Collective Consent: Who Needs to Consent to the Donation of Data Representing Multiple People?

EMMA WALQUIST, University of Michigan-Flint, USA
ISHA DATEY, Oakland University, USA
WENQI ZHENG, Oakland University, USA
XIANGYU ZHOU, Wayne State University, USA
KELLY BERISHAJ, Oakland University, USA
MELISSA MCDONALD, Oakland University, USA
MICHELE PARKHILL, Oakland University, USA
DONGXIAO ZHU, Wayne State University, USA
DOUGLAS ZYTKO, University of Michigan-Flint, USA

Data donation is a growing form of personal data collection that foregrounds consent and conscious participation of the data donor. There remains little guidance on who must consent to data donation, particularly when the data represents multiple people. We provide empirical perspectives on this question through in-situ observation and interviews (N=18) with online daters who chose to donate messaging interactions with potential sexual partners for sexual violence research. Findings elucidate two diverging perspectives. Participants advocating for "unilateral consent" argued that consent of their messaging partner is not necessary, in part, because the anticipated benefit of data donation superseded consent. Participants advocating for "collective consent" wanted both messaging partners to consent to its donation, citing concerns for privacy of, and personal relationships with, the other person. Findings suggest that collective consent interfaces should be incorporated in data donation platforms, even if not strictly required by legal regulation, to improve donation of multi-person data.

CCS Concepts: • **Human-centered computing → Collaborative and social computing systems and tools**; **Human computer interaction (HCI)**; • **Applied computing → Psychology**.

Additional Key Words and Phrases: Sexual Violence, Data Donation, Consent, Online Dating, Harm, AI, Risk Detection, Trauma

ACM Reference Format:
Emma Walquist, Isha Datey, Wenqi Zheng, Xiangyu Zhou, Kelly Berishaj, Melissa McDonald, Michele Parkhill, Dongxiao Zhu, and Douglas Zytko. 2025. Collective Consent: Who Needs to Consent to the Donation of Data Representing Multiple People?. *Proc. ACM Hum.-Comput. Interact.* 9, 7, Article CSCW386 (November 2025), 30 pages. https://doi.org/10.1145/3757567

Authors' Contact Information: Emma Walquist, walquist@umich.edu, University of Michigan-Flint, Flint, MI, USA; Isha Datey, ishadatey@oakland.edu, Oakland University, Auburn Hills, MI, USA; Wenqi Zheng, wenqizheng@oakland.edu, Oakland University, Auburn Hills, MI, USA; Xiangyu Zhou, hp6438@wayne.edu, Wayne State University, Detroit, MI, USA; Kelly Berishaj, berishaj@oakland.edu, Oakland University, Auburn Hills, MI, USA; Melissa McDonald, mmmcdonald@oakland.edu, Oakland University, Auburn Hills, MI, USA; Michele Parkhill, parkhill@oakland.edu, Oakland University, Auburn Hills, MI, USA; Dongxiao Zhu, dzhu@wayne.edu, Wayne State University, Rochester, Michigan, USA; Douglas Zytko, dzytko@umich.edu, University of Michigan-Flint, Flint, MI, USA.

ACM 2573-0142/2025/11-ARTCSCW386
https://doi.org/10.1145/3757567

1 Introduction

In light of legal regulation [105] and coercive design patterns [74] around consent to personal data collection, HCI research has contended with how to support individuals in making truly informed consent decisions to requests for their personal data [23, 24, 31, 34, 50, 64, 68, 97, 108]. Data donation [96] has emerged as an alternative approach to personal data collection that foregrounds consent by making the giving of personal data a deliberate, proactive process of transferring data from one source to a third party platform. Data subjects have shown incredible willingness to donate their data for both personal and public benefit [42, 96], including intimate and sensitive data about menstrual tracking [35] and other medical conditions [56, 61]. Prior work has used data donation as a context to ask hard questions about - and pose answers to [38] - consent to data collection, such as: do donors truly understand the contents of the data they are donating [37, 44, 51, 77], and how can donors consent to particular and future uses of their donated data [44, 72]?

In this paper, we add to the discourse on data donation consent by asking *who* needs to consent to donation. Increasingly data donation involves what we call multi-person data, or data that represents more than one person. This can be incidental, such as donated voice assistant speech records where a family member is speaking in the background [34]. In other cases it is quite deliberate, such as donation of private messaging interactions on social platforms [87] to learn about online harassment and sexual violence. Multiple instances of prior work have involved donation of multi-person data in which only one person represented in the data gave consent [22, 32, 34, 50, 87, 117]. This could be interpreted as a passive argument that only one person needs to consent, although the question has not been directly broached let alone directly answered and justified in said work. The only deliberate stance in the data donation literature comes from Garimella and Chauchard [32], arguing that anonymization of multi-person data renders it unnecessary to receive consent from all persons originally represented in the data. Beyond the data donation literature, multi-person data is also mentioned in legal regulations around consent to data collection - although such regulations are far from definitive guidance given their penchant for subjective interpretation, flexibility, and lack of enforcement [58]. For instance, the EU's General Data Protection Regulation (GDPR) [105] recommends that “data controllers" who receive transported data "should implement consent mechanisms for other data subjects involved" [30] (p. 12).

Missing in the fray of conflicting and often implied stances on multi-person data consent is the perspective of data donors themselves—those who are depicted in the data, and likely have an understanding of the contextual factors surrounding its creation and donation. This leads to our research question: ***Who do data donors think must give consent to the donation of multi-person data, and why?***

We explored this question through in-situ observation and interviewing of dating app users (N = 18) who chose to donate private messaging interactions onto a third-party data donation platform for improving knowledge of, and data-driven solutions for, sexual violence. Findings revealed two perspectives on who needs to consent to donation of messaging interactions, which we call *unilateral consent* and *collective consent*. Participants who supported unilateral consent believed that only one person represented in multi-person data should have to provide consent to its donation. Rationale varied drastically, including: anticipated personal and public benefit from donation superseding consent, excessive labor involved in contacting the other person, and potential harm to the donor if their messaging partner became aware of the data donation attempt.

Participants advocating for collective consent believed both messaging partners should consent to data donation, and they justified their perspective with concerns for privacy of, and sustained relationships with, the other person. They likewise wanted collective consent to be a social process through which they personally contact the other person and discuss the mutual data donation decision. We use these findings to argue that data donation platforms should provide collective consent interfaces even if the consent of multiple subjects represented in data could be argued as optional on a legal or scholarly basis. Doing so could increase the likelihood of data donation by individuals who value the perspective of others represented in their data.

2 Background

This section reviews data donation and the different types of data that are currently given special consideration. We then define and propose multi-person data as a future consideration. We review existing research in HCI and legal works, and calls for exploration of multi-person consent.

2.1 Data Donation

Data donation is a data collection method that enables participants to voluntarily transfer their personal data to third party platforms [96]. The deliberate and proactive giving of data through data donation contrasts from other forms of data collection, such as consent management popups [65, 108] and terms of service [75], where users become reactive to requests for one's data upon accessing a website or app (often through dark patterns that may coerce users into providing their personal data with little thought [74]).

Data donation is most commonly facilitated by the donor either (1) downloading their personal data from the source website or app in the form of a consolidated data file (e.g., JSON) and providing the file to researchers [10, 34, 35, 50, 79, 87, 110], or (2) donors "scraping" data using their own personal accounts [50], although HCI research continues to propose alternative data donation processes [120, 121]. Data donation can also include more elaborate forms of participation. These include labeling one's donated data (e.g., labeling Instagram direct message conversations for the type of harm they represent [87]), contextualizing one's data through semi-structured interviews with researchers about donated data [34, 35], and even co-constructing uses of–or research on–one's donated data [38].

2.1.1 Situating Multi-Person Data Amongst Other Types of Donated Data. Designed processes for data donation are increasingly being specialized to the particular types of data anticipated for donation, most notably: personal, sensitive, and intimate data. Personal data [105] is defined as any information that links to an identifiable person either directly or indirectly. Data donation scholars have argued that collection of personal data must only be done to answer a specific research question [50, 79], that those collecting it must set limits on its future use [44, 72, 85], and that scholars must avoid misuse [14, 72, 77]. Sensitive data [105] is a subtype of personal data that has been exemplified in the GDPR with individual-level information such as race, political stance, religious beliefs, health information, or data concerning a person's sex life or sexual orientation. Similarly, within data donation literature, data is considered "intimate" [93] when it is private from others, such as data collected in personal spaces [36, 81], or data related to bodily functions [35, 41]. To be considerate of the sensitive or intimate nature of some donated data, Gomez Ortega et al. [38] proposed Sensitive Data Donation (sDD), based on principles of Data Feminism [28], to expand donor involvement beyond simply uploading data. Rather, they can serve as co-creators with joint responsibilities in "scoping the research questions and goals" [38].

The data donation literature, to our knowledge, has not adopted a clear term for donated data that represents multiple people, despite such data featuring heavily in prior work [22, 32, 34, 50, 87, 117]. We will use the term multi-person data in this paper. Donation of multi-person data can happen both incidentally and deliberately; for instance, donation of private Instagram [87] and dating app [120, 121] message conversations for the purpose of training risk mitigation AI deliberately include at least one other person in order to understand both sides of a messaging exchange. In contrast, donation of voice assistant data may incidentally include the voices of visitors and others living or working near the device [34, 111, 113]. Participants donating TikTok data [118] could choose to provide direct message conversations which included usernames, messages exchanged, and links to videos sent. Similarly, one paper introduces a designed platform to support data donation of WhatsApp messages both sent and received from other people beyond the immediate donor [32]. Prior studies involving Facebook data donation also allowed participants to donate multi-person data [22, 50] in the form of public groups including posts made by others.

2.1.2 Consent to Data Donation.

Despite emergent interest around consent in CSCW/HCI literature, there has been relatively little direct attention in the data donation literature to consent to multi-person data. The closest is [32]'s designed app for WhatsApp data donation, which can include messages sent/received by the immediate donor that represent other WhatsApp users. Garimella and Chauchard note concerns of accidentally collecting personally identifiable information about individuals who have not consented to data donation, though they consider anonymization of donated data to curtail these concerns.

Nonetheless, the data donation literature has given a dedicated focus to other aspects of consent, such as allowing donors to revoke their consent [34]. Data donation scholars' attention to consent has most often been on whether donation decisions are truly informed [34, 42, 51, 77, 78, 83, 85, 101, 110, 112], given that informed consent is a required aspect of affirmative consent (the most widely advocated model for consent in HCI [46, 66]). Critical reflection on informed consent to data donation led to questions of whether users are adequately informed of the contents of their data and what recipients of the data will do with it. Data donation sometimes requires participants to provide large, complex files which they may donate without a full understanding or review of the contents, or without closely selecting which parts of the data they do and do not consent to donating [5, 15, 34]. Furthermore, donors may not understand future uses of their data [44, 72] and may thus consent to data donation under misinformed pretenses. Prior research has also proposed ways data donation processes can support informed consent by design. For example, data donation platforms designed by Araujo et al. [8] and Boeschoten et al. [14] aim to improve the informedness of participants by explaining data to participants before they consent or process their donations. The data donation platform designed by Gomez Ortega et al. [34, 35] visually depicts data uploaded by the participant, allows them to interact with it and choose which data to omit from donation.

2.2 Complexities of Consent to Multi-Person Data

The complexities of consent to multi-person data have been discussed, or at least alluded to, in the broader scholarly literature on data consent as well as some legal regulations pertaining to data consent. We review these in separate subsections below.

2.2.1 Data Donation and Multi-Person Consent.

While the data donation literature has not directly considered questions of who needs to consent to donated data, the broader data consent literature has recognized quandaries related to multi-person data. For example, researchers of a collaborative pregnancy tracking app found tension in data sharing preferences between pregnant people and their collaborative trackers [63]; pregnant people wanted to keep some information private from their collaborators, and their collaborators often wanted access to as much information as possible. Similarly, literature on negotiating consent to smart homes finds differences in privacy preferences between multiple people living within one home as impacted by power imbalances [1, 33, 59, 119]. Finally, research exploring user perceptions of privacy in relation to shared homes finds differences in privacy concerns among those living together, and a need for improved multi-person privacy settings largely due to concerns raised by those sharing the device [33].

To our understanding, one app has been designed to help users negotiate consent when more than one user is creating data on a shared device. Based on recorded, verbal privacy consent negotiations, Zhou et al. developed an app called ThingPoll to facilitate these multi-person consent negotiations for Internet of Things (IoT) devices [122]. ThingPoll asks each user for their preferred privacy settings, and then suggests potential negotiations based on user inputs. ThingPoll is a big step forward in that it acknowledges the need for multi-person consent negotiations and simplifies the process; however, being that data sometimes unintentionally involves multiple people, and given that technology for negotiating multi-person consent is not yet widespread, those collecting multi-person data would benefit from guidance on whether everyone depicted in a dataset should provide consent, and how.

Other research has noted how multi-person data poses complications, and potentially insurmountable challenges, to "individual" consent models (if not consent broadly speaking as a feasible lens for which to reflect on data privacy self-management [98]). Lovato et al. [62] comment that current models framing consent as something that individual stakeholders provide may be ineffective for data collection contexts that implicate more than one person, and Zong [123] brings to light issues that may arise when two individuals who each have a stake in the same piece of data disagree on whether to consent. Seymour et al. express concern over allowing people to provide consent to voice assistants verbally as voice recognition of different users often fails [95]. Voice assistants thus cannot be certain that the correct person is providing consent [95].

2.2.2 Legal Discourse on Multi-Person Data Consent. Additional perspectives on multi-person data consent can be derived from legal regulation and scholarship, although we would refrain from referring to such regulation as definitive conclusion on our paper's research question due to limits in jurisdiction, subjectivity in interpretation [58], and inconsistent explicit reference to multi-person data in particular. Perhaps most applicable to the specific context of data donation is the Data Governance Act [107], which advocates for the sharing of personal and non-person data for public benefit (called data altruism). When personal data is concerned the DGA coincides with the General Data Protection Regulation (GDPR; [105]). Both the DGA and the GDPR are EU regulations, though they have extraterritorial scope as they apply to data processing done anywhere on EU subjects as well as any data processing done within the EU on subjects from other jurisdictions.

The GDPR [105] acknowledges that personal data may involve multiple people, such as data from social media platforms, in Article 20 on data portability (downloading one's personal data from a platform in a common digital format [106]). Article 20 [105] recommends that "data controllers should implement consent mechanisms for other data subjects involved" - a clear stance that other people represented in the data should have the opportunity to (not) consent, however this is not a hard requirement: "it is up to data controllers to decide on the leading practice to follow." HCI scholars have researched and critiqued the GDPR for various reasons, [26, 48, 55, 57, 57, 71, 99, 103, 104, 114, 115] though only one paper, to our knowledge, directly discusses the lack of clear protection for "third parties" represented in the data [49]. The GDPR makes notable exemptions for consent when data collection is in the "public interest" or for "scientific research" [105] - and importantly, there is confusion among scholars over how to qualify their work for such exemptions [70, 82] and whether de-identification of data alleviates consent requirements. Scholars have criticized the GDPR for complicating secondary uses of data [11, 70], for specifically creating barriers to biobank research [100], and for inconsistent applications across countries [21]. One such paper discusses differing laws and requirements that biobank researchers must follow [100], elucidating how complicated it is to truly follow all proposed data protection rules. One paper, to our knowledge, more directly discusses the lack of clear protection for "third parties" represented in the data [49].

We should not expect legal regulation to provide any definitive answers on multi-person data consent - debates over what "consent" is have persisted in legal scholarship for decades [12, 69, 73]. For instance, Hurd [45] calls attention to the critical role of autonomy in consent and under what conditions the validity of consent can be challenged - both of which are brought into question when considering data representing multiple people. Legal regulation nonetheless can be a valuable source for additional view points and even design ideas for multi-person data consent to be converged with empirical insight.

2.3 Context Of Study: Online Dating Sexual Violence

Consent has become an important concept across multiple areas within HCI/CSCW [18, 66, 92, 126]. To explore data donor’s perspectives on consent to multi-person data, we use the context of donating messaging interactions from dating apps. The intent for donating said data is to improve empirical knowledge of sexual harm in online dating by detecting behavioral patterns in messaging interactions that precede physical sexual violence (nonconsensual sexual acts) [19] between online daters upon meeting in the physical world.

Sexual violence is defined as a sexual act that is committed or attempted by another person without freely given consent of the victim or against someone who is unable to consent [9]. It is a common and traumatic experience [80, 102], with nearly one in five women and one in thirteen men reporting experiencing contact sexual violence [60]. Use of dating apps has continued to rise [7, 47] and with it, their facilitation of online and physical experiences of sexual violence, with some studies finding that up to 10% of in-person experiences of sexual violence are tied to online dating [90, 109].

Current empirical understanding of, and solutions to, online dating sexual violence are still in formative stages, necessitating more expansive datasets. Concerns of dating apps being used by bad actors to find and coerce victims into physical sexual violence are at the forefront of user concerns, particularly women [6, 25]. Yet recent qualitative studies in HCI demonstrate that sexual violence between online daters may not always be intentional: users interpret interest and consent to sex through unreliable cues in dating app interfaces [27, 125] and do not always validate their understanding of consent before initiating a sexual act during face-to-face meetings [27]. This can result in sexual violence without conscious intent to cause harm due to misunderstanding of consent believed to have been received online. Relatedly, many victims of sexual violence do not label themselves as “victims” as they may incorrectly perceive themselves as partially to blame for their own victimization [40, 52].

Understanding of how computer-mediated sexual consent practices facilitate both intentional and unintentional sexual violence could be improved with larger scale datasets of, for example, users of diverse demographics and from across multiple dating apps [127]. However, the aforementioned research demonstrates how attempts at amassing datasets about online dating sexual violence can be complicated because self-identification as victim or perpetrator cannot be assumed.

Previous research in HCI has explored technologies to intervene in-person (i.e., offline) sexual violence, however none appear suited to prevent harm through consent in online dating. For instance, previously designed safety technologies monitor the user’s location [4], provide safe-routes [13, 76, 91, 116], and alert others that the user is in danger [53]. There are opportunities for AI-driven detection of the antecedents to nonconsensual acts in online dating [25] and AI-driven scaffolding of sexual consent exchange [124], yet related work notes that existing datasets to train such AI are limited [88], especially private messaging interactions between users. Detecting risky online interactions that follow similar patterns to those who have reported experiences of sexual violence could mitigate sexual violence proactively, saving many from a traumatic experience. Importantly, useful datasets for training sexual risk detection AI require data from both consensual and nonconsensual (i.e., sexual violence) experiences so that patterns antecede to these opposing experiences can be accurately differentiated.

3 Method

To explore our research question, we conducted in-situ observations and interviews with dating app users (N = 18) while they used a data donation platform built for this research and verbally reflected on decisions to (not) donate multi-person data. The platform supported the donation of messaging interactions that the donor had with other online daters, particularly interactions with people who attempted or engaged in physical sexual encounters with them. Our University's Institutional Review Board (IRB) approved the study.

3.1 Participants and Recruitment

Participants were compensated with a $30 gift card and recruited through the following: (1) Craigslist (under the "gigs" category), (2) university email lists, (3) an empirical research participant pool managed by the university's Psychology department, (4) the university's LGBTQ+ Discord server, (5) Reddit (r/SampleSurvey), and (6) as public posts on the research team's personal social media accounts such as LinkedIn and X.

Inclusion criteria required prior use of dating apps and being at least 18 years of age. The recruitment message specified that the purpose of the study was to use, and assess the usability of, a data donation platform that collected data about their online dating experiences to help researchers better understand the connection between dating app-use and sexual activity, including sexual violence. The recruitment message clarified that they would be asked, although not required, to provide data of their "messaging conversations" and "sexual encounters" with other online daters. Understanding predictive factors of perpetration and victimization of sexual violence requires the collection of online dating interactions antecedent of consensual physical sexual encounters, nonconsensual physical sexual encounters, and interactions that did not manifest in any sexual activity. As such, our participants were not required to self-identify with, or report on, experiences of sexual violence. See section 3.2 for further rationale behind avoiding forced identification as "victims" of sexual harm.

All participants were from the United States. Participants ranged in age from 19 to 44. Of our 18 participants, 7 were Black or African-American, 6 identified as White or Caucasian, 2 were Asian, 1 was Latino, Hispanic, or of Spanish origin, 1 was Middle Eastern or North African, and 1 was Mixed. Ten identified as women, 5 as men, 1 as non-binary, 1 as gender non-conforming, and 1 as transgender man. All but one participant had at least one self-identified sexual experience through online dating, and half of participants (9) experienced sexual harm or harassment from an online dater either in-person or online in messaging. Dating apps they used were Tinder (6), Bumble (6), and Hinge (6), OkCupid (2), CoffeeMeetsBagel (1), PlentyofFish (1), Match.com (1), and eharmony (1). See Table 1 for participant demographic information.

3.2 Donor Care Precautions

The method for this study, and the design of the data donation platform, was informed through consultations with two sexual violence researchers, a sexual assault nurse examiner (SANE), and two domestic violence shelter workers, all with several years of experience interacting with victims and perpetrators of sexual harm. Our SANE consultant referenced the trauma-informed approach (TIA) [43] as the basis for her recommendations (see also [3, 20, 29]).

Table 1. Demographic information about participants from Round 1 and 2 referred to by their participation order and round of participation.

Donor	Age	Reported experience of harassment through dating apps	Self-reported Gender and Sex	Race or Ethnicity	State
ROUND 1					
R1P1	23	Yes	Gender Non-Conforming	White or Caucasian	Michigan
R1P2	27	Yes	Man	Black or African-American	Michigan
R1P3	26	Yes	Woman	Black or African-American	Michigan
R1P4	30	Yes	Woman	Black or African-American	Michigan
R1P5	29	Yes	Man	Black or African-American	Pennsylvania
R1P6	25	No	Woman	Middle Eastern or North African	Michigan
R1P7	30	No	Man	White or Caucasian	Michigan
R1P8	25	Yes	Man	White or Caucasian	Washington
ROUND 2					
R2P1	44	No	Cisgender Woman	Latino, Hispanic, or Spanish origin	Florida
R2P2	32	Yes	Transgender Man	Black or African-American	New york
R2P3	19	Yes	Non-Binary	White or Caucasian	Michigan
R2P4	32	Yes	Cisgender Woman	Black or African- American	California
R2P5	25	No	Cisgender Man	White or Caucasian	California
R2P6	22	No	Cisgender Woman	Asian	Michigan
R2P7	21	No	Cisgender Woman	Black or African-American	Michigan
R2P8	22	No	Cisgender Woman	Asian	California
R2P9	42	No	Cisgender Woman	White or Caucasian	Michigan
R2P10	21	No	Cisgender Woman	White and Black	Michigan

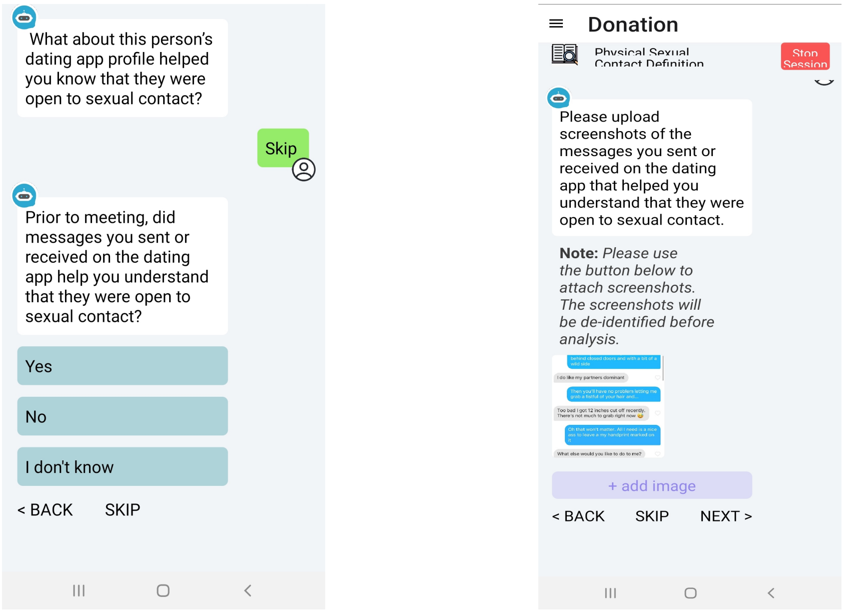
Regarding the data donation platform design, their guidance informed phrasing of questions in the interface to avoid re-traumatization [120] and forced labeling of participants' sexual experiences [121]. Specifically, we avoided the use of any language that might indicate harm (e.g., consent, rape) or insist upon participants that they are a victim or perpetrator. This extended to recruitment strategies and inclusion criteria as well; we did not require self-identification with experiences of sexual violence because victims of sexual harm often do not self-identify *as* victims, and because their labeling as “victims” by researchers may be traumatizing in itself.

Towards donor agency and control, we opted to support data donation through upload of messaging interaction screenshots rather than a file of all messaging interactions downloaded from the dating app. Participants could also skip any question verbally asked of them during the interview, and any request for data/information in the data donation interface. All donors were reminded that actually donating their data was not a required condition of participation (they could opt not to donate). No data inputted to the data donation platform was actually retained because it was not the focus of this study and thus posed an unnecessary data security risk, although participants were not informed of this until the conclusion of their session so as not to bias their donation decisions and consent perspectives.

3.3 Data Collection

All sessions were conducted online via Zoom, ranging from 94-210 minutes. The data donation platform was run on the researcher’s laptop, which participants were able to directly manipulate through remote share functionality. The sessions were audio- and screen-recorded. All sessions involved a verbal reconfirmation with the participant about the purposes of data donation in this context: to inform research on sexual violence in online dating and train sexual risk detection AI.

The brunt of the protocol was dedicated to the participant freely using the data donation platform to progress through the data donation journey while they spoke aloud about their experience and answered researchers’ questions about their decisions to (not) donate data. Our data donation platform intended to study sexual violence through the lens of consent - how people give and perceive to receive indicators of interest in sexual activity (both online and in-person) in ways that



What about this person’s dating app profile helped you know that they were open to sexual contact?

Skip

Prior to meeting, did messages you sent or received on the dating app help you understand that they were open to sexual contact?

Yes

No

I don't know

< BACK SKIP

(a) A sexual experience context question

Donation

Physical Sexual Contact Definition

Stop Session

Please upload screenshots of the messages you sent or received on the dating app that helped you understand that they were open to sexual contact.

Note: *Please use the button below to attach screenshots. The screenshots will be de-identified before analysis.*

behind closed doors and with a bit of a wild side

I do like my partners dominant

Then you'll have no problem letting me grab a fistful of your hair and...

Too bad I got 12 inches cut off recently. There's not much to grab right now 😂

Oh that won't matter. All I need is a nice ass to leave a my handprint marked on it

What else would you like to do to me?

+ add image

< BACK SKIP NEXT >

(b) A data upload prompt after clicking ’Yes’

Fig. 1. An example of a question to contextualize the sexual experience followed by a data upload prompt in the data donation app.

could lead to misinterpretation of a partner's agreement to sex. Accordingly, the data donation platform sought to collect trace data of messaging interactions with online daters with whom the donor experienced attempted or completed sexual activity.

The platform first asked the donor a series of questions to contextualize the sexual experience, including: 1) the specific sexual act that occurred or was attempted, followed by 2) how the act was initiated, followed by 3) if/how the donor knew the other person wanted the sexual act and if/how they conveyed their own desire for the sexual act, and finally 4) the role that the dating app and/or other social platforms played in understanding the other person's desire for and consent to the sexual act and conveying one's own desire for and consent to the sexual act. The donor was then prompted to upload screenshots of their messaging interactions with the other person (no uploaded data was actually saved because it was unnecessary for the purposes of this study, which participants were aware of). See Figure 1 for an example of questions donors were asked that aimed to understand how they perceive that the messaging partner is conveying sexual interest followed by a prompt to upload relevant data.

During the screenshot upload phase the data donation platform afforded options for the donor to manually edit any part of an uploaded screenshot through the use of virtual stickers and paint tools to censor content in the screenshot. Participants were directed to review this functionality even if they did not actually upload any data so as to gather their feedback on how it would influence perspectives on donation and data consent. Participants were allowed to skip any data contextualization and donation opportunity, and researchers encouraged participants to explain their rationale and reactions to key decisions made during the data donation journey. Sessions concluded with an open discussion of if and how the data donation platform could incorporate interfaces for better supporting consent to data donation.

3.4 Data Analysis

The study generated audio and screen recordings along with corresponding transcripts, which underwent reflexive thematic analysis (RTA) [16] by two members of the research team. RTA is comprised of six steps [17]: 1) familiarization with the data; 2) coding; 3) generating initial themes; 4) developing and reviewing themes; 5) refining, defining and naming themes; and 6) writing up results.

Familiarization of the data (step 1) was performed first by proofreading auto-generated transcripts of interviews to ensure accuracy. Subsequently, coding (step 2) began through extraction of quotes relevant to the research question into a separate document, loosely organized around semantic codes reflecting donors' verbatim verbal content. Initial theme generation (step 3) involved consolidation of semantic codes and beginning stages of elucidating latent constructs within themes even if such constructs did not immediately pertain to this paper (e.g., participants' reflections on how their donated data could be used). In steps 4-5 themes specific to this paper were further elucidated, and unrelated themes moved to a different document, through recurrent discussions among the research team over a multi-month period. Two fundamentally opposing perspectives on multi-person data consent became apparent at this point based on whether one's messaging partner need also be involved in giving consent. This theme development evolved into writing early drafts of paragraph-form descriptions of the findings, which sparked further recoding and restructuring of themes, particularly around justifications from participants for their perspectives on multi-person data consent. Step 6 concluded with the writing of this manuscript.

4 Findings

Participants elucidated varying perspectives and rationales on whether they alone could consent to donation of multi-person data. Participant perspectives landed in two categories: those who believed they *and* their messaging partner needed to consent (which we coined *collective consent*), and those who believed they alone could consent (which we coined *unilateral consent*). The rationale for these divergent opinions of consent are summarized in Table 2.

Participants who believed both messaging partners should consent to data donation foregrounded their interest and care for the other person: they cited concern for their messaging partner's privacy - which was rooted in privacy concerns of their data - and respect for their ongoing relationship with the messaging partner. They accordingly preferred to personally reach out to their messaging

Perspective on who needs to consent to multi-person data donation	**Rationale for perspective**	**Explanation of rationale**
Collective Consent: Everyone represented in the data must consent to its donation	Valuing privacy for oneself and messaging partner	Participants wanted to ask the other person for consent because they would want to be asked if the roles were reversed
	Relationship with messaging partner	Participants valued their ongoing relationship with the messaging partner
Unilateral Consent: Only one person represented in the data needs to consent to its donation	Capacity to edit/de-identify data	The potential for de-identification made some participants comfortable providing data without their messaging partner's consent
	Personal and public benefit	The anticipated personal and public benefits of data donation were more important than their messaging partner's consent
	Procuring the messaging partner's consent is arduous and unnecessary	Getting consent from the messaging partner is difficult and therefore not necessary, especially if they do not have a strong relationship
	Contacting the messaging partner for their consent could cause harm to the data donor	Some participants did not want their messaging partner contacted for consent because they were previously harmed by them

Table 2. A summary of the two diverging perspectives on who needs to consent to donation of data about online dating messaging interactions.

partner about consent to data donation, although they differed on whether they could submit the messaging partner's consent decision on their behalf or if the messaging partner should directly use the data donation platform (see Figures 2 and 3 for perspectives on how consent of the messaging partner should be procured). In contrast, those who believed they did not need consent from their messaging partner cited anticipated personal and public benefit from their data donation, capacity to de-identify the data during donation, and concerns for personal harm if their messaging partner were aware of their data donation attempt - particularly if their messaging partner had caused them harm in the past.

We unpack the collective consent perspective (requiring both messaging partners to consent) in section 4.1, and participants' preferences for how collective consent could be operationalized in data donation processes in section 4.2. We unpack the unilateral consent perspective (the donor alone can consent to donating messaging interaction data) in section 4.3.

4.1 Collective Consent: Rationale for Requiring Consent from All People Represented in the Data

Several participants considered it necessary to receive consent from their messaging partner before donating data about their online dating interaction; we call this stance *collective consent*. These participants provided two overarching reasons for this perspective: (1) privacy concerns for their messaging partner and (2) importance of their relationship with the messaging partner.

4.1.1 Framing Collective Consent as an Act of Privacy. Some participants described needing consent from their messaging partner because they valued their own and their messaging partner's privacy. They wanted to ask for their partner's consent because they would want to be asked if the roles were reversed. In some cases, they openly imagined themselves in the opposite role during the interview and how they would feel if their messaging partner donated data about their interaction without asking. Per R2P8: "*You know, I am [a] private person, and, you know, I wouldn't want anyone to leak my private texts. Even if they're normal texts, I wouldn't want anyone to leak that.*" R2P8's use of the word "*leak*" - in reference to unwanted and covert data breaches - was indicative of a pattern of framing the donation of multi-person data without collective consent as a negative, potentially harmful, outcome. Similarly, R1P7 noted concern over how their messaging partner might feel about their data being shared without their consent: "*Just in general, you know [I wouldn't want to share] messages between myself and another individual, who might not want other people to have [that data].*" They considered the feelings of the other person, and how difficult it may be to know whether the other person would be okay with them providing their data without asking for consent.

Some participants implied that this concern for privacy, or at least awareness of potential privacy implications for the other person represented in the data, may not be shared or understood by all data donors. As R2P5 described it: "*[People providing data] might not think anything [. . .] of taking a screenshot of images that have been exchanged in like a text message, and that could be a privacy issue for the other person involved.*" R2P5 brings attention to the differences in comfort that may exist between users who are both represented in the data, which may go unrealized by those considering only their own comfort level and consent with donating the data.

Privacy concerns were exacerbated for data that had pictures of the donor's messaging partner, be it in the messaging interaction or in their partner's profile page. The latter in particular, while not multi-person data according to our definition, drew the strongest claims of privacy violations if donated without consent of the messaging partner, even though participants considered profile pages to be otherwise "*public information*" (R2P3). The identifiability of their messaging partner through prominence of their face was typically cited as the basis of their concern. R2P7 indicated most directly: "*It feels like an invasion of trust or privacy, because people's faces are in it.*" Whereas

R2P3 compared the relative privacy of text-based data from messaging interactions to pictures: "*I think screenshots of text is more like, I can understand that more [for donation]. There's not much tied to that, like with the screenshot of the person's [dating app] profile that has, like, probably their face and a lot of information about them there. The text [from our messages] that's just text.*"

4.1.2 Relational Dynamics Behind the Perceived Necessity of Multi-Person Consent. Many participants explained that they needed consent from their messaging partner for donation of their messaging interactions because they valued their relationship with the other person. Such participants almost always had positive interactions and face-to-face meetings with the partner represented in their messaging interactions, and often had a sustained and rewarding relationship with that partner at the time of interview.

Their rationale drew on values of trust and confidence, with participants citing examples or expectations that personal information relayed to someone in a private messaging interaction would not be shown to anyone else. In at least one case this perceived responsibility to keep a messaging interaction private led a participant (R2P2) to refuse to donate messaging interaction data, instead asking if they could provide manually typed summaries of the interaction instead: "*I feel like [messaging conversations] [...] they're really, really private. So for me, it doesn't really matter if it's all part of the research, but like I can explain those kinds of situations, at least, at least I can try and push it out there [in manually typed summaries of the interaction] to the best of my ability. But then, having to actually drop a screenshot of the whole stuff, not so much.*"

Similarly, R1P5 explained how they trusted their messaging partner not to relay any "*secretive*" information about them to others and assumed their messaging partner would have placed the same trust in them. Per R1P5: "*Once you say something secretive, maybe somewhere, like I'm sure I trust you not going to deliver that information, maybe [. . .] even to your friend. That's between just me and you, so like trying to share that one sounds like you're betraying one party. What if something bad happens?*" R1P5's likening of data donation without consent to betrayal is one of the clearest examples in our data of how some participants saw unilateral decisions to donate messaging interactions as antithetical to the close relationships they built with their messaging partners. R1P5's open pondering about "*something bad*" happening was in reference to potential misuse of the data, such as a data breach and/or re-identification. Since some of these participants were worried about data misuse themselves, they projected that concern onto their messaging partners as well.

Not all participants necessarily maintained contact with the messaging partner represented in the data they were considering to donate. Conversely, some participants pointed to the absence of a strong personal relationship with their messaging partner as a reason to procure their consent to data donation. This was based on the perception that they did not know their messaging partner well enough to assume or infer their stance on consent to data donation. Per R1P1: "*I don't know them well enough to be like, oh, yeah, I can volunteer their information to this app or like to this study.*"

Rather than framing unilateral data donation decisions as a betrayal, participants in this case found the prospect of donating data on their own volition to be strange or "*weird.*" This line of thinking extended to messaging data as well as data about their messaging partner's profile page. Per R2P7: "*I mean, yeah, if it's like your own profile, then that you will be able to [donate]. But if it's like somebody else that you only had contact with, for, like, a couple of days, that [sharing someone else's dating profile] would just make it a lot more weirder.*"

4.2 Operationalizing Collective Consent in Data Donation Processes

Collective consent was not explicitly supported in our data donation platform design at the time of study. As such, participants who advocated for collective consent also brainstormed ways to support

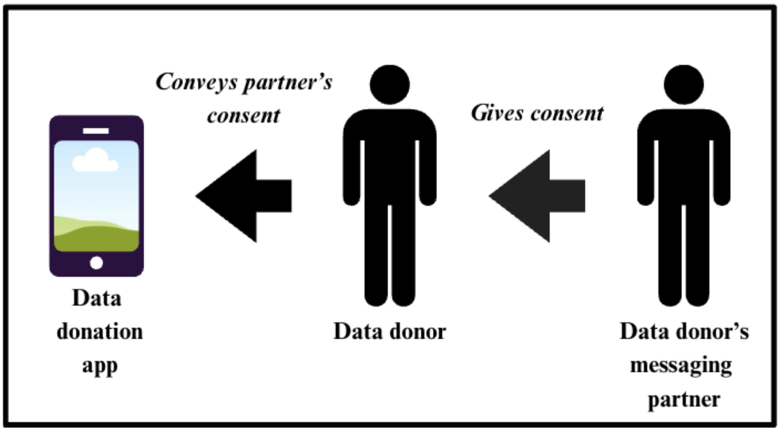


Fig. 2. Authors' rendition of how participants envisioned communicating directly with their messaging partner to procure their consent to data donation.

the involvement of their messaging partner in the data donation process. Our analysis articulated three commonly advocated approaches: 1) *collective consent as a social process* in which the original donor handles all interaction with their messaging partner and relays their consent decision to the data donation platform; 2) *collective consent as a computer-mediated process* in which the messaging partner uses the data donation platform directly to give consent; and 3) *collective contextualization* in which the messaging partner does not simply provide consent but also participates in data contextualization or annotation.

4.2.1 Collective Consent as Social Process. Given the prioritization of personal relationships expressed by participants advocating for collective consent, this emphasis on relational dynamics also extended to how collective consent could be asked for and received from individuals who are not the immediate data donor. R1P5 articulated a collective consent process in which they would personally reach out to their messaging partner to explain their intent to donate data about their messaging interaction (see Figure 2). Their partner would then give (or deny) consent directly to the donor. If their partner denies consent, the donor would simply discontinue the data donation process. In essence this process relies heavily on the data donor respecting the wishes of their messaging partner because the data donation platform would otherwise not be confirming the messaging partner's consent decision. In R1P5's words:

> R1P5: "*Yeah. First, I have to inform her [my messaging partner]. [...] Maybe she's not interested [...] she don't know who that person that her [data] is going to is, how are they going to react? [...] Yeah, yeah, I must ask them, if they confirmed [it was okay to share data] to me, then I'll share it to you definitely.*"

At first glance this social process of collective consent looks rife for abuse: a data donor could simply lie about contacting and receiving consent from their messaging partner and proceed with their data donation unchecked. Yet R1P5's use of wording like "*I have to inform her*" represents a broader theme around participants adopting a moral duty and responsibility for protecting their messaging partner. It is a personal responsibility - not an opportunity for consent fabrication - that is being emphasized in this social process of collective consent.

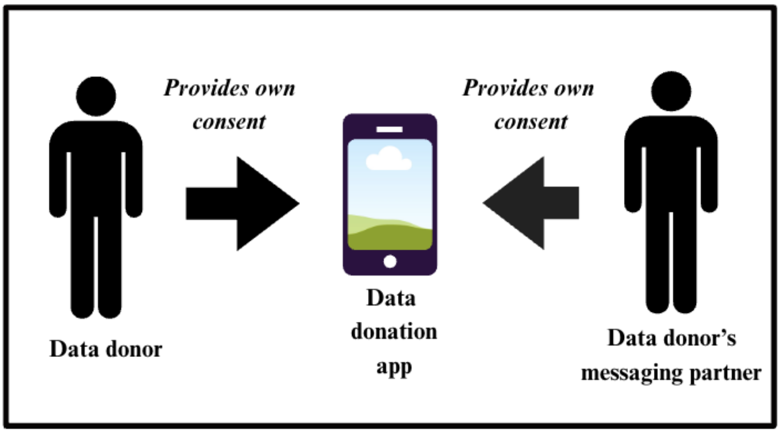


Fig. 3. Authors' rendition of how participants envisioned communicating directly with their messaging partner to provide them a link to the data donation platform to provide collective consent.

4.2.2 Collective Consent as Computer-Mediated Process. A variation of the socially driven collective consent process reported above involved providing a link to the donation donation platform so one's messaging partner could directly provide their consent (see Figure 3). This would partially mitigate misuse of an honor system-based collective consent process, however it would still put responsibility on the original donor to explain the purpose of data donation and the data they intend to donate. R1P7 briefly speculated on a process in which the donor's messaging partner is sent a link to a "*pre-populated*" donation interface by the data donation platform, which would essentially excuse the original donor from any responsibility to directly contact and procure consent from their messaging partner. However, R1P7 dismissed this idea on the basis that it might be considered "*spam*" by the messaging partner. They instead concluded with a similar idea as R1P5 - manually reaching out to the messaging partner - albeit with a link to the data donation platform. R1P7 described it this way:

> R1P7: "*I think maybe it might be more appropriate to have the person reach out to them first, and if they agree, they can kinda like give that to them, the information [to access the data donation platform]. I was more thinking like, if it's pre populated, or whatever. And then you have to, it might seem like, you know, like like a spam kind of you know what I mean like, it might seem kind of spammy. It might be better for the person to reach out to them [directly] and then and then, if they agree, they can send them the link [to the data donation platform] and all that stuff.*"

4.2.3 Collective Contextualization and Annotation of Data. The aforementioned socially oriented processes of collective consent limit the purview of the messaging partner's participation to simply confirming/giving their consent to donation of pre-prepared data. A third variation to collective consent involved expanding the purview of the messaging partner's involvement to also include collective contextualization or annotation of the data to be donated. (Contextualization in our data donation platform involved answering open-ended questions about how a donated messaging interaction was indicative of the donor's or partner's interest/consent to sexual activity). Collective contextualization was suggested in situations where participants acknowledged having subjective interpretations of the sexual experience they were donating data about, and therefore the possibility that their messaging partner may contextualize a donated messaging interaction differently. Per R2P1:

> R2P1: "*It would be cool if there was an option, so that you could, you know, enter the email address or something of the other person. If they you know, if they were claiming that it was non-consensual at any point during an in person sexual act.*"

R2P1's quote is indicative of a larger recognition from participants that they can only provide their side of the story about online dating sexual experiences, which may be biased or misinformed. Given motivations for data donation that pertained to an improved understanding of sexual violence and tools to mitigate sexual harm, some participants expressed the utility of involving their messaging partner in contextualization data. R2P3 elaborated on the utility of collective contextualization in relation to the anticipated purposes of data donation:

> R2P3: "*I think like if they [the other person in the data] wanted to be a part of it, or if you're investigating more of like, why [a sexual experience happened], they, if you wanted to follow up with them you could be like, hey, I just wanted to check in. We're doing a study. You could contact them and be like, hey, like, I just wanted to ask if you would like to be part of this. We just wanted to ask a few questions about your profile, and why you had things like this [in your messages], and how they could come across, or something like that.*"

4.3 Unilateral Consent: Relationale for Not Requiring Consent from All People in the Data

There were other participants who believed they could unilaterally consent to donation of data about their online dating messaging interactions, without awareness or consent of their messaging partner(s) depicted in the data; we call this unilateral consent. Participants provided one or more of the following justifications for this perspective: (1) capacity to edit/de-identify donated data; (2) anticipated personal and public benefit from data donation; (3) the absence of a personal relationship with their messaging partner; (4) the potential harm that the donor's messaging partner could inflict on them if aware of the data donation attempt.

4.3.1 Capacity to Edit Donated Data Alleviates Perceived Need for Collective Consent. Our data donation platform afforded participants the ability to edit donated messaging interactions by applying virtual 'stickers' over any part of the messaging interaction screenshot to censor the applicable content. Some participants explained that providing them with this interface affordance to edit their screenshot donations rendered it unnecessary or "*optional*" (R2P2) to ask for their messaging partner's consent. This was on the basis that the data editing capabilities allowed them to effectively de-identify their messaging partner in the data, or what R2P3 called taking "*their identity away*" from the data. In R2P3's words:

> R2P3: "*If you, like, depersonalize it, or like take the person and their identity away from that, that is still fine [to donate the data without their consent], and especially like you're not looking at the person's full intent. You're looking at how it [the data] was perceived [by the donor], you know? So it's like this text in the way that this person expresses themselves. There [it] was interpreted this way and sort of their intention may have been lost along the way.*"

R2P3's quote demonstrates how the alleviated need for procuring consent from their messaging partner was the result of an interplay between 1) the perceived ability to de-identify the data and 2) the perceived irrelevance of the messaging partner's identity to the intent for donation. In other words, R2P3's intention for donating their messaging interaction was to contextualize the data with their personal interpretation of their partner's messages - specifically, how their partner's messages influenced their understanding that their partner was interested in sex. The partner's actual intent behind their messages was irrelevant in this case, and with it any personally identifying information that may otherwise warrant their involvement in consent to data donation.

In some cases the capacity for de-identification was the key determinant of whether participants thought messaging interaction data could ever be donated with unilateral consent from the donor. Even then, there was still acknowledgment that donors should have the option to procure consent from their messaging partner for donation - in effect making it a personal judgment call as to whether to involve the messaging partner in the consent process. As R2P3 indicated: "*I would like [to] de-identify stuff like that, and so I think it [asking for the other person's consent] would just be an option, it just depends on the person.*"

Interestingly, participants who advocated most strongly for de-identification as the basis for their unilateral consent perspective failed to acknowledge the subjectivity and complexity in what qualifies as identifiable and de-identified data. In some cases participants implied that the determination of what content in a messaging interaction needs to be de-identified was straightforward or obvious, whereas R1P2 described confidence in their ability to "*know*" what data needs to be censored. In their words: "*If given some features to hide some statements made in conversation, I won't require an approval [from my messaging partner to donate], since I know which kind of sensitive information I'm supposed [to] hide and which ones I'm supposed to share.*" There was no acknowledgment that a donor may overlook content in their data that could be traced back to their partner, or that a donor's perspectives on what data needs to be censored may differ from that of their messaging partner depicted in the data.

One participant openly pondered whether providing what they consider "*someone else's*" data was acceptable if they could remove identifying information:

> R1P4: "*[A dating app profile,] it's someone else's, I think it's a bit, not exposing them, but I think I'd be violating privacy. [...] If I could hide the information, it could be a bit easier because [...] there's a bit of privacy there about this information. So yeah, that could be different.*"

R1P4 identified dating app profiles of other users as data that does not belong to them, and they use the lens of privacy to characterize the donation of another user's profile data without their consent as wrong (*"violating"*). However they simultaneously use the notion of data privacy, particularly its modifiability (*"if I could hide the information"*), to rationalize their ability to give unilateral consent to donation of *"someone else's"* data. This suggests that the (non-)existence of personally identifiable information about others depicted in data is core to R1P4's perception of whether they alone can consent to its donation. They did not, however, extrapolate on how one determines which information they need to *"hide"* or otherwise how to qualify multi-person data as sufficiently privacy-protective to allow for unilateral consent.

4.3.2 Expected Personal and Public Benefit to Data Donation Supersedes Consent. For some, the anticipated benefits of donating data about their online dating messaging interactions superseded the consent (or lack thereof) of their messaging partner. Participants described anticipated benefits at the personal level - direct benefits to themselves - as well as expected benefits to the public as a consequence of their donated data.

Participants citing personal benefit seldom mentioned specific benefits that would result from data donation, but rather an abstract sense of benefit to the donor. For instance, R1P3 spoke directly to how personal benefit alleviates the need to get consent from the other person depicted in their messaging interactions: "*As long as whatever you are sharing is to benefit you, I don't think there is a reason to go ahead and ask this person on [for] their consent.*"

R1P3 elaborated further, particularly on situations where their messaging partner might outright disagree to the donation of their messaging interaction. Even in this type of instance, they considered it acceptable to proceed with data donation because it is what they "*want*." This speaks to a perspective shared by some participants that personal benefit does not only render the asking of consent from their messaging partner superfluous, but that it can directly override their messaging partner's denial of consent.

"*If I go ahead and ask them [for] their consent and they say they are not comfortable with that. So for me, I feel I want to share. But they're not comfortable with that. So I feel like at this juncture, [...] they are preventing me from doing what I want.*"

Participants that justified unilateral consent with anticipated public benefit similarly talked about the direct overriding of their messaging partner's (lack of) consent to data donation, albeit for the greater good rather than any personal benefit they would receive. R2P3 used an analogy of someone needing CPR after a car accident to illustrate why it would ethically justified in some situations to donate data without consent or awareness of all represented in the data, even if said person later explicitly indicates they would not have given consent:

> R2P3: "*I think there's like certain current kinds of things where, if you were to try and like, give someone CPR, if they were in a car accident or something, and they like get saved, they could be like, I didn't want you to give me CPR, and like sue you about it. That's like what? Hello! I assumed you didn't want to die!*"

Whereas references to personal benefit from participants remained abstract, those citing public benefit as a justification for unilateral consent were referring to the goal "*to understand sexual violence*" (R1P7) through analysis and risk mitigation model training of a donor-created dataset of online dating messaging interactions preceding sexual activity. As R1P3 confirmed, "*if [this] purpose is given, then I will be okay.*"

Other participants elaborated on how the particular type of experience depicted in the donated data could ethically justify the overriding of consent from all people represented in the data. R1P4 described a hypothetical situation where a messaging interaction indicative of sexual abuse would justify unilateral consent for donation because the importance of that data to potential public benefit through improved understanding sexual violence would supercede consent of any party to that messaging interaction. They went on to describe that data, despite coming from a private messaging interaction, as "*not at all private*" because the experience depicted in the data warrants its public use for sexual violence mitigation. As they discussed with the interviewer:

> R1P4: "*So if if I had if the situation was reversed, and then maybe I was sexually abused by a via text or something like that, that's when I would be comfortable to share, because that is something that I will want to [...] I'll be [willing] to share my story on that, that is not private that is not at all private. That is, yeah.*"
> Interviewer: "*So so you're saying, like, if you had been, like, maybe the screenshots were about someone harassing you or something on maybe Tinder, that you would be okay with sharing [without the messaging partner's consent]?*"
> R1P4: "*Yeah, because I, I, I wasn't on board with them because and it's actually not a right thing to do.*"

4.3.3 Relational Dynamics Make Multi-Person Consent Arduous and Unnecessary. Other participants explained collective consent as unnecessary, not because of a subsuming goal for donation that overrides the importance of consent, but because the relationship with the messaging partner depicted in the data was never strong enough to render their consent important. This finding is almost a direct contrast to the relational dynamics driving collective consent cited by participants who had strong, sustained relationships with their messaging partners (see section 4.1.2). Here, the data being considered for donation involved messaging interactions that were very short or with whom the donor had lost contact, posing uncertainty as to whether they would ever respond to a request for data donation consent.

R1P2 described their relationship with the applicable messaging partner this way: "*That's somebody I don't know, so he's just a stranger [...] I don't need their approval to [donate data about our interaction].*" Their quote conveys a dismissal of the messaging partner's consent on the basis that they did not really know the partner on a personal level, even to the extent of not being sure they were a real person. R1P2 described such a possibility in this way: *"Maybe he's trying to fake the pictures. It's not a real one, so I won't care about that."* We should note that some participants' views about their messaging partner and their argument against asking for their consent to data donation evolved in real time, seemingly as a way to build justification for skipping the effort of contacting their messaging partner for consent. As R1P2's quote exemplifies, their thinking evolved from their messaging partner's profile "*maybe*" being fake to it definitely being fake and therefore exempt from needing to consent to data donation.

Other participants were even more blatant about their motivation to save time and effort through unilateral consent to data donation. As R1P3 directly put it: "*It's a long process [to reach out to the other person and get their consent], and it's not necessary. If as long as the individual [donor] is ready to share the information, the data, there is no need to refer to the non-individual consent user.*" This reference to a "*long process*" connects back to the severed or fleeting nature of the participant's interaction with the person represented in the messaging interaction. Communication with such a messaging partner may no longer be possible, or at the very least quite awkward given the absence of rapport that could be relied on for broaching the notion of data donation. There were yet other vague rationales for why the donor should not have to contact their former messaging partner for consent to data donation. For example, R1P3 used the argument that consent could be unilaterally given as long as the donated data is not edited, although they struggled to expand on this justification: "*I think it's [getting the other person's consent] not necessary as long as what I'm sharing is genuine. It's just exactly what is in [...] the conversation we had.*"

4.3.4 Multi-Person Consent Could Lead to Harm Against the Data Donor. Some participants expressed concern over asking their messaging partner's consent to data donation because the act of informing them of the attempt to donate data and procuring their consent could itself cause personal harm. This harm was only cited by participants who wanted to donate data about messaging interactions indicative of harassment, or that preceded an act of physical sexual harm during a face-to-face date. Because their messaging partner depicted in this data had harmed them before, they considered the prospect of contacting them for any reason to be potentially traumatizing. They also voiced concerns of retaliatory harm for their intent to donate data about their messaging interaction for sexual violence mitigation-related goals.

R1P1 mentioned some unpleasant face-to-face meetings with online daters that they used to speculate on more severe online dating experiences that would discourage a donor from ever wanting to reconvene contact. R1P1 explained, "*What if this experience is bad? [...] What if someone suffering [...] as a victim of sexual violence like it was just a horrible experience? I've had those times where I've gone out to meet a person, and they've already been belligerently drunk. I've had several drinks spilled on me, [...] not a fun time, and so like, that's when you get out of there, [...] I wouldn't want the person to come [consent].*"

Aside from a reluctance to contact a former perpetrator of harm for data donation consent, there was also mention that contacting the perpetrator may no longer be possible due to prior steps taken to prevent contact. Blocking the perpetrator on the applicable dating app was one example, which forces the donor to make a choice over whether to unilaterally consent to donate data about their messaging interaction or to not donate the data at all. Given the intent behind data donation in our study being towards improved sexual violence understanding and prevention, they opted to donate.

R2P3 elaborated on how blocking a perpetrator prevents their involvement in consent to future data donation: "*Something with my specific experience with this is the two people that I have had, like, some form of encounter with, it has not been entirely positive and so I blocked them. So I do not have access to their profiles. So that is something to note is that if something is negative, they might just not have the ability to check.*"

5 Discussion

This paper sought to provide empirical perspective on the question of who needs to consent to the donation of data that represents multiple people (multi-person data). Through in-situ observations and interviews with online daters who chose to donate messaging interactions with potential sexual partners, we uncovered two opposing perspectives: collective consent, through which everyone depicted in the data should provide consent to its donation, and unilateral consent, through which only the immediate donor provides consent. Participants advocating for collective consent did so because of their relationship with the other person, or because of their concern for the other person's privacy. Those who advocated for unilateral consent cited alleviated concerns after editing their data, personal and public benefit, relational dynamics with the other person depicted in the data, and harm that they could incur if obtaining consent from the other person.

In this section we first critically review participant perspectives on consent to donation of multi-person data and situate our findings within the broader literature. Next, we provide methodological suggestions for incorporating collective consent into data donation processes so as not to dissuade participation from donors who value the inclusion of other people represented in donated data. We conclude with limitations of our study and associated future research directions.

5.1 Reflection on Participants' Arguments for Unilateral Consent to Multi-Person Data

Some advocates for unilateral consent cited the anticipated value of their donated data beyond themselves, particularly to improved public knowledge about sexual violence and AI-driven tools for sexual violence mitigation. This motivation to donate data for a cause echoes prior work in the data donation sphere finding that research context and goals are important in decisions to donate data [36, 96]. Perhaps the most compelling argument from our participants was the fear of retaliatory harm if their (former) messaging partner became aware of the data donation attempt, particularly when said messaging partner had perpetrated sexual harm in the past (and thus may do it again). There is empirical basis for this fear in the broader sexual assault literature; a common barrier to victims of sexual assault reporting to authority is the fear of retaliation [84]. Participants' concerns about excessive labor to obtain consent from the other person do seem reasonable as well, especially in light of other research acknowledging that it may not always be possible to procure consent of all individuals in multi-person data–or even to identify who they are [34].

Yet other arguments for unilateral consent initially appear as manufactured reasons to justify avoiding the labor of contacting one's messaging partner for consent, which could delay the data donation process (particularly claims that personal benefit of data donation should supersede consent). Claims of personal benefit may in part be due to limited understanding of the relative risks and benefits in providing personal data [98], or a general undervaluing of privacy [73]. While data donation scholars have sought to ensure data donors fully understand the scope of the data they provide [34, 42, 51, 77, 78, 83, 85, 101, 110, 112], future work could explore if unilateral consent perspectives may be more influenced by understandings of the relative privacy risks and benefits of donation.

Some participants who advocated for unilateral consent also considered the data anonymization capabilities in our data donation platform to exempt the need for consent from people de-identified in the data (in effect, defining multi-person data with identifiability). This is a similar argument to one made in prior literature on WhatsApp data donation [32]. However, de-identification does not guarantee protection of a person's data–in fact, seemingly de-identified data has been used on multiple occasions to re-identify persons, especially when the dataset can be connected with other publicly available data [67]. Furthermore, this perspective that de-identification is an ethical way to alleviate the need for consent from others who also have a stake in the data brings into question "who" is doing the de-identifying, and if they can adequately recognize all aspects of the data that could directly or indirectly lead to identification [39].

5.2 Implications: Supporting Collective Consent by Design

Participant justifications for collective consent align with the public's concern for privacy [73], as well as the GDPR's assertion to avoid adverse effects to "the rights and freedoms of the other data subject" and recommendation of "consent mechanisms for other data subjects involved" (article 20, [105]). Precise designs or design approaches to said consent mechanisms remain largely absent in scholarly discourse, however. We use our study's findings to offer three design suggestions for collective consent interfaces: (1) default to allowing, but not requiring, consent from all parties, (2) consult with context-specific experts, and (3) do not allow donors to record collective consent decisions for other people. These are explored in depth below, while noting that the applicability of these design directions may be limited to data donation contexts where the donor has an accurate understanding of the contents of the data to be donated, including accurate identification of other people depicted in the data.

5.2.1 Default to Allowing, but Not Requiring, Consent from All Parties. We initially motivated our study by asking who "must" give consent to donation of multi-person data. Our findings, particularly from participants advocating for collective consent, suggest the question should be rephrased to who should be "able" to consent to donation of multi-person data. Some of our participants advocating for collective consent made clear that they would be unwilling to donate their messaging interaction data without the consent of their messaging partner. This begs the question of how many would-be donors have been, and will be, dissuaded from participating in multi-person data donation efforts simply because the data donation platform lacks affordances to involve other people represented in the data. The firm position of these participants provides a compelling argument for why data donation platforms should at least afford opportunities for collective consent, even if not strictly required for use.

5.2.2 Consult with Context-Specific Experts. Referring back to an argument from participants supporting unilateral consent, we also urge consideration of data donation contexts where collective consent may itself pose risk to immediate and tertiary donors. Our participants cited concerns of retaliatory harm, but there is also a risk of retraumatization [43, 121] if the respective multi-person data is reflective of a particularly traumatic experience for one or more people represented in the data. For instance, a donor may invite their online dating messaging partner to provide consent to the donation of their messaging interaction, unaware that the messaging partner considered their sexual interaction to be deeply painful–memories of which the invitation to be involved in data donation may reawaken. In light of other HCI literature advocating for the trauma-informed approach in computing [2, 54, 86, 89, 89, 94, 120, 121], we would recommend that domain experts or trauma-informed care professionals be consulted for contexts of multi-person data donation known to be associated with harm or particularly intimate experiences.

5.2.3 Do Not Allow Donors to Record Collective Consent Decisions for Other People. Some design concepts from participants in this study for collective consent were heavily reliant on the honor system: they wanted to assume much of the collective consent process themselves, including reaching out to their messaging partner and communicating their consent decision on their behalf. Aside from the opportunity for intentional fabrication of the other person's consent decision, there is also the possibility that the donor may unintentionally misrepresent important details about the data being donated. The contents of the data being donated in our particular study were relatively straightforward because donors actively created the data to be donated through screenshots. However the contexts of prior data donation research (e.g., voice records) demonstrate how donors may have a difficult time understanding the contents of their data to be donated, especially in situations of downloading one's personal data from a separate platform or app as a single JSON file with scarce or nonexistent innate capabilities to review the data [37, 44, 51, 77]. We would thus recommend that collective consent be supported through features that require other subjects represented in multi-person data to directly use the data donation platform to assess the purpose for data donation and the particular data being donated.

5.3 Limitations and Future Work

There are important limitations of our study that should be noted, and which can serve as the basis for future research into multi-person data consent. For one, donor perspectives on multi-person consent are likely contingent on the nature of the experience reflected in the data. Participants in our study did experience a variety of messaging and sexual interactions with online daters, some of which were harmful, some positive, and some forgettable. Those advocating for collective consent had generally positive experiences, and in some cases were still on speaking terms with the messaging partner represented in their data. There may be additional, and more nuanced, perspectives on multi-person data consent from donors who had, for example, prolonged interactions with online daters with a mix of positive and negative parts of the interaction. The context of data donation, and sensitivity of donated data, may also play a role in willingness, and associated dissuasion, from donating multi-person data [36, 96]. This study's focus on data related to online dating sexual experiences may limit its transferability to other data donation contexts.

The type of data (messaging interactions) focused on in this study, as well the manner of donation (screenshots hand-picked by donors), also diverge from other data donation contexts where the contents of donated data - including "who" is depicted in the data and what the data precisely contains - are not always well understood by the donor [37, 44, 51, 77]. This is especially poignant in situations of incidental multi-person data (e.g., an unknown person speaking in the background on voice record data) and when donating single JSON files that automatically compile vast amounts of personal data. The transferability of our findings, and applicability of design suggestions for collective consent, may not apply to data donation contexts where the donor does not know if other people are depicted in their data, or who they are, or what specific parts of the data pertain to them. This is a prime opportunity for future work: to explore dynamics and design for collective consent under conditions of donor unfamiliarity with data.

6 Conclusion

Data donation research has been at the forefront of designed processes to center consent in the collection of personal data. In addition to critical reflections and improvements to informed consent that have been the subject of prior data donation research, we explored the question of who must consent to data donation. This question necessitates deliberate consideration because data donation efforts often focus on data that represents multiple people, which we call multi-person data. While prior literature and legal regulation provide varying guidance on who needs to consent to the donation of multi-person data, we provided empirical perspectives from online daters who decided to donate data about their dating app messaging interactions with sexual partners. Findings articulated two divergent perspectives. Those advocating for unilateral consent believed they alone could consent to multi-person data donation, citing anticipated personal and public benefit. Those advocating for collective consent wanted their messaging partner to also give consent, rooted in genuine concern for their messaging partner's safety and valuing of their personal relationship. We used the findings to argue that data donation platforms targeting multi-person data should provide affordances for collective consent so as not to discourage participation of donors who value collective decision-making with other people represented in their data. Opportunities for future work likewise involve design and development of collective data consent interfaces to be subjected to usability assessment.

Acknowledgments

This material is based upon work partially supported by the U.S. National Science Foundation under Grant No. National Science Foundation 2211896, 2401775, 2339431, and 2211897. It was also partially supported by University of Michigan-Flint through the CIT Research Seed Grant Program and IST Large Grant Award.

References

[1] Luca Hernández Acostsa and Delphine Reinhardt. 2022. Multi-User Privacy with Voice-Controlled Digital Assistants. In *2022 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)*. 30–33. doi:10.1109/PerComWorkshops53856.2022.9767270

[2] Naseem Ahmadpour, Lian Loke, Carl Gray, Yidan Cao, Chloe Macdonald, and Rebecca Hart. 2023. Understanding how technology can support social-emotional learning of children: a dyadic trauma-informed participatory design with proxies. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. ACM, Hamburg Germany, 1–17. doi:10.1145/3544548.3581032

[3] Alex A. Ahmed, Teresa Almeida, Judeth Oden Choi, Jon Pincus, and Kelly Ireland. 2018. What's at Issue: Sex, Stigma, and Politics in ACM Publishing. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM, Montreal QC Canada, 1–10. doi:10.1145/3170427.3188400

[4] Mohammed Eunus Ali, Shabnam Basera Rishta, Lazima Ansari, Tanzima Hashem, and Ahamad Imtiaz Khan. 2015. SafeStreet: empowering women against street harassment using a privacy-aware location based application. In *Proceedings of the Seventh International Conference on Information and Communication Technologies and Development* (Singapore, Singapore) *(ICTD '15)*. Association for Computing Machinery, New York, NY, USA, Article 24, 4 pages. doi:10.1145/2737856.2737870

[5] Fatemeh Alizadeh, Timo Jakobi, Jens Boldt, and Gunnar Stevens. 2019. GDPR-Reality Check on the Right to Access Data: Claiming and Investigating Personally Identifiable Data from Companies. In *Proceedings of Mensch Und Computer 2019* (Hamburg, Germany) *(MuC '19)*. Association for Computing Machinery, New York, NY, USA, 811–814. doi:10.1145/3340764.3344913

[6] Hanan Khalid Aljasim and Douglas Zytko. 2023. Foregrounding Women's Safety in Mobile Social Matching and Dating Apps: A Participatory Design Study. *Proceedings of the ACM on Human-Computer Interaction* 7, GROUP, 1–25. doi:10.1145/3567559

[7] Monica Anderson, Emily A Vogels, and Erica Turner. 2020. The virtues and downsides of online dating. Pew Research Center report. (2020). https://coilink.org/20.500.12592/q2dgn9

[8] Theo Araujo, Jef Ausloos, Wouter van Atteveldt, Felicia Loecherbach, Judith Moeller, Jakob Ohme, Damian Trilling, Bob van de Velde, Claes De Vreese, and Kasper Welbers. 2022. OSD2F: An open-source data donation framework. *Computational Communication Research* 4, 2, 372–387. doi:10.5117/CCR2022.2.001.ARAU

[9] Kathleen C. Basile and Linda E. Saltzman. 2002. *Sexual violence surveillance; uniform definitions and recommended data elements.* Report. Centers for Disease Control and Prevention, National Center for Injury Prevention and Control, Division of Violence Prevention. https://stacks.cdc.gov/view/cdc/6545

[10] Susanne E. Baumgartner, Sindy R. Sumter, Vladislav Petkevič, and Wisnu Wiradhany. 2023. A Novel iOS Data Donation Approach: Automatic Processing, Compliance, and Reactivity in a Longitudinal Study. *Social Science Computer Review* 41, 4, 1456–1472. doi:10.1177/08944393211071068

[11] Regina Becker, Davit Chokoshvili, Giovanni Comandé, Edward S. Dove, Alison Hall, Colin Mitchell, Fruzsina Molnár-Gábor, Pilar Nicolàs, Sini Tervo, and Adrian Thorogood. 2022. Secondary Use of Personal Health Data: When Is It "Further Processing" Under the GDPR, and What Are the Implications for Data Controllers? *European Journal of Health Law* 30, 2, 129 – 157. doi:10.1163/15718093-bja10094

[12] Deryck Beyleveld and Roger Brownsword. 2007. *Consent in the Law.* Hart Publishing. https://durham-repository.worktribe.com/output/1126548

[13] Jan Blom, Divya Viswanathan, Mirjana Spasojevic, Janet Go, Karthik Acharya, and Robert Ahonius. 2010. Fear and the city: role of mobile services in harnessing safety and security in urban use contexts. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Atlanta, Georgia, USA) *(CHI '10)*. Association for Computing Machinery, New York, NY, USA, 1841–1850. doi:10.1145/1753326.1753602

[14] Laura Boeschoten, Jef Ausloos, Judith E. Möller, Theo Araujo, and Daniel L Oberski. 2022. A framework for privacy preserving digital trace data collection through data donation. *Computational Communication Research* 4, 2, 388–423. doi:10.5117/CCR2022.2.002.BOES

[15] Alex Bowyer, Jack Holt, Josephine Go Jefferies, Rob Wilson, David Kirk, and Jan David Smeddinck. 2022. Human-GDPR Interaction: Practical Experiences of Accessing Personal Data. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (New Orleans, LA, USA) *(CHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 106, 19 pages. doi:10.1145/3491102.3501947

[16] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3, 2, 77–101. doi:10.1191/1478088706qp063oa

[17] Virginia Braun and Victoria Clarke. 2021. Thematic Analysis: A Practical Guide. SAGE Publications Ltd, 1–376.

[18] Braeden Burger, Devin Tebbe, Emma Walquist, Toby Kind, and Douglas Zytko. 2025. Saying No to "Yes Means Yes": Limitations of Affirmative Consent for Mitigating Unwanted Behavior Online According to Women and LGBTQIA+ Stakeholders. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems (CHI '25)*. Association for Computing Machinery, New York, NY, USA, Article 106, 17 pages. doi:10.1145/3706598.3713236

[19] Centers for Disease Control and Prevention (CDC). 2024. Sexual Violence: Definitions. https://www.cdc.gov/sexual-violence/about/index.html Accessed: 2024-10-29.

[20] Janet X. Chen, Allison McDonald, Yixin Zou, Emily Tseng, Kevin A Roundy, Acar Tamersoy, Florian Schaub, Thomas Ristenpart, and Nicola Dell. 2022. Trauma-Informed Computing: Towards Safer Technology Experiences for All. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (New Orleans, LA, USA) *(CHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 544, 20 pages. doi:10.1145/3491102.3517475

[21] Niamh Clarke, Gillian Vale, Emer P. Reeves, Mary Kirwan, David Smith, Michael Farrell, Gerard Hurl, and Noel G. McElvaney. 2019. GDPR: an impediment to research? *Irish Journal of Medical Science (1971-)* 188, 1129–1135. doi:10.1007/s11845-019-01980-2

[22] Joao Couto and Kiran Garimella. 2024. Examining (Political) Content Consumption on Facebook Through Data Donation. (2024). arXiv:2407.08171 [cs.SI] https://arxiv.org/abs/2407.08171

[23] Mathieu Cunche, Daniel Le Métayer, and Victor Morel. 2020. ColoT: a consent and information assistant for the IoT. In *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks* (Linz, Austria) *(WiSec '20)*. Association for Computing Machinery, New York, NY, USA, 334–336. doi:10.1145/3395351.3401797

[24] Bart Custers, Simone van Der Hof, Bart Schermer, Sandra Appleby-Arnold, and Noellie Brockdorff. 2013. Informed consent in social media use-the gap between user expectations and EU personal data protection law. *SCRIPTed* 10, 435.

[25] Isha Datey and Douglas Zytko. 2024. "Just Like, Risking Your Life Here": Participatory Design of User Interactions with Risk Detection AI to Prevent Online-to-Offline Harm Through Dating Apps. *Proc. ACM Hum.-Comput. Interact.* 8, CSCW2, Article 367, 41 pages. doi:10.1145/3686906

[26] Paul De Hert, Vagelis Papakonstantinou, Gianclaudio Malgieri, Laurent Beslay, and Ignacio Sanchez. 2018. The right to data portability in the GDPR: Towards user-centric interoperability of digital services. *Computer Law & Security Review* 34, 2, 193–203. doi:10.1016/j.clsr.2017.10.003

[27] Christopher Dietzel. 2024. Clickable Consent: How Men Who Have Sex with Men Understand and Practice Sexual Consent on Dating Apps and in Person. *The Journal of Sex Research* 61, 3, 481–494. arXiv:https://doi.org/10.1080/00224499.2023.2235584 doi:10.1080/00224499.2023.2235584 PMID: 37526356.

[28] Catherine D'ignazio and Lauren F Klein. 2023. *Data feminism.* MIT press.

[29] Catherine D'Ignazio, Rebecca Michelson, Alexis Hope, Josephine Hoy, Jennifer Roberts, and Kate Krontiris. 2020. "The Personal is Political": Hackathons as Feminist Consciousness Raising. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW2, 1–23. doi:10.1145/3415221

[30] European Data Protection Board (EDPB). 2016. Guidelines on the Right to Data Portability under Regulation 2016/679. https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-right-data-portability-under-regulation-2016679_en Accessed: 2024-10-29.

[31] Batya Friedman, Edward Felten, and Lynette I Millett. 2000. Informed consent online: A conceptual model and design principles. *University of Washington Computer Science & Engineering Technical Report 00–12–2* 8 (2000). https://dada.cs.washington.edu/research/tr/2000/12/UW-CSE-00-12-02.pdf

[32] Kiran Garimella and Simon Chauchard. 2024. WhatsApp Explorer: A Data Donation Tool To Facilitate Research on WhatsApp. arXiv:2404.01328 [cs.SI] https://arxiv.org/abs/2404.01328

[33] Christine Geeng and Franziska Roesner. 2019. Who's In Control? Interactions In Multi-User Smart Homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–13. doi:10.1145/3290605.3300498

[34] Alejandra Gomez Ortega, Jacky Bourgeois, Wiebke Toussaint Hutiri, and Gerd Kortuem. 2023. Beyond data transactions: a framework for meaningfully informed data donation. *AI & SOCIETY*, 1–18. doi:10.1007/s00146-023-01755-5

[35] Alejandra Gomez Ortega, Jacky Bourgeois, and Gerd Kortuem. 2022. Reconstructing Intimate Contexts through Data Donation: A Case Study in Menstrual Tracking Technologies. In *Nordic Human-Computer Interaction Conference* (Aarhus, Denmark) *(NordiCHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 8, 12 pages. doi:10.1145/3546155.3546646

[36] Alejandra Gómez Ortega, Jacky Bourgeois, and Gerd Kortuem. 2023. What is Sensitive About (Sensitive) Data? Characterizing Sensitivity and Intimacy with Google Assistant Users. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (Hamburg, Germany) *(CHI '23)*. Association for Computing Machinery, New York, NY, USA, Article 586, 16 pages. doi:10.1145/3544548.3581164

[37] Alejandra Gómez Ortega, Jacky Bourgeois, and Gerd Kortuem. 2024. Participation in Data Donation: Co-Creative, Collaborative, and Contributory Engagements with Athletes and their Intimate Data. In *Proceedings of the 2024 ACM Designing Interactive Systems Conference* (Copenhagen, Denmark) *(DIS '24)*. Association for Computing Machinery, New York, NY, USA, 2388–2402. doi:10.1145/3643834.3661503

[38] Alejandra Gómez Ortega, Jacky Bourgeois, and Gerd Kortuem. 2024. Sensitive Data Donation: A Feminist Reframing of Data Practices for Intimate Research Contexts. In *Proceedings of the 2024 ACM Designing Interactive Systems Conference* (Copenhagen, Denmark) *(DIS '24)*. Association for Computing Machinery, New York, NY, USA, 2420–2434. doi:10.1145/3643834.3661524

[39] Wentao Guo, Aditya Kishore, Adam J. Aviv, and Michelle L. Mazurek. 2024. A Qualitative Analysis of Practical De-Identification Guides. In *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security* (Salt Lake City, UT, USA) *(CCS '24)*. Association for Computing Machinery, New York, NY, USA, 1611–1625. doi:10.1145/3658644.3690270

[40] Kate Lockwood Harris. 2011. The Next Problem With No Name: The Politics and Pragmatics of the Word Rape. *Women's Studies in Communication* 34, 1 (2011), 42–63. arXiv:https://doi.org/10.1080/07491409.2011.566533 doi:10.1080/07491409.2011.566533

[41] Karey Helms. 2019. Do You Have to Pee? A Design Space for Intimate and Somatic Data. In *Proceedings of the 2019 on Designing Interactive Systems Conference* (San Diego, CA, USA) *(DIS '19)*. Association for Computing Machinery, New York, NY, USA, 1209–1222. doi:10.1145/3322276.3322290

[42] Yasemin Hirst, Sandro T Stoffel, Hannah R Brewer, Lada Timotijevic, Monique M Raats, and James M Flanagan. 2023. Understanding Public Attitudes and Willingness to Share Commercial Data for Health Research: Survey Study in the United Kingdom. *JMIR Public Health Surveill* 9, e40814. doi:10.2196/40814

[43] Larke N Huang, Rebecca Flatow, Tenly Biggs, Sara Afayee, Kelley Smith, Thomas Clark, and Mary Blake. 2014. SAMHSA's concept of trauma and guidance for a trauma-informed approach. (2014). http://hdl.handle.net/10713/18559

[44] Patrik Hummel, Matthias Braun, and Peter Dabrock. 2019. Data donations as exercises of sovereignty. *The ethics of medical data donation*, 23–54. https://doi.org/10.1007/978-3-030-04363-6_3

[45] Heidi M. Hurd. 1996. The Moral Magic of Consent. *Legal Theory* 2, 2, 121–146. doi:10.1017/S1352325200000434

[46] Jane Im, Jill Dimond, Melody Berton, Una Lee, Katherine Mustelier, Mark S. Ackerman, and Eric Gilbert. 2021. Yes: Affirmative Consent as a Theoretical Framework for Understanding and Imagining Social Platforms. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 403, 18 pages. doi:10.1145/3411764.3445778

[47] Mansoor Iqbal. 2019. YouTube revenue and usage statistics. *Business of Apps. [Accessed: 2020-01-15]* (2019). https://www.businessofapps.com

[48] Jack Jamieson and Naomi Yamashita. 2023. Escaping the Walled Garden? User Perspectives of Control in Data Portability for Social Media. *Proc. ACM Hum.-Comput. Interact.* 7, CSCW2, Article 339, 27 pages. doi:10.1145/3610188

[49] Ruth Janal. 2017. Data portability-a tale of two concepts. *J. Intell. Prop. Info. Tech. & Elec. Com. L.* 8 (2017), 59. https://nbn-resolving.de/urn:nbn:de:0009-29-45324

[50] Mario Haim Johannes Breuer, Zoltán Kmetty and Sebastian Stier. 2023. User-centric approaches for collecting Facebook data in the 'post-API age': experiences from two studies and recommendations for future research. *Information, Communication & Society* 26, 14, 2649–2668. arXiv:https://doi.org/10.1080/1369118X.2022.2097015 doi:10.1080/1369118X.2022.2097015

[51] Kerina H Jones. 2019. Incongruities and dilemmas in data donation: juggling our 1s and 0s. *The Ethics of Medical Data Donation*, 75–93. https://doi.org/10.1007/978-3-030-04363-6_5

[52] Arnold S. Kahn, Jennifer Jackson, Christine Kully, Kelly Badger, and Jessica Halvorsen. 2003. Calling it Rape: Differences in Experiences of Women Who do or do not Label their Sexual Assault as Rape. *Psychology of Women Quarterly* 27, 3 (2003), 233–242. arXiv:https://doi.org/10.1111/1471-6402.00103 doi:10.1111/1471-6402.00103

[53] Naveena Karusala and Neha Kumar. 2017. Women's Safety in Public Spaces: Examining the Efficacy of Panic Buttons in New Delhi. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (Denver, Colorado, USA) *(CHI '17)*. Association for Computing Machinery, New York, NY, USA, 3340–3351. doi:10.1145/3025453.3025532

[54] Shannon Kelly, Benjamin Lauren, and Kaitlyn Nguyen. 2021. Trauma-informed Web Heuristics for Communication Designers. In *Proceedings of the 39th ACM International Conference on Design of Communication* (Virtual Event, USA) *(SIGDOC '21)*. Association for Computing Machinery, New York, NY, USA, 172–176. doi:10.1145/3472714.3473638

[55] Johann Kranz, Sophie Kuebler-Wachendorff, Emmanuel Syrmoudis, Jens Grossklags, Stefan Mager, Robert Luzsa, and Susanne Mayr. 2023. Data portability. *Business & Information Systems Engineering* 65, 5, 597–607. https://doi.org/10.1007/s12599-023-00815-w

[56] Jenny Krutzinna, Mariarosaria Taddeo, and Luciano Floridi. 2019. An Ethical Code for Posthumous Medical Data Donation. In *The Ethics of Medical Data Donation*, Jenny Krutzinna and Luciano Floridi (Eds.). Springer International Publishing, Cham, 181–195. doi:10.1007/978-3-030-04363-6_12

[57] Sophie Kuebler-Wachendorff, Robert Luzsa, Johann Kranz, Stefan Mager, Emmanuel Syrmoudis, Susanne Mayr, and Jens Grossklags. 2021. The right to data portability: Conception, status quo, and future directions. *Informatik Spektrum* 44, 264–272. https://doi.org/10.1007/s00287-021-01372-w

[58] Lin Kyi, Sushil Ammanaghatta Shivakumar, Cristiana Teixeira Santos, Franziska Roesner, Frederike Zufall, and Asia J. Biega. 2023. Investigating Deceptive Design in GDPR's Legitimate Interest. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (Hamburg, Germany) *(CHI '23)*. Association for Computing Machinery, New York, NY, USA, Article 583, 16 pages. doi:10.1145/3544548.3580637

[59] Vincent K. N. Lau, Fan Zhang, and Ying Cui. 2013. Low Complexity Delay-Constrained Beamforming for Multi-User MIMO Systems With Imperfect CSIT. *IEEE Transactions on Signal Processing* 61, 16, 4090–4099. doi:10.1109/TSP.2013.2264058

[60] Ruth W Leemis, Norah Friar, Srijana Khatiwada, May S Chen, Marcie-jo Kresnow, Sharon G Smith, Sharon Caslin, and Kathleen C Basile. 2022. The national intimate partner and sexual violence survey: 2016/2017 report on intimate partner violence. (2022). https://stacks.cdc.gov/view/cdc/124646

[61] David Leimstädtner, Peter Sörries, and Claudia Müller-Birn. 2022. Unfolding Values through Systematic Guidance: Conducting a Value-Centered Participatory Workshop for a Patient-Oriented Data Donation. In *Proceedings of Mensch Und Computer 2022*. Association for Computing Machinery, New York, NY, USA, 477–482. doi:10.1145/3543758.3547560

[62] Juniper L. Lovato, Antoine Allard, Randall Harp, Jeremiah Onaolapo, and Laurent Hébert-Dufresne. 2022. Limits of Individual Consent and Models of Distributed Consent in Online Social Networks. In *Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency* (Seoul, Republic of Korea) *(FAccT '22)*. Association for Computing Machinery, New York, NY, USA, 2251–2262. doi:10.1145/3531146.3534640

[63] Xi Lu, Jacquelyn E Powell, Elena Agapie, Yunan Chen, and Daniel A. Epstein. 2024. Unpacking the Lived Experience of Collaborative Pregnancy Tracking. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '24)*. Association for Computing Machinery, New York, NY, USA, Article 815, 17 pages. doi:10.1145/3613904.3642652

[64] Ewa Luger and Tom Rodden. 2013. An informed view on consent for UbiComp. In *Proceedings of the 2013 ACM International Joint Conference on Pervasive and Ubiquitous Computing* (Zurich, Switzerland) *(UbiComp '13)*. Association for Computing Machinery, New York, NY, USA, 529–538. doi:10.1145/2493432.2493446

[65] Célestin Matte, Nataliia Bielova, and Cristiana Santos. 2020. Do Cookie Banners Respect my Choice? : Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework. In *2020 IEEE Symposium on Security and Privacy (SP)*. 791–809. doi:10.1109/SP40000.2020.00076

[66] Brian James McInnis, Ramona Pindus, Daniah Kareem, Savannah Gamboa, and Camille Nebeker. 2024. Exploring the Future of Informed Consent: Applying a Service Design Approach. *Proceedings of the ACM on Human-Computer Interaction* 8, CSCW1, 1–31.

[67] D. Kim Rossmo Michelle V. Hauge, Mark D. Stevenson and Steven C. Le Comber. 2016. Tagging Banksy: using geographic profiling to investigate a modern art mystery. *Journal of Spatial Science* 61, 1, 185–190. arXiv:https://doi.org/10.1080/14498596.2016.1138246 doi:10.1080/14498596.2016.1138246

[68] Lynette I Millett, Batya Friedman, and Edward Felten. 2001. Cookies and web browser design: Toward realizing informed consent online. In *Proceedings of the SIGCHI conference on Human factors in computing systems*. 46–52.

[69] Andreas Müller and Peter Schaber. 2018. *The Routledge handbook of the ethics of consent*. Routledge New York.

[70] János Mészáros and Chih hsing Ho. 2018. Big Data and Scientific Research: The Secondary Use of Personal Data under the Research Exemption in the GDPR. *Hungarian Journal of Legal Studies AHistA* 59, 4, 403 – 419. doi:10.1556/2052.2018.59.4.5

[71] Gabriel Nicholas. 2020. Taking it with you: platform barriers to entry and the limits of data portability. *Mich. Tech. L. Rev.* 27, 263. doi:10.36645/mtlr.27.2.taking

[72] Philip J. Nickel. 2019. *The Ethics of Uncertainty for Data Subjects*. Springer International Publishing, Cham. 55–74 pages. doi:10.1007/978-3-030-04363-6_4

[73] Helen Nissenbaum. 2004. Privacy as contextual integrity. *Washington Law Review* 79, 1, 119–157. https://nyuscholars.nyu.edu/en/publications/privacy-as-contextual-integrity

[74] Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger, and Lalana Kagal. 2020. Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–13. doi:10.1145/3313831.3376321

[75] Jonathan A. Obar and Anne Oeldorf-Hirsch. 2020. The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society* 23, 1, 128–147. arXiv:https://doi.org/10.1080/1369118X.2018.1486870 doi:10.1080/1369118X.2018.1486870

[76] University of Wollongong. 2020. AI Research to Aid Women's Safety on Public Transport. https://www.uow.edu.au/media/2020/ai-research-to-aid-womens-safety-on-public-transport.php. Accessed: October 28, 2024.

[77] Jakob Ohme and Theo Araujo. 2022. Digital data donations: A quest for best practices. *Patterns* 3, 4. doi:doi:10.1016/j.patter.2022.100467

[78] Jakob Ohme, Theo Araujo, Laura Boeschoten, Deen Freelon, Nilam Ram, Byron B. Reeves, and Thomas N. Robinson. 2024. Digital Trace Data Collection for Social Media Effects Research: APIs, Data Donation, and (Screen) Tracking. *Communication Methods and Measures* 18, 2, 124–141. arXiv:https://doi.org/10.1080/19312458.2023.2181319 doi:10.1080/19312458.2023.2181319

[79] Jakob Ohme, Theo Araujo, Claes H. de Vreese, and Jessica Taylor Piotrowski. 2021. Mobile data donations: Assessing self-report accuracy and sample biases with the iOS Screen Time function. *Mobile Media & Communication* 9, 2, 293–313. arXiv:https://doi.org/10.1177/2050157920959106 doi:10.1177/2050157920959106

[80] Geneviève Paquette, Alexa Martin-Storey, Manon Bergeron, Jacinthe Dion, Isabelle Daigneault, Martine Hébert, Sandrine Ricci, and Sonn Castonguay-Khounsombath. 2021. Trauma Symptoms Resulting From Sexual Violence Among Undergraduate Students: Differences Across Gender and Sexual Minority Status. *Journal of Interpersonal Violence* 36, 17-18, NP9226–NP9251. arXiv:https://doi.org/10.1177/0886260519853398 doi:10.1177/0886260519853398 PMID: 31195873.

[81] Emmi Parviainen and Marie Louise Juul Søndergaard. 2020. Experiential Qualities of Whispering with Voice Assistants. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–13. doi:10.1145/3313831.3376187

[82] David Peloquin, Michael DiMaio, Barbara Bierer, and Mark Barnes. 2020. Disruptive and avoidable: GDPR challenges to secondary research uses of data. *European Journal of Human Genetics* 28, 6, 697–705. doi:10.1038/s41431-020-0596-x

[83] Nico Pfiffner and Thomas. N. Friemel. 2023. Leveraging Data Donations for Communication Research: Exploring Drivers Behind the Willingness to Donate. *Communication Methods and Measures* 17, 3, 227–249. arXiv:https://doi.org/10.1080/19312458.2023.2176474 doi:10.1080/19312458.2023.2176474

[84] Valérie Pijlman, Veroni Eichelsheim, Antony Pemberton, and Mijke de Waardt. 2023. "Sometimes It Seems Easier to Push It Away": A Study Into the Barriers to Help-Seeking for Victims of Sexual Violence. *Journal of Interpersonal Violence* 38, 11-12, 7530–7555. arXiv:https://doi.org/10.1177/08862605221147064 doi:10.1177/08862605221147064 PMID: 36710513.

[85] Barbara Prainsack. 2019. Data donation: How to resist the iLeviathan. *The ethics of medical data donation*, 9–22. doi:10.1007/978-3-030-04363-6_2

[86] Casey Randazzo, Carol F. Scott, Rosanna Bellini, Tawfiq Ammari, Michael Ann Devito, Bryan Semaan, and Nazanin Andalibi. 2023. Trauma-Informed Design: A Collaborative Approach to Building Safer Online Spaces. In *Companion Publication of the 2023 Conference on Computer Supported Cooperative Work and Social Computing* (Minneapolis, MN, USA) *(CSCW '23 Companion)*. Association for Computing Machinery, New York, NY, USA, 470–475. doi:10.1145/3584931.3611277

[87] Afsaneh Razi, Ashwaq Alsoubai, Seunghyun Kim, Nurun Naher, Shiza Ali, Gianluca Stringhini, Munmun De Choudhury, and Pamela J. Wisniewski. 2022. Instagram Data Donation: A Case Study on Collecting Ecologically Valid Social Media Data for the Purpose of Adolescent Online Risk Detection. In *Extended Abstracts of the 2022 CHI Conference on*

Human Factors in Computing Systems (New Orleans, LA, USA) *(CHI EA '22)*. Association for Computing Machinery, New York, NY, USA, Article 39, 9 pages. doi:10.1145/3491101.3503569

[88] Afsaneh Razi, Seunghyun Kim, Ashwaq Alsoubai, Gianluca Stringhini, Thamar Solorio, Munmun De Choudhury, and Pamela J. Wisniewski. 2021. A Human-Centered Systematic Literature Review of the Computational Approaches for Online Sexual Risk Detection. *Proc. ACM Hum.-Comput. Interact.* 5, CSCW2, Article 465, 38 pages. doi:10.1145/3479609

[89] Afsaneh Razi, John S. Seberger, Ashwaq Alsoubai, Nurun Naher, Munmun De Choudhury, and Pamela J. Wisniewski. 2024. Toward Trauma-Informed Research Practices with Youth in HCI: Caring for Participants and Research Assistants When Studying Sensitive Topics. *Proc. ACM Hum.-Comput. Interact.* 8, CSCW1, Article 134, 31 pages. doi:10.1145/3637411

[90] Janine Rowse, Caroline Bolt, and Sanjeev Gaya. 2020. Swipe right: the emergence of dating-app facilitated sexual assault. A descriptive retrospective audit of forensic examination caseload in an Australian metropolitan service. *Forensic Science, Medicine and Pathology* 16, 71–77. https://doi.org/10.1007/s12024-019-00201-7

[91] Muhammad Yasir Sarosh, Muhammad Abdullah Yousaf, Mair Muteeb Javed, and Suleman Shahid. 2016. MehfoozAurat: Transforming Smart Phones into Women Safety Devices Against Harassment. In *Proceedings of the Eighth International Conference on Information and Communication Technologies and Development* (Ann Arbor, MI, USA) *(ICTD '16)*. Association for Computing Machinery, New York, NY, USA, Article 61, 4 pages. doi:10.1145/2909609.2909645

[92] Kelsea Schulenberg, Lingyuan Li, Caitlin Lancaster, Douglas Zytko, and Guo Freeman. 2023. "We Don't Want a Bird Cage, We Want Guardrails": Understanding & Designing for Preventing Interpersonal Harm in Social VR through the Lens of Consent. *Proc. ACM Hum.-Comput. Interact.* 7, CSCW2, Article 323, 30 pages. doi:10.1145/3610172

[93] Britta Schulte and Eva Hornecker. 2020. Full Frontal Intimacy - on HCI, Design & Intimacy. In *Companion Publication of the 2020 ACM Designing Interactive Systems Conference* (Eindhoven, Netherlands) *(DIS' 20 Companion)*. Association for Computing Machinery, New York, NY, USA, 123–129. doi:10.1145/3393914.3395889

[94] Carol F Scott, Gabriela Marcu, Riana Elyse Anderson, Mark W Newman, and Sarita Schoenebeck. 2023. Trauma-Informed Social Media: Towards Solutions for Reducing and Healing Online Harm. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (Hamburg, Germany) *(CHI '23)*. Association for Computing Machinery, New York, NY, USA, Article 341, 20 pages. doi:10.1145/3544548.3581512

[95] William Seymour, Mark Cote, and Jose Such. 2023. Legal Obligation and Ethical Best Practice: Towards Meaningful Verbal Consent for Voice Assistants. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (Hamburg, Germany) *(CHI '23)*. Association for Computing Machinery, New York, NY, USA, Article 166, 16 pages. doi:10.1145/3544548.3580967

[96] Anya Skatova and James Goulding. 2019. Psychology of personal data donation. *PloS one* 14, 11, e0224240. https://doi.org/10.1371/journal.pone.0224240

[97] Luke Sloan, Curtis Jessop, Tarek Al Baghal, and Matthew Williams. 2020. Linking Survey and Twitter Data: Informed Consent, Disclosure, Security, and Archiving. *Journal of Empirical Research on Human Research Ethics* 15, 1-2, 63–76. arXiv:https://doi.org/10.1177/1556264619853447 doi:10.1177/1556264619853447 PMID: 31220995.

[98] Daniel J. Solove. 2013. Introduction: Privacy Self-Management And The Consent Dilemma. *Harvard Law Review* 126, 7, 1880–1903. http://www.jstor.org/stable/23415060

[99] Laura Somaini. 2018. The right to data portability and user control: ambitions and limitations. *MediaLaws: Rivista di Diritto dei Media* 3, 164–190. https://www.medialaws.eu/wp-content/uploads/2019/05/8.-Somaini.pdf

[100] Ciara Staunton, Santa Slokenberga, and Deborah Mascalzoni. 2019. The GDPR and the research exemption: considerations on the necessary safeguards for research biobanks. *European Journal of Human Genetics* 27, 8, 1159–1167. https://doi.org/10.1038/s41431-019-0386-5

[101] Veronika Strotbaum, Monika Pobiruchin, Björn Schreiweis, Martin Wiesner, and Brigitte Strahwald. 2019. Your data is gold – Data donation for better healthcare? *it - Information Technology* 61, 5-6, 219–229. doi:doi:10.1515/itit-2019-0024

[102] Erin C. Tansill, Katie M. Edwards, Megan C. Kearns, Christine A. Gidycz, and Karen S. Calhoun. [n. d.]. The mediating role of trauma-related symptoms in the relationship between sexual victimization and physical health symptomatology in undergraduate women. *Journal of Traumatic Stress* 25, 1, 79–85. arXiv:https://onlinelibrary.wiley.com/doi/pdf/10.1002/jts.21666 doi:10.1002/jts.21666

[103] Sarah Turner, July Galindo Quintero, Simon Turner, Jessica Lis, and Leonie Maria Tanczer. 2021. The exercisability of the right to data portability in the emerging Internet of Things (IoT) environment. *New Media & Society* 23, 10, 2861–2881. arXiv:https://doi.org/10.1177/1461444820934033 doi:10.1177/1461444820934033

[104] Sarah Turner and Leonie Maria Tanczer. 2024. In principle vs in practice: User, expert and policymaker attitudes towards the right to data portability in the internet of things. *Computer Law & Security Review* 52, 105912. doi:10.1016/j.clsr.2023.105912

[105] European Union. 2016. 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). *Official Journal of the European Union*

L119 (May 4 2016), 1–88.

[106] European Union. 2016. Right to data portability. General Data Protection Regulation (GDPR). Accessed: 2024-10-29.

[107] European Union. 2022. Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act). *Official Journal of the European Union* L152 (June 3 2022), 1–44. https://eur-lex.europa.eu/eli/reg/2022/868/oj/eng

[108] Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. 2019. (Un)informed Consent: Studying GDPR Consent Notices in the Field. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (London, United Kingdom) *(CCS '19)*. Association for Computing Machinery, New York, NY, USA, 973–990. doi:10.1145/3319535.3354212

[109] Julie L. Valentine, Leslie W. Miles, Kristen Mella Hamblin, and Aubrey Worthen Gibbons. 2023. Dating App Facilitated Sexual Assault: A Retrospective Review of Sexual Assault Medical Forensic Examination Charts. *Journal of Interpersonal Violence* 38, 9-10, 6298–6322. arXiv:https://doi.org/10.1177/08862605221130390 doi:10.1177/08862605221130390 PMID: 36310506.

[110] Irene I. van Driel, Anastasia Giachanou, J. Loes Pouwels, Laura Boeschoten, Ine Beyens, and Patti M. Valkenburg. 2022. Promises and Pitfalls of Social Media Data Donations. *Communication Methods and Measures* 16, 4, 266–282. arXiv:https://doi.org/10.1080/19312458.2022.2109608 doi:10.1080/19312458.2022.2109608

[111] Rebecca Wald, Johanna M.F. Van Oosten, Jessica T. Piotrowski, and Theo Araujo. 2024. Smart Speaker Data Donations in Families: The Project Rosie Perspective. In *Proceedings of the 23rd Annual ACM Interaction Design and Children Conference* (Delft, Netherlands) *(IDC '24)*. Association for Computing Machinery, New York, NY, USA, 680–685. doi:10.1145/3628516.3659374

[112] John Wilbanks and Stephen H Friend. 2016. First, design for data sharing. *Nature biotechnology* 34, 4, 377–379. https://doi.org/10.1038/nbt.3516

[113] Lauren Wilcox, Robin Brewer, and Fernando Diaz. 2023. AI Consent Futures: A Case Study on Voice Data Collection with Clinicians. *Proc. ACM Hum.-Comput. Interact.* 7, CSCW2, Article 316, 30 pages. doi:10.1145/3610107

[114] Janis Wong and Tristan Henderson. 2018. How Portable is Portable? Exercising the GDPR's Right to Data Portability. In *Proceedings of the 2018 ACM International Joint Conference and 2018 International Symposium on Pervasive and Ubiquitous Computing and Wearable Computers* (Singapore, Singapore) *(UbiComp '18)*. Association for Computing Machinery, New York, NY, USA, 911–920. doi:10.1145/3267305.3274152

[115] Janis Wong and Tristan Henderson. 2019. The right to data portability in practice: exploring the implications of the technologically neutral GDPR. *International Data Privacy Law* 9, 3, 173–191. arXiv:https://academic.oup.com/idpl/article-pdf/9/3/173/31063862/ipz008.pdf doi:10.1093/idpl/ipz008

[116] Chaeyoon Yoo and Paul Dourish. 2021. Anshimi: Women's Perceptions of Safety Data and the Efficacy of a Safety Application in Seoul. *Proc. ACM Hum.-Comput. Interact.* 5, CSCW1, Article 147, 21 pages. doi:10.1145/3449221

[117] Savvas Zannettou, Olivia Nemes-Nemeth, Oshrat Ayalon, Angelica Goetzen, Krishna P. Gummadi, Elissa M. Redmiles, and Franziska Roesner. 2024. Analyzing User Engagement with TikTok's Short Format Video Recommendations using Data Donations. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '24)*. Association for Computing Machinery, New York, NY, USA, Article 731, 16 pages. doi:10.1145/3613904.3642433

[118] Savvas Zannettou, Olivia-Nemes Nemeth, Oshrat Ayalon, Angelica Goetzen, Krishna Gummadi, Elissa M Redmiles, and Franziska Roesner. 2023. Leveraging rights of data subjects for social media analysis: Studying TikTok via data donations. *arXiv preprint arXiv:2301.04945*. https://arxiv.org/abs/2301.04945

[119] Eric Zeng and Franziska Roesner. 2019. Understanding and Improving Security and Privacy in Multi-User Smart Homes: A Design Exploration and In-Home User Study. In *28th USENIX Security Symposium (USENIX Security 19)*. USENIX Association, Santa Clara, CA, 159–176. https://www.usenix.org/conference/usenixsecurity19/presentation/zeng

[120] Wenqi Zheng, Emma Walquist, Isha Datey, Xiangyu Zhou, Kelly Berishaj, Melissa Mcdonald, Michele Parkhill, Dongxiao Zhu, and Douglas Zytko. 2023. Towards Trauma-Informed Data Donation of Sexual Experience in Online Dating to Improve Sexual Risk Detection AI. In *Adjunct Proceedings of the 36th Annual ACM Symposium on User Interface Software and Technology* (San Francisco, CA, USA) *(UIST '23 Adjunct)*. Association for Computing Machinery, New York, NY, USA, Article 39, 3 pages. doi:10.1145/3586182.3616689

[121] Wenqi Zheng, Emma Walquist, Isha Datey, Xiangyu Zhou, Kelly Berishaj, Melissa Mcdonald, Michele Parkhill, Dongxiao Zhu, and Douglas Zytko. 2024. "It's Not What We Were Trying to Get At, but I Think Maybe It Should Be": Learning How to Do Trauma-Informed Design with a Data Donation Platform for Online Dating Sexual Violence. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '24)*. Association for Computing Machinery, New York, NY, USA, Article 743, 15 pages. doi:10.1145/3613904.3642045

[122] Haozhe Zhou, Mayank Goel, and Yuvraj Agarwal. 2024. Bring Privacy To The Table: Interactive Negotiation for Privacy Settings of Shared Sensing Devices. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '24)*. Association for Computing Machinery, New York, NY, USA, Article 770,

22 pages. doi:10.1145/3613904.3642897

[123] Jonathan Zong. 2020. From individual consent to collective refusal: changing attitudes toward (mis)use of personal data. *XRDS* 27, 2, 26–29. doi:10.1145/3433140

[124] Douglas Zytko and Nicholas Furlo. 2023. Online Dating as Context to Design Sexual Consent Technology with Women and LGBTQ+ Stakeholders. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (Hamburg, Germany) *(CHI '23)*. Association for Computing Machinery, New York, NY, USA, Article 339, 17 pages. doi:10.1145/3544548.3580911

[125] Douglas Zytko, Nicholas Furlo, Bailey Carlin, and Matthew Archer. 2021. Computer-Mediated Consent to Sex: The Context of Tinder. *Proc. ACM Hum.-Comput. Interact.* 5, CSCW1, Article 189, 26 pages. doi:10.1145/3449288

[126] Douglas Zytko, Jane Im, and Jonathan Zong. 2022. Consent: A Research and Design Lens for Human-Computer Interaction. In *Companion Publication of the 2022 Conference on Computer Supported Cooperative Work and Social Computing* (Virtual Event, Taiwan) *(CSCW'22 Companion)*. Association for Computing Machinery, New York, NY, USA, 205–208. doi:10.1145/3500868.3561201

[127] Douglas Zytko, Nicholas Mullins, Shelnesha Taylor, and Richard H. Holler. 2022. Dating Apps Are Used for More Than Dating: How Users Disclose and Detect (Non-)Sexual Interest in People-Nearby Applications. *Proc. ACM Hum.-Comput. Interact.* 6, GROUP, Article 30, 14 pages. doi:10.1145/3492849

Received October 2024; revised April 2025; accepted August 2025