HAL open science

“I thought you were okay”: Participatory Design with Young Adults to Fight Multiparty Privacy Conflicts in Online Social Networks

Kavous Salehzadeh Niksirat, Evanne Anthoine-Milhomme, Samuel Randin, Kévin Huguenin, Mauro Cherubini

To cite this version:

Kavous Salehzadeh Niksirat, Evanne Anthoine-Milhomme, Samuel Randin, Kévin Huguenin, Mauro Cherubini. “I thought you were okay”: Participatory Design with Young Adults to Fight Multiparty Privacy Conflicts in Online Social Networks. Designing Interactive Systems Conference (DIS), ACM, Jun 2021, Virtual event, United States. 10.1145/3461778.3462040 . hal-03195167

HAL Id: hal-03195167

https://hal.science/hal-03195167v1

Submitted on 25 Apr 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution - NonCommercial - NoDerivatives 4.0 International License

"I thought you were okay": Participatory Design with Young Adults to Fight Multiparty Privacy Conflicts in Online Social Networks

KAVOUS SALEHZADEH NIKSIRAT, University of Lausanne, Switzerland
EVANNE ANTHOINE-MILHOMME*, University of Lausanne, Switzerland
SAMUEL RANDIN*, University of Lausanne, Switzerland
KÉVIN HUGUENIN, University of Lausanne, Switzerland
MAURO CHERUBINI, University of Lausanne, Switzerland

Although sharing multimedia content on online social networks (OSNs) has many benefits, publishing photos or videos of other people—without obtaining permission—can cause multiparty privacy conflicts (MPCs). Early studies developed technical solutions and dissuasive approaches to address MPCs. However, none of these studies involved, in the design process, the OSN users who have experienced MPCs. Hence, they possibly overlooked the valuable experiences these individuals have accrued. To fill this gap, we recruited participants specifically from this population of users, and we involved them in participatory design sessions to find solutions to reduce the incidence of MPCs. To frame the activities of our participants, we borrowed terminology and concepts from a well-known framework used in the justice systems. Over the course of several design sessions, our participants designed 10 solutions to mitigate MPCs. The designed solutions are based on different mechanisms, including preventing MPCs from occurring, dissuading users from sharing, resolving the conflicts, and educating users about community standards. We discuss the open design and research opportunities suggested by the designed solutions and contribute an ideal workflow that synthesizes the best of each solution. We contribute to the innovation of privacy-enhancing technologies to limit the incidence of MPCs in OSNs.

CCS Concepts: • **Security and privacy → Usability in security and privacy**; • **Human-centered computing**;

Additional Key Words and Phrases: interdependent privacy; multiparty privacy conflicts; privacy; social networking sites; participatory design; MPC

ACM Reference Format:
Kavous Salehzadeh Niksirat, Evanne Anthoine-Milhomme, Samuel Randin, Kévin Huguenin, and Mauro Cherubini. 2021. "I thought you were okay": Participatory Design with Young Adults to Fight Multiparty Privacy Conflicts in Online Social Networks. In *Designing Interactive Systems Conference 2021 (DIS '21), June 28-July 2, 2021, Virtual Event, USA.* ACM, New York, NY, USA, 33 pages. https://doi.org/10.1145/3461778.3462040

1 INTRODUCTION

Social media has significantly developed, as the volume of interpersonal exchanges has increased exponentially in the last years [60]. Users are increasingly willing to share personal multimedia content, such as photos and videos on online social networks (OSNs). Although content sharing enables users to present themselves and gain attention [57, 86, 121], exposing other people can harm their privacy. One privacy-threatening behavior is the non-consensual sharing of

*Both authors contributed equally to the article.

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).
© 2021 Copyright held by the owner/author(s).
Manuscript submitted to ACM

co-owned content [70, 98]; content that belongs to an *uploader* who shares the content, and to one or several *data subjects* depicted in that content. Such non-consensual sharing can create interdependent privacy conflicts [29, 53] or so-called multiparty privacy conflicts (MPCs) [21, 116, 117].

MPCs are too prevalent [117]. For example, in a large-scale survey targeted at OSN users [117], most of the respondents reported experiencing an MPC at least once in their social media use. Users cause MPCs, as they like to share photos portraying others [78] and perceive group photos as less privacy-violating than photos where a single person is portrayed [48]. They also have less of a tendency to tag their friends [95] or obtain their consent before sharing [117]. There are many reasons that data subjects do not approve of MPCs [21, 117]. Some data subjects worry because they do not look good in the shared content, and others have concerns about private facts that can be deduced from the content, such as where, how, and with whom they were at the time the content was recorded.[1] The consequences of MPC can be severe. One out of every thirteen US adults deals with severe MPCs [21] that cause grave consequences, such as public shaming [69, 124], cyberbullying [23], and discrimination [43]. The most severe case of MPC is revenge pornography, where uploaders retaliate against their ex-partners by sharing intimate content after the relationship is over [73, 76]. Unfortunately, revenge pornography can even occur on general-purpose OSNs [28], and it can lead to dramatic situations [67].

Two main research streams have studied MPCs [117]. The first stream attempted to understand how users cope with privacy conflicts on OSNs, in general [71, 103, 130] or in particular, for MPCs [117]. Although these studies provide deep insights into user practices, they do not directly propose solutions to manage MPCs. The second stream includes studies that propose privacy-preserving solutions for OSNs. They provide either technical solutions [52, 55, 95, 115] or dissuasive strategies stemming from persuasion theories [6, 7, 21, 81]. These studies do not, however, place users at the heart of the design process, instead they propose solutions that do not necessarily consider users' real-life MPC experiences, attitudes, and behaviors in OSNs.

To address this research gap, we use the participatory design approach [61, 62]: a well-established methodology for co-designing with end-users in the early stages of the design process. We seek, in particular, to know what types of solutions will be suggested by users who have experienced an MPC, and at what stage the proposed solutions can address an MPC (e.g., prevention or support). We are also interested in knowing whether the participants who reported having caused an MPC (i.e., henceforth *MPC infringers*) would design solutions that differ from those who reported having suffered from an MPC (i.e., henceforth *MPC subjects*). At the same time, inspired by crime-prevention studies, we borrow a well-recognized framework to guide us in our participatory design practices. We explore existing practices in justice systems and use justifications for punishment (i.e., henceforth *justice strategies*), namely deterrence, incapacitation, rehabilitation, restoration, and retribution [20, 32, 85]. We believe these justice strategies have potential benefits for addressing MPCs, hence we use them as seeds, or inspirations, to guide us in our participatory design sessions. Until now, only a few of these strategies were used to manage MPCs (e.g., see the *Law Threat* strategy in [21], an approach based on deterrence). To the best of our knowledge, the use of these practices has not been studied in the MPC context. Last, we organized these design sessions with young adults because these users deal with MPCs more often than older adults [21].

In this study, we invited 26 MPC-experienced young adults to attend 16 design activities. We were interested in both types of participants: MPC infringers and MPC subjects. Our participants had a variety of experiences, ranging from mild to severe MPCs. The participants reflected on their personal experiences, thus created 21 solutions. Based on our

[1]Even in countries such as the United States, where photography in the public sphere can be taken and published without prior authorization [66], publishing someone's photo on social media can disclose private facts and could have negative consequences for the reputation of the data subjects [100].

expert evaluation and the feedback from participants, the ten best solutions were reviewed and are presented here. These solutions address MPCs from mild to severe consequences and with varying stages of impacts, including preventive, dissuasive, educative, and restorative approaches. In this paper, we provide insights and design ideas collected from non-technical—yet expert—young adults who have valuable real-life experiences with MPC. We contribute to the innovation of privacy-enhancing technologies that could be incorporated into the design of online social networks to reduce the incidence of MPCs.

We organized the rest of this paper as follows: In Section 2, we report the related work by describing two main streams of research relevant to MPC. In Section 3, we delineate and justify our research methodology and describe the types of participants recruited for the study. We also give background information on five main justice strategies used in participatory design sessions. In Section 4, we summarize the participants' design rationale and explain the selected solutions and the participants' evaluations of each solution. In conclusion, in Sections 5 and 6, we discuss the potential benefits and the implications of the designed solutions.

2 RELATED WORK

Multiparty privacy conflicts (MPCs) or interdependent privacy situations have been addressed through various research approaches (see the work [29, 53, 116] for comprehensive surveys on the topic). We consider two relevant privacy theories: (i) Based on contextual integrity [93], privacy is preserved when the information has a proper flow, depending on the context, and it is violated when information is propagated further outside of this context (i.e., with different norms). (ii) Based on communication privacy-management theory [99], when the owner of the information shares a piece of information, they define a set of rules to control collective boundaries with other individuals (i.e., co-owners). The privacy violation, or so-called boundary turbulence, occurs if the co-owner discloses the information outside of these defined boundaries. In this section, we first describe related studies on understanding the way users develop their own strategies for dealing with privacy conflicts in OSNs. Second, we present the summary of solutions developed to address privacy conflicts in OSNs.

2.1 Coping Strategies on OSNs

Building upon the notion of boundary regulation [5, 96] and the principle of *co-ownership* in the communication privacy management theory [99], empirical studies investigated how OSN users spontaneously create manual strategies to manage their privacy. For example, Lampinen et al. [71] present a framework showing that OSN users usually correct or prevent privacy conflicts in two different manners: individually (e.g., adjusting privacy settings) or collaboratively (e.g., asking another person to delete content). The corrective, collaborative, and preventive strategies are also identified by the study of Cho and Filippova [22]. In general, the literature identifies the following strategies enacted by OSN users to deal with MPCs: (i) deliberately anticipate the consequences of non-consensual sharing and avoid it [71], (ii) ask for consent before sharing [71, 102], or (iii) practice self-control to reduce time spent on OSNs [22, 131]. Users also report regulating their actions in real-life settings (e.g., avoiding getting drunk at a party) to reduce the risk of being caught in inconvenient pictures that could end up online [13, 71]. Other studies identify practices where users attempt to discourage uploaders from sharing. For instance, in the case of non-consensual sharing, they negotiate [13, 71, 102, 130] or use sanctioning strategies [103]. More relevant to MPC, a recent study [117] lists practices reported by MPC infringers to resolve MPC by discussing with MPC subjects, apologizing, and by cropping or deleting the troubling content. Note that users' privacy and security practices can be changed. For example, OSN users' perceived information sensitivity [128], their values [24], attitudes [24, 74, 94], technical experiences [94], and cultural background [30, 122] can alter their practices.

The type of OSN can also influence these practices [24]. Although users' spontaneous coping strategies are not fully effective per se, understanding these practices served as an inspiration for researchers to design technologies to manage MPC.

2.2 Protective Mechanisms for OSNs

To protect OSN users, the following families of solutions were developed and tested in past literature: (i) item modification, (ii) audience modification, and (iii) deterrent approaches. The first two approaches use machine learning and computational techniques to modify the items in the photo or to limit the audiences. The third approach borrows techniques from persuasive-technology research to deter MPC infringers from sharing.

The first family of solutions uses face-recognition algorithms to recognize MPC subjects in the photo [1] then, to hide MPC subjects, it applies obfuscation techniques, such as blurring or masking the face [45]. Apart from item obfuscation, these researchers attempted to collect consent [95], to predict users' consent, based on their OSN behaviors [77], and to develop multiparty access control models [54, 55] for managing privacy conflicts. A new stream of research [46, 47, 79] also contributes to identifying the way to address aesthetic-related issues raised by item-modification techniques. The second family of solutions hides the content from undesired audiences, for instance, hiding family related content from friends in the colleague circle. To determine the 'undesired audiences', earlier studies relied on computational approaches to automate privacy decisions such as novel access-control models [49–52, 123, 129], recommender systems [35, 36], adaptive audience recommendations [114, 115], aggregated voting [19, 104, 119], a collaborative access-control system based on secret sharing [12], trust-based consent collection [2], and mechanisms for supporting co-owners' interactions in negotiating privacy settings [58, 59, 101]. Some of these studies were built upon theories such as the use of game theory for negotiation [101, 118], argumentation theory [35, 37, 63, 88, 90], and human-values theory [88–90].

Research on the third family of solutions is limited to a few studies [6, 7, 21, 81]. Cherubini et al. [21] developed dissuasive mechanisms to deter MPC infringers. They proposed solutions in the form of design frictions that warn users before sharing multimedia content. They presented a comparative analysis based on the desirability of dissuasive mechanisms versus technical solutions (i.e., item and audience modification approaches). Their results show that vulnerable users (e.g., young women) might prefer technical solutions, and that users who frequently share multimedia content might prefer dissuasive solutions because they can publish with less effort. Other researchers [7, 81] used nudges to influence users' sharing decisions. For instance, Masaki et al. [81] studied the effectiveness of different types of nudging strategies on non-consensual sharing in OSNs and found that nudges with negative framing can be deterrents in scenarios in which users do not have consensus about the scenarios.

In conclusion, all of these approaches were designed by expert designers, building upon existing theories. However, the research did not involve the end-users of OSNs in the design of such strategies. We believe this is a notable shortcoming, because any technological solution must be designed taking into account the user's current practices and the existing ecosystem. We contribute to overcome this omission by involving users of OSNs, who might have experienced or caused an MPC. Also, we involved younger adults in the solution design to the MPC problem because typically, compared with other age groups, these users have a higher level of engagement with this technology [21]. Therefore, we ask the following research questions:

RQ1. What solutions would young OSN users, who have experienced MPCs, co-design to address the problem of MPCs?

RQ2. What are the differences between solutions designed by MPC infringers and MPC subjects?

3 METHOD

We take a user-centric approach to design effective solutions for non-consensual multimedia sharing on OSNs. In particular, we involved young users of OSNs who either experienced or caused MPCs. To this end, we used a participatory design approach [61, 62, 107]. Participatory design has been widely used by earlier studies in human-computer interaction for purposes ranging from food-tracker design [80] to addressing the stigma in measuring blood-glucose levels [82], and to promoting the health of minority populations [113]. Recently, the participatory design was used to address issues related to OSNs such as cyberbullying [9, 14]. In this study, we conducted several sessions with users who are the main stakeholders of MPC: MPC infringers and MPC subjects. To promote participants' creativity and generate effective solutions, we practiced several participatory design activities such as 'focus groups', 'storyboarding', 'value ranking', and 'mutual evaluation'. In this section, we first explain the recruitment process and the characteristics of our participants. We then introduce a well-recognized framework in justice systems that have been used for crime prevention. We explored this framework in our participatory design practices to understand how it could be beneficial to design interventions for MPCs. Finally, we describe the design activities.

3.1 Recruitment

We used a participant pool from the University of Lausanne, which entails over 8,000 volunteers for behavioral experiments.[2] Most of the volunteers in the subject pool were students. An earlier study showed that young adults have the most susceptible user profiles for MPC [21]. The same study also identified women as vulnerable user types, where they reported being subject to MPC, significantly more than men were. Therefore, we recruited young adults who experienced (or caused) MPCs and we recruited more women than men. We targeted the age range of 18 to 25, but given the availability of the participants, we also considered participants older than 25.[3]

One month prior to the study, we sent invitations to all the participants in the pool; the invitation included a link to fill an online screener to check the eligibility of the participants for the study.[4] A total of 286 participants enrolled online for the study and were assessed for eligibility. We also used the online screener (cf. supplementary material A) to collect demographic information, to understand which online services and OSN platforms they use for multimedia sharing, and the frequency of sharing (or being shared in) co-owned multimedia material. We also collected information about the number of MPC incidents they were involved in over the last 12 months, and the severity of the experienced MPCs (i.e., MPCs with severe consequences such as public shaming and discrimination that could be related to nudity and sexual content).

We recruited only MPC infringers and MPC subjects. Given that these users are the two main types of stakeholders, we excluded participants without MPC experience or third-party viewers (i.e., those who witnessed MPCs via their relatives or friends, but who were not involved in an incident). Respondents of the screener who selected *never* for Q4 (i.e., never sharing co-owned content depicting others) and Q5 (i.e., never being depicted in co-owned content shared by others) were excluded. We also excluded those who selected *never* for Q8 (i.e., never made someone unhappy for privacy reasons about sharing co-owned content) and Q9 (i.e., never felt unhappy for privacy reasons about co-owned content shared by others). When selecting the sample, we maximized diversity on a best effort basis. We selected participants from various stages of young adulthood, with frequencies of sharing/being shared in co-owned content, and with diverse

[2] A specialized unit at our institution managed the subject pool, took care of the enrollment processes, automated the transfers of financial incentives, and kept secure the contact information of the study participants.
[3] Note that 18 to 40 is a standard age-range for "young adults", and it was used by several earlier studies [4, 83].
[4] All materials used in the study are available in an open science framework (OSF) accessible online at https://doi.org/10.17605/OSF.IO/ZXHF3.

frequencies and severities of MPCs (i.e., mild and severe). To ensure a mix of backgrounds and technical expertise, we also selected participants from several faculties at our university. We slightly over-recruited female participants in each experimental group, as explained above.

3.2 Participants

We selected 48 candidate participants out of the respondents who completed the screener and matched our profiles. We contacted the participants via e-mail and, according to their response and availability, we recruited $N = 26$ participants (17 women) for the study. The pre-study survey also served as criteria for grouping; we assigned 13 participants as *MPC Subject* and 13 participants as *MPC Infringer*. The grouping was done based on the answers provided for Q4–Q5 and Q8–Q11. All participants reported using either OSNs or instant messaging (IM) platforms to share photos and videos (IM: 84.6%, OSN: 80.7%). Some participants also mentioned using cloud repositories (23.1%), multimedia-sharing websites (15.4%), e-mails (11.5%), and personal websites (3.8%) to exchange multimedia content. Participants reported using a variety of platforms for multimedia sharing, including WhatsApp (96.1%), Instagram (76.9%), Snapchat (65.4%), Facebook (57.7%), Messenger (57.7%), Telegram (23.1%), iCloud (23.1%), TikTok (11.5%), YouTube (7.7%), Twitter (7.7%), and others (3.8%).

3.2.1 MPC Subjects. Of the 13 participants, eight were female and five were male.[5] The mean age of the participants was 23.3 (SD=5.9) ranging from 19 to 41. All MPC subjects were students (9 bachelor students and 3 master's students[6]), except for one female participant (41 years old) who was a brand manager working in a private company. The other MPC subjects belonged to different faculties such as engineering (4P, or 30.8%), social and political sciences (2P, 15.4%), computer and communication sciences (1P, 7.7%), geosciences and environment (1P, 7.7%), basic sciences (1P, 7.7%), business and economics (1P, 7.7%), biology and medicine (1P, 7.7%), and law and criminal sciences (1P, 7.7%). Participants reported being depicted in photos and videos by other individuals in OSNs, daily (6P, 46.1%), several times a month (4P, 30.8%), and a few times a year or less (3P, 23.1%). Most of the participants (8P, 61.5%) reported being unhappy three or more times for privacy reasons about a photo that someone had shared in OSNs (in the last 12 months). Whereas, others (5P, 38.5%) reported being unhappy only once or twice in the last year. Almost half of the MPC subjects (6P, 46.1%) reported being involved in MPCs with severe consequences (e.g., public shaming and discrimination) at least once in the previous year, where some participants (3P, 23.1%) reported that such consequences were related to nudity or sexual content. We assessed participants' post-traumatic stress disorder (PTSD) by using the PTSD Checklist for DSM-5 [125] to check if they had a mental health problem caused by any traumatic event such as a severe MPC.[7] Our results show that four participants (P2, P5, P10, P11) had moderate post-traumatic stress (32.3/80), whereas the others did not have such symptoms (15.3/80). The tables with all the demographic details of the study participants are available in the supplementary material B linked above.

Before starting the participatory design sessions, we asked the participants to answer a few open-ended questions about their last MPC incident. We asked all participants to explain, in particular, the content of the photo or video involved. We also asked MPC subjects why they were unhappy with the content and what consequences they faced, such as bullying, discrimination, or public shaming, due to the non-consensual sharing. We asked the MPC infringers about their motivation to share such content. Eleven participants reported MPC incidents caused by the sharing of photos or videos in which they were portrayed. They reported being unhappy because they did not look nice in the

[5]Even though we included a 'non-binary' option in the gender question (cf. Q1 of the screener, supplementary material A), no participant selected it.
[6]For brevity in the remainder of the article, we refer to the number of participant with the capital 'P'.
[7]The questionnaire includes 20 questions with a Likert scale from 0 to 4, and the total score varies between 0 and 80.

published content (4P, 36.4%) or because the content was published too broadly and they were afraid of what people they did not know would think (5P, 45.4%). [P7, male, 21 y.o.]: "*Someone shared a video of me drinking. My parents saw that video and I had problems at home. My family is fundamentally against drinking for religious reasons, and I have been hiding that side of me from them to avoid problems. I was ashamed in front of my parents, and had a conflict with them.*"; [P10, female, 19 y.o.]: "*In a video, I was dancing in a ridiculous and tendentious way. It was posted on an Instagram story by a friend. I got a bit of backlash from people from my school. My mom also saw the video, and we got into a big fight. I was unhappy because what I was doing in the video was destined for a small circle of friends, not for the Internet.*" Some participants also mentioned their desire to not appear on social media (3P, 27.2%) and to not lose control of their personal information (1P, 9.1%).

3.2.2 MPC Infringers. Nine participants were female and four were male. The mean age of the participants was 20.9 (SD=2.0), ranging from 18 to 26. All participants were students (8 bachelor students and 5 master's students). They belong to different faculties, including business and economics (5P, 38.5%), humanities (3P, 23.1%), engineering (2P, 15.4%), basic sciences (1P, 7.7%), social and political sciences (1P, 7.7%), and biology and medicine (1P, 7.7%). The infringer participants reported depicting other individuals by sharing photos or videos online using OSNs daily (1P, 7.7%), several times a month (9P, 69.2%), and a few times a year or less (3P, 23.1%). The majority of the MPC infringers (8P, 61.5%) reported making someone else unhappy three or more times by sharing photos or videos online (in the last 12 months). The remaining infringer participants (5P, 38.5%) reported the same phenomenon once or twice in the previous year. More than half of the participants (7P, 53.8%) reported causing MPCs with severe consequences, such as public shaming and discrimination, once or several times in the previous year (4P, 30.8%: more than three times; 3P, 23.1%: less than three times). Some participants (4P, 30.8%) reported causing consequences related to nudity or sexual content (1P, 7.7%: more than three times; 3P, 23.1%: less than three times).

Twelve participants described the incidents that caused the MPC. The participants' motivations for non-consensual sharing were to share a funny moment (6P, 50.0%), to make fun of MPC subjects (2P, 16.7%), to get revenge on a MPC subject (2P, 16.7%), to take advantage of a MPC subject (1P, 8.3%), and to snoop on a MPC subject (1P, 8.3%). [P25, female, 22 y.o.]: "*I was a bit selfish trying to share one of my friends' photos where I think she did not look as pretty as I did and then having people reacting to the picture and making compliments about me and not her.*"; [P21, male, 22 y.o.]: "*I went with my friends to a disco bar. I saw a friend of my friend far from me. I decided to take a photo of him and sent it to a friend who knows him. Just a few seconds later he received my snap, and he wrote to this guy [MPC subject]. Then he came to me asking me 'why did you take a picture of me and shared it? I have children and I don't want to be filmed here.'* "

3.3 Justice Framework

The justice framework, which is relevant to this research, is typically used to deal with behaviors that lead to conflictual interactions between individuals or that cause harm to others. Punishments are negative sanctions assigned by legal officials, such as government agencies or judges, to discourage deviant behavior [27, p. 32]. Overall, the results of the philosophical reflections on legal punishments are five justice strategies, that is, deterrence, incapacitation, rehabilitation, restoration, and retribution [20, 32, 85]. Table 1 summarizes these five justice strategies. Some have a long history (e.g., retribution) [3]. Whereas, others are quite modern approaches that support both wrongdoers and victims, after the offense has occurred (e.g., restoration). Although some of these justice strategies, such as incapacitation and deterrence, can be effective for *irrational* and *rational* actors, respectively, others, such as restoration, are quite useful for *virtuous*

Table 1. Summary of the Justice Framework

Title	Definition	Additional notes
Deterrence	The threat of punishment to avoid a crime before it happens. The two main forms are specific and general deterrence [91, 106].	The specific deterrence aims at deterring an offender from further misconduct (e.g., giving a ticket to a driver who breaks the law). The general deterrence aims at creating public awareness to warn society (e.g., media coverage relative to increasing traffic ticket fines).
Incapacitation	Limiting the physical capacity of offenders to avoid committing deviant behavior [132].	In its traditional form, incapacitation is the removal of offenders from society to prevent future crimes and includes incarceration (e.g., jail, prison) and probation (e.g., house detention, supervised release).
Rehabilitation	Re-educating offenders to overcome factors that have led them to commit a crime [3, 105].	It is a pedagogical approach proposed in 1949 and that aims at changing offenders' behaviors and re-integrating them into society by developing occupational skills or resolving psychological issues.
Restoration	Mediation between victims and offenders to repair the harm [20, 109, 112].	It is the most recent justice strategy. It serves as an opportunity for the victim to be heard and to ask questions. It also enables the offender to make amends and receive forgiveness, to 'repair' the wrong.
Retribution	The most traditional strategy, built on the principle of "an eye for an eye" [18, 87].	It emphasizes that a person who breaks the law should in turn suffer the same harm. In this approach, the level of punishment should be proportionate to the severity of the offense.

and *socially responsible* actors such as young offenders who committed minor offenses [16]. We will explain the use of the justice framework later in Section 3.4.

3.4 Procedure

Our study design was inspired by earlier studies that used participatory design [9, 14, 82]. Prior to running the study, two of the authors did a dry run of the sessions with a (non-author) HCI practitioner from our institution to refine the study protocol.

Figure 1 shows the study procedure. Each participant attended two study sessions organized on two distinct days. We conducted 1st and 2nd sessions on different days because we required enough time to collect and review all solutions designed by the different groups and prepare them for the subsequent activities. Thus, we first finished all activities related to session 1 for all groups, and a week later, we conducted activities related to session 2. We organized the sessions in groups of six to seven participants. Based on prior guidelines [68], we felt that six to seven participants per session was the optimal size to facilitate discussion and group activities. Therefore, we organized participants into four groups: two groups of MPC infringers and two groups of MPC subjects. All the sessions were conducted in the same lab on the campus. MPC subjects and MPC infringers did not attend the same sessions. All of the sessions were conducted by at least two of the authors (i.e., one facilitator and one assistant). We did this because one of the authors had to focus on guiding the sessions and answering the questions while the other author helped with note-taking and recording the sessions. Participants read and signed the consent forms before the sessions. All sessions were conducted in English and they were audio- and video-recorded. Participants received the equivalent of 65 USD for their participation.

The sessions involved four main activities: *Focus Group*, *Storyboarding*, *Value Ranking*, and *Mutual Evaluation*. The activities of the first session supported the *ideation* of new strategies to contrast the occurrence of MPCs. These were *evaluated* through the activity of the second session. In the following paragraphs, we explain the procedure and our rationale for each of these parts.

3.4.1 Focus Group [Session 1, Activity 1]. Focus groups are often used in participatory design studies to ground the design activities and to facilitate brainstorming [9]. We started the session with introductions and by presenting the

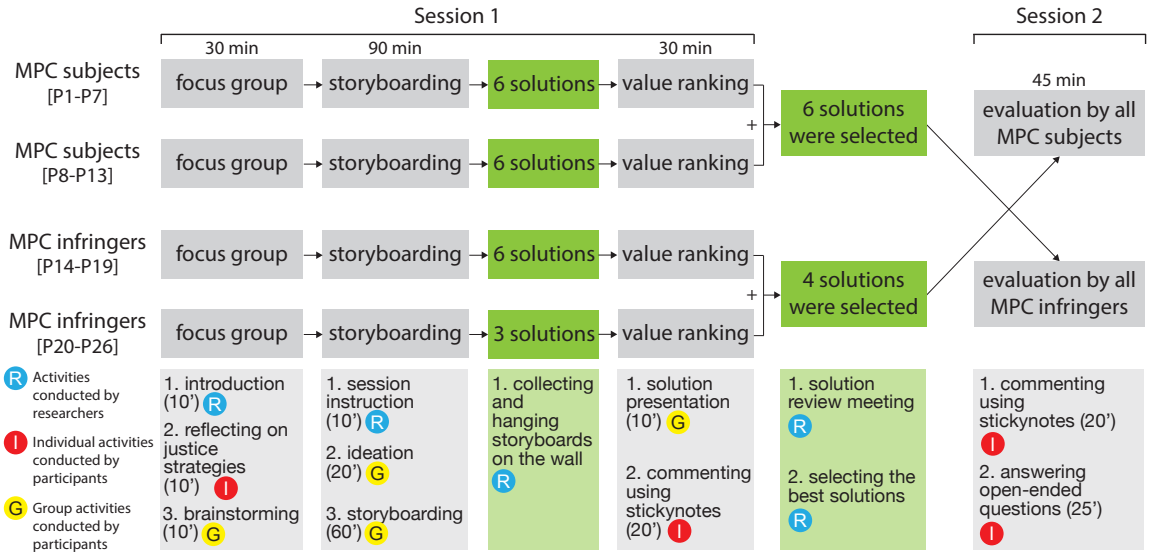
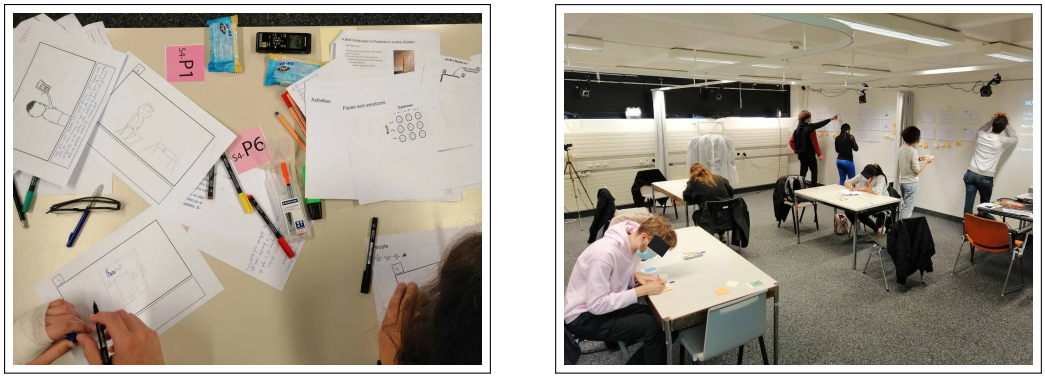


Fig. 1. Procedure of the study. The gray boxes represent activities while the green boxes the output of the activities. Color icons are used to indicate the subjects of each activity.

goal of the session to the participants. Then, we provided a brief description of MPCs and their consequences [21, 117]. To avoid biasing the participants we did not mention any existing solution to the problem of MPCs to the participants. We also did not discuss the privacy regulations of existing OSNs to avoid restricting the creativity of our participants.[8] In addition, following a methodology from an earlier study [82], we presented the framework of the justice system that is typically applied to deal with any misbehavior or felony [85]. The framework includes strategies and practices that are commonly used by the justice systems to reduce crime rates (cf. Section 3.3). We did this for two reasons: (i) to *center* the subsequent design activities around commonly accepted approaches that have been developed over the course of centuries and debated in philosophy and law studies; and (ii) to *ground* the language of the participants over well-defined concepts and approaches. The whole presentation took ~ 10 minutes.

As a warm-up sub-activity, and to encourage participants to reflect on the justice strategies, we asked them to individually create a list of pros and cons of the justice strategies, considering how each strategy could be adapted to the MPC context. This activity took ~ 10 minutes. Next, following prior research [14, 113], we grouped participants in subgroups of two or three[9] asking them to sit around a table, share their list with their group mates, and together brainstorm the advantages and disadvantages. Given that in the later stage (cf. Section 3.4.2), the participants in the same subgroups were supposed to work together on storyboards, the brainstorming activity was intended to help them to form a common design rationale. The activity took ~ 10 minutes, where participants first exchanged the lists with each other and then verbally discussed. At the end of the activity, we asked participants in each subgroup to wrap up the discussion by making a conclusion verbally.

[8]However, note that the participants likely took into account privacy regulations when proposing a solution (1) to determine what would be considered an MPC (mix of social norms and privacy regulations) and (2) which solution one could reasonably imagine being implemented and put in place.
[9]Participants were assigned to each subgroup randomly.



(a) Two participants drawing a storyboard.

(b) Participants evaluating solutions from the other group.

Fig. 2. Setup of the participatory design sessions.

3.4.2 Storyboarding session [Session 1, Activity 2]. As a *core* ideation activity, we employed storyboarding since it has been commonly employed as a participatory design activity [14, 113, 127]. Storyboarding is a visual narrative inquiry and a powerful storytelling technique to foster participant creativity. This technique allows researchers to study an experience and guide participants to design respective solutions using a story [10, 15, 25]. For this activity as well participants worked in subgroups. We first introduced the storyboarding technique to participants using a short slideshow. Then, we presented an example storyboard that had been drawn for a different context (i.e., using a smartphone to capture a bar code on an announcement board [42]). Later, we asked participants to craft two technological solutions (for each subgroup) to *dissuade*, *mitigate*, or *prevent* MPCs. These three concepts were derived directly from the justice framework introduced in activity 1. We let each subgroup decide freely which of these concepts to use to build their solution on.[10] We informed the participants that they could either design a feature incorporated inside an existing technology (e.g., a new feature in an existing OSN) or propose an independent technological solution (e.g., a novel application or service). We strove to set a constructive working environment by: (i) informing participants that their solutions were not going to be judged as correct or incorrect; and that (ii) their contribution could help design better solutions against MPCs.

Participants were asked to create one storyboard per solution using 5-8 canvases (Figure 2a). Participants were provided with A4 size templates (one page for each canvas), color pens, and color markers. Each A4 template contained three frames to note the number of each canvas, to make a drawing, and to add captions under the drawing.[11] Participants were asked to draw all necessary steps from A to Z in their storyboards including 'before sharing', 'when sharing', 'the intervention', and 'after the intervention'. They were also asked to give a title for their storyboard. At the end of the session, we collected and hung all of the storyboards on the walls in the room where the sessions were held. The participatory design sessions took ∼ 90 minutes in total. After four storyboarding sessions, we collected 21 design solutions (i.e., 12 from MPC subjects and 9 from MPC infringers).

3.4.3 Value Ranking [Session 1, Activity 3]. Evaluation activities are usually conducted at the end of participatory design sessions in order to help participants reflect on the design outcomes of the previous activities [9, 14, 82]. The

[10] Note that at the end of the study, seven solutions (or 70%) used one of these approaches. The remaining solutions used techniques that were not inspired by these concepts.

[11] The template of the canvas is available in the OSF repository.

purpose of this activity was to collect feedback from participants on the designed solutions. Particularly, we asked participants to think about the effectiveness of each solution in addressing the MPC problem and about any feasibility and implementation obstacle that could be encountered when implementing the solution. We asked a leader in each subgroup to shortly present their storyboard to the participants of the other subgroups. Next, we asked all participants to individually review all the storyboards (except for their own storyboards, see Figure 2b). More specifically, we asked participants to write their comments on sticky notes. We provided sticky notes of different colors for positive and negative remarks. As prompts, we asked participants to consider whether the solution could work in real-life situations, whether it could be usable, how it might impact different stakeholders, and whether it could be feasible to implement. To clarify what we meant by feasible, we provided an example of an infeasible solution: a time machine where the MPC infringer and MPC subject(s) can travel back in time, before the MPC happened. After the participants were done writing on the sticky notes, we had a short debriefing reviewing the comments and reflecting on the overall session. Then, we wrapped the session. This last activity took $\sim$ 30 minutes. Once pictures of the sticky notes were taken, these were removed from the storyboards for the activities of the second session.

At the end of the first session activities, three of the authors (familiar with the MPC literature) reviewed each solution designed by the participants. The goal of this review was to remove redundant solutions and to bring the designs to a manageable set that could be further discussed and refined in the upcoming session.[12] To select a subset of solutions, we considered the following points: a. whether the solution was *redundant* with regard to a previous solution; b. whether the solution *existed already* in OSNs; c. whether it would be *ethically viable* (e.g., not exposing the MPC subject to retaliation); d. whether the solution was *technically feasible*; e. whether it was not specific to the problem of MPCs. We then reviewed the positive and negative remarks collected via sticky notes, and discussed those remarks before making the final decision. Last, the three authors voted independently for all solutions. Each author could vote "keep" or "discard". As a result, we selected 10 solutions out of 21 storyboards for the second session (6 from MPC subjects and 4 from MPC infringers) and discarded the remaining ones. We discarded 11 solutions for the following reasons: 6 solutions for being redundant; 2 solution as they already existed in OSNs; 1 solution for not complying with our ethical assessment; 1 solution for being infeasible from a technical standpoint. Finally, we removed 1 additional solution as it was not specific to the problem of MPCs.

3.4.4 Mutual Evaluation [Session 2, Activity 4]. The designs of the first session were prepared by homogeneous types of participants: either MPC subjects or MPC infringers. As solutions impact both kinds of users, the activity of the second session was aimed at collecting feedback from the opposite types of participants (i.e., MPC subjects evaluated the solutions designed by MPC infringers and vice versa). We did this because the designs developed by one type of stakeholder might have not adequately considered the needs of other types of stakeholders. For instance, an MPC subject might be interested in threatening or punishing severely the attacker without understanding the motivations that initiated the MPC or the burden it would put on legitimate uploads. An MPC infringer could also provide very mild interventions that could not be effective to prevent MPCs. To mitigate this, each solution was reviewed and commented on by participants of the opposite type.

To avoid biasing the participants, we did not mention the identity of the designers of the solutions. Participants were asked to go individually through the storyboards, look at each drawing and read their captions carefully, and list the pros and cons of each solution by adding sticky notes to the walls. After this short warm-up activity, we asked

[12] At this stage, due to the lack of time between the first and second sessions, we refrained from using a systematic analytic approach (e.g., Thematic Analysis [17]). Instead, we organized a design review meeting that allowed the researchers to make quick reflections on the proposed solutions.

participants to fill in a questionnaire including four open-ended questions (cf. supplementary material C in the OSF repository). We asked participants to identify a. whether a particular solution could help to fight against MPC and in what ways it has an effect on MPC, b. to what extent this solution could support them as an MPC subject and could help them not cause MPC (as an MPC infringer), c. whether a particular solution could work in real-life scenarios, and d. how a particular solution could be improved. At the end of the session, we thanked participants for their participation. The activity of the second session lasted ∼ 45 minutes.

3.5 Analysis

We used thematic analysis [17] to study the content of the conversation that participants had during the focus group sessions. The analysis started with transcribing the data and then reading and coding the data in an iterative manner. Two authors worked together on data analysis, identifying over 200 codes that led to generating three main themes for the design rationale (cf. Section 4.1). We also used affinity diagramming [108] to analyze the participants' feedback on each solution. We combined the answers collected via sticky notes and the answers given to the open-ended questions described above (we will refer collectively to this qualitative feedback as *comments*). In total, we extracted 685 comments during the sessions. Of these, 172 were extracted from the sticky notes, and 513 from the open-ended questions. The number of comments per solution ranged from 64 to 74 ($median = 68.5$). Next, we grouped the comments and generated 3 to 6 clusters ($median = 5$) for each solution. These clusters were used to summarize the participants' feedback on each solution (see, for example, Section 4.2.1).

3.6 Ethical Considerations

Our study was approved by institutional review board (IRB) of the University of Lausanne. We recruited participants in September 2020 and conducted the participatory design sessions in October 2020. Even though we run the study in the COVID-19 era, the direction of the university allowed small gatherings (e.g., less than 15 people) as long as all participants wore a mask and respected sanitary measures. A sanitary plan was included in the request submitted to our IRB and in the recruitment e-mails. It specified that participants would have to wear masks. We cleaned all surfaces (e.g., pens, desks), aired the room before and after each session, and provided participants with hand sanitizers. In addition, the anonymity of the participants in the dataset was ensured by replacing each name with a participant number. We also did not use participants' real names and allowed the use of pseudonyms in the session instead of real names (if they preferred). In addition, we organized distinct sessions with MPC subjects and with MPC infringers. This way, we prevented accidentally gathering participants who could have been involved in the same MPC incident in the same sessions. Finally, during the sessions, we did not let participants self-identify themselves as victims or attackers. Rather we described them generically as OSN users.

4 FINDINGS

In this section, we present the outcome of the participatory design sessions. We first report the analysis of the participants' feedback on the application of the justice strategies in the design of solutions to address MPCs. Then, we give a descriptive summary of the designed solutions and the feedback collected from the mutual evaluation practices.

4.1 Design Rationale

Here we present three main themes generated from the participants' discussions in the focus group activity, where they discussed the use of justice strategies in the context of addressing MPCs. We also provide a summary of the pros and cons of these strategies, as discussed by participants.

4.1.1 Theme 1: Sanctions should be Commensurate to the Crime. Most of the participants mentioned that sanctions should be adapted to the seriousness of the committed offense or, in other words, *proportionate* to the crime. For example, participants found incapacitation too hard and restoration too soft as it does not include any penalty. Conversely, for severe MPCs, participants mentioned that incapacitation and retribution approaches could be effective. Participants argued that advertising the punishments that MPC infringers might receive could be sufficient to deter potential perpetrators before committing their misdeeds. [P16, female, 22 y.o.]: "*Yes, but afterward it could be scary too ... you don't want to go to jail.*" The severity of the offenses was mentioned several times. [P7, male, 21 y.o.]: "*Maybe, in this case, if someone published a pornographic video of you, retribution will be proportional.*"; [P10, female, 19 y.o.]: "*It really depends on the situation. There is a huge difference between revenge porn and posting the video of your drunk friend!*" The participants also discussed the fairness of the techniques. In particular, regarding the deterrence strategy, participants thought monetary fines can create inequities and then might not be effective. [P8, female, 41 y.o.]: "*It can create financial inequalities. It really depends on how the fines are set. If it is the same amount for everybody then it is not fair. If you are rich, you don't care.*"[13]

4.1.2 Theme 2: Educational and Punitive Strategies should be Applied Together. According to a large majority of the participants, rehabilitative and restorative strategies would be useful for educating MPC infringers or for mending the wrongdoing.[14] [P5, female, 29 y.o.]: "*It's good because it enables people to understand that they cannot do whatever they want. It is a punishment, but also an educational act.*" But, participants also reported that educative and restorative strategies might fail if MPC infringers do not cooperate. [P15, female, 18 y.o.]: "*Offenders might just not care and it's not going to change their mind ... Yes, if people do not agree* [with the restorative request]*, it can worsen the conflict.*" Furthermore, some MPC infringers could use these light approaches as a way to cover up the issue by pretending to be sincere or by whitewashing the conflictual report. [P24, male, 20 y.o.]: "*Some people can just use this* [mechanism] *to play the good guy. It can be frustrating for the victim to see that the offender is just using that to get away.*" Therefore, the participants indicated such approaches should always be combined with punitive strategies. [P4, female, 24 y.o.]: "*I would say restoration, but combined with incapacitