	Data is processed for commercial purposes, without consent to share for commercial purposes.
Data is shared without explicit consent.	Data is shared with explicit consent to do so.
Second-order enforcement of consent means that secondary use is possible because this was indicated at the time of consent.	Second-order enforcement of consent is not carried out as data is used and consent was not originally given.
Second-order enforcement of consent means that secondary use is possible because this was indicated after the original consent.	Second-order enforcement of consent is not carried out as data is used and consent was not given at any point.

3.2 Dynamic Consent Specification

The following (table 2) has been constructed from existing literature on dynamic consent (basic principles [21, 16], trust-building [17], interface design [29], biobank consent methods [3, 28]) and inclusive approaches to engagement (reciprocity [30, 31], awareness [32, 33] and trust [34]). This specification is currently a list of design and implementation prompts aimed at encouraging thought around data-use at the start of a research project that will make use of personal data.

Table 2. Prompts for incorporating dynamic consent and building trustworthiness into the research process.

Included	Design prompt	Implementation
☐	Will dynamic consent impact participant recruitment?	☐ Standardised recruitment ☐ No geographical limitations ☐ Process entirely/partly online ☐ Other
☐	Will dynamic consent impact how informed consent is collected?	☐ Various info. formats ☐ Record is viewable online ☐ Process can be entirely/partly online ☐ Communication options set ☐ Other
☐	Will dynamic consent impact consent management?	☐ Electronic authorisation ☐ Standardised access to preferences ☐ Secure storage/access ☐ Revocation options available ☐ Other
☐	Will dynamic consent impact participant retention?	☐ Online forums ☐ Feedback is delivered online ☐ Data can be collected online ☐ Other
☐	Is dynamic consent going to save resources?	☐ Money ☐ Time ☐ Other
☐	What does the researcher/participant relationship look like?	☐ Is this a culture change? ☐ Participants feed into process ☐ Other
☐	Who do you have buy-in from (who gains from/supports the project)?	☐ Researchers ☐ Clinicians ☐ Public services ☐ Other
☐	How will you feed back to participants?	☐ Regularly/occasionally/when prompted ☐ Using a method they have specified ☐ Other
☐	What will you feed back to participants?	☐ Information about the research process ☐ Where their data is used ☐ Who their data has been used by ☐ Parties data is shared with ☐ Other

4 Discussion

Dynamic consent is a model resting on participant engagement and the facilitation of data, participation and consent revocation if necessary. Rather than protecting privacy as an abstract concept, this protects tangible privacy interests. Individuals need to be given the option to say no and this option needs to be communicated. There need to be options that allow data-sharing as well as options to share sharing privileges. Data subjects may want a flexible level of participation and it is the controller's responsibility to check-in (and keep checking in, especially in the case of longitudinal studies) to gauge understanding of the study, which could also indicate whether understandings are shared between controller and subject. One concern with recent data protection legislation is the level of ambiguity around implementation. Establishing transparent and relevant policy is important, but to be able to communicate and measure those rules institutionally would be invaluable when providing an audit trail, for example.

Consent provides assurance about what data is used for and why, but it has not been helpful as an information control. This is largely due to it being considered n obstacle, particularly in research where ethical oversight can delay or otherwise impact research. Rather than talk about controlling data, proponents of contextual integrity aspire to control flows of data, the contexts in which those flows act, and what happens when data crosses contexts it is not meant to. This "socialised" construct can direct technical implementation - dynamic consent could support the flow of new knowledge between the laboratory and the clinic, central to translational research and personalised medicine [21]. Consent was not designed to work as an assurance in every possible case. It can be unclear at the point of initial consent as to what exactly data might be used for and individual preferences should be direct future action. This thinking is in a similar vein as EnCoRe's development of consent preferences as filters for automated data-use [15].

Informed consent was established to prevent harm, specifically research consequences which are identifiable as they are physical or otherwise obvious. In terms of data-use, it is much harder to know what information could be used for and the impact, or impacts, this might have. Bad consent practice is demonstrated online through cookies that coerce data-donation, privacy policy obfuscation, and designs that actively draw attention away from options that inhibit data-sharing. Research involving human beings makes heavy use of consent and this is especially the case in medical research. Consent can be used as a basis for data-processing as enshrined in recent data-protection legislation like GDPR, but so can contracts, legal obligation, vital interests, public contribution or "legitimate interests". Cases in which consent might not be required might mean that anonymised datasets can be used, but individuals still express a preference for ultimate control even when publicly accessible data about them is used.

This paper models privacy as the "how" rather than the "what", focusing on safeguarding interests rather than specific pieces of information. Dynamic consent originated in the context of bio-banking where those who donate tissue may wish to delegate consent to an oversight panel or retain ultimate control over who uses what and when. In a similar vein, individuals must also make their own risk calculations when sharing personal data. As different people have different risk levels, the way in which these preferences are going to be collected must take these differences into account. This does

not exclude automation – preferences should be able to be translated as rules that are checked before data is transmitted or put to use. Privacy is a moral and social issue, as is consent. A key driver behind why people should have a say is because organisations are obliged to give them one. As society tends towards inclusivity and away from paternalism in research, there is still considerable trust in experts to make decisions in the best interests of data subjects. These subjects want a say but also want to leave the details to those who know better.

5 Conclusion

Rather than trying to re-word consent forms or privacy policies the position of this paper is that an overhaul is needed. By claiming that dynamic consent can be used as a privacy control, we mean that it can be used by data subjects to manage how they share information and the extent to which those details can be shared further, and by data controllers to provide evidence that they are complying with individual consent preferences. This, by extension, provides evidence of compliance with data-protection regulations like the GDPR and the Data Protection Act.

While there are persuasive arguments as to why consent in its current form has no place in conversations around privacy, these arguments are largely grounded in two assumptions: that privacy is a social construct and that there is an ideal version of informed consent that current implementations will eventually become through various modifications. We address these concerns through two things. The first, by modelling privacy as the "how" rather than the "what", rather than focusing on which data are shared (or not) we explore how privacy interests can be safeguarded. The second is that our approach to consent is that there is no single solution, it must be flexible and allow the participant to indicate their preference or preferences for the data controller to act on accordingly.

To conclude, there are few cases in which user preferences are not sought at all regarding data-use. They may be coerced, obfuscated or hidden but they are there. Consent is a central tenet of research and needs developing as technology improves and the way we think about data changes. Dynamic consent provides an updated model for privacy control and rather than exclaim "Death to Consent!", it is our intention to demonstrate that given the very real concerns around data ownership in the digital age we find ourselves in, current practices are unfit for purpose and the need to re-think consent as a privacy control is very much alive.

6 Future work

This is part of a work in progress, there is a clear need for empirical work that looks at whether projects that are actually implementing dynamic consent match up to the academic claims made by the literature.

References

1. Rickham, P.: Human experimentation. Code of ethics of the world medical association. Declaration of Helsinki. British Medical Journal 2, (1964).
2. Barreteau, O., Bots, P., Daniell, K.: A framework for clarifying participation in participatory research to prevent its rejection for the wrong reasons. Ecology and Society 15(2), 1-22 (2010).
3. Whitley, E., Kanellopoulou, N., Kaye, J.: Consent and research governance in biobanks: evidence from focus groups with medical researchers. Public Health Genomics 15(5), 232–242 (2012).
4. Manson, N., O'Neill, O.: Rethinking informed consent in bioethics. Cambridge University Press, (2007).
5. O'Neill, O., Bardrick, J.: Trust, trustworthiness and transparency. Brussels: European Foundation Centre, (2015).
6. Nissenbaum, H.: (Interview) Stop Thinking About Consent: It Isn't Possible And It Isn't Right. URL: https://hbr.org/2018/09/stop-thinking-about-consent-it-isnt-possible-and-it-isnt-right. Accessed: 25-Sep-2018.
7. Boulton, M., Parker, M.: Informed consent in a changing environment. Social Science and Medicine 65(11), 2187-2198 (2007).
8. Whitley, E., Kanellopoulou, N.: Privacy and informed consent in online interactions: Evidence from expert focus groups. In: International Conference on Information Systems, Missouri, (2010).
9. Kinnersley, P., Phillips, K., Savage, K., Kelly, M. J., Farrell, E., Morgan, B., Whistance, R., Lewis, V., Mann, M. K., Stephens, B. L., Blazeby, J., Elwyn, G., Edwards, A. G. K.: Interventions to promote informed consent for patients undergoing surgical and other invasive healthcare procedures. Cochrane Database of Systematic Reviews 7, (2013).
10. O'Neill, O.: Some limits of informed consent. Journal of Medical Ethics 29, 4–7 (2003).
11. Hall, D.: Reflecting on Redfern: What can we learn from the Alder Hey story?. Archives of Disease in Childhood 84(6), 455–456 (2001).
12. Limb, M.: Controversial database of medical records is scrapped over security concerns. British Medical Journal Online 354, (2016).
13. Godlee, F.: (Editor's Choice) What can we salvage from care.data?. British Medical Journal, (2016).
14. Schuler Scott, A., Goldsmith, M., Teare, H.: Wider Research Applications of Dynamic Consent. In: Kosta, E., Pierson, J., Slamanig, D., Fischer-Hübner, S., Krenn, S. (eds.) PRIVACY AND IDENTITY MANAGEMENT. FAIRNESS, ACCOUNTABILITY, AND TRANSPARENCY IN THE AGE OF BIG DATA 2018, pp. 114-120. Springer International Publishing (2019).
15. EnCoRe: EnCoRe - Ensuring Consent and Revocation, http://www.hpl.hp.com/breweb/encore-project/index.html, last accessed 2018/07/03. (2008).
16. Budin-Ljøsne, I., Teare, H., Kaye, J., Beck, S., Bentzen, H. B., Caenazzo, L., Collett, C., D'Abramo, F., Felzmann, H., Finlay, T., Javaid, M. K., Jones, E., Katić, V., Simpson, A., Mascalzoni, D.: Dynamic consent: a potential solution to some of the challenges of modern biomedical research. BMC Medical Ethics 18(1), p. 4-14 (2017).
17. Williams, H., Spencer, K., Sanders, C., Lund, D., Whitley, E., Kaye, J., Dixon, W. G.: Dynamic consent: a possible solution to improve patient confidence and trust in how electronic patient records are used in medical research. JMIR Medical Informatics 3(1), (2015).

18. Aitken, M., Cunningham-Burley, S., Pagliari, C.: Moving from trust to trustworthiness: Experiences of public engagement in the Scottish Health Informatics Programme. Science and Public Policy 43(5), 713–723 (2016).
19. Goodman, J. R.: A data dividend tax would help the NHS monetise health data. The British Medical Journal Opinion, (2019).
20. Meslin, E. M., Cho, M. K.: Research ethics in the era of personalized medicine: updating science's contract with society. Public Health Genomics 13(6), 378–384 (2010).
21. Kaye, J., Whitley, E., Lund, D., Morrison, M., Teare, H., Melham, K.: Dynamic consent: a patient interface for twenty-first century research networks. European Journal of Human Genetics 23, 141–146 (2015).
22 Hansson, M. G., Dillner, J., Bartram, C. R., Carlson, J. A., Helgesson, G.: Should donors be allowed to give broad consent to future biobank research?. The Lancet Oncology 7(3), 266–269 (2006).
23. Whitley, E.: Informational privacy, consent and the 'control' of personal data. Information Security Technical Report 14(3), 154–159 (2009).
24. Hammami, M. M., Al-Gaai, E. A., Al-Jawarneh, Y., Amer, H., Hammami, M. B., Eissa, A., Al Qadire, M.: Patients' perceived purpose of clinical informed consent: Mill's individual autonomy model is preferred. BMC Medical Ethics 15(1), (2014).
25. Kanellopoulou, N.: Legal philosophical dimensions of privacy. EnCoRe Project Briefing Paper, (2009).
26. Nissenbaum, H.: Privacy in context: Technology, policy, and the integrity of social life. Stanford University Press, (2009).
27. European Parliament, Regulation (EU) 2016 of the European Parliament and of the Council, 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), vol. 2012/0011 (COD), (2016).
28. Teare, H., Morrison, M., Whitley, E., Kaye, J.: Towards 'Engagement 2.0': Insights from a study of dynamic consent with biobank participants. Digital Health 1, 1–13 (2015).
29. Sanders, C., Van Staa, T., Spencer, K., Hassan, L., Williams, H., Dixon, W.: Dynamic Consent Workshop Report: Exploring new ways for patients to consent for research and use of health data. (2014).
30. Gottweis, H., Gaskell, G., Starkbaum, J.: Connecting the public with biobank research: reciprocity matters. Nature Reviews Genetics 12(11), 738 (2011).
31. Hobbs, A., Starkbaum, J., Gottweis, U., Wichmann, H., Gottweis, H.: The privacy-reciprocity connection in biobanking: comparing German with UK strategies. Public Health Genomics 15(5), 272–284 (2012).
32. Riordan, F., Papoutsi, C., Reed, J. E., Marston, C., Bell, D., Majeed, A.: Patient and public attitudes towards informed consent models and levels of awareness of Electronic Health Records in the UK. International Journal of Medical Informatics 84(4), 237–247 (2015).
33. Ludman, E. J., Fullerton, S. M., Spangler, L., Trinidad, S. B., Fujii, M. M., Jarvik, G. P., Larson, E. B., Burke, W.: Glad you asked: participants' opinions of re-consent for dbGap data submission. Journal of Empirical Research on Human Research Ethics 5(3), 9-16 (2010).
34. Lipworth, W., Morrell, B., Irvine, R., Kerridge, I.: An empirical reappraisal of public trust in biobanking research: rethinking restrictive consent requirements. Journal of law and Medicine 17, 119-132 (2009).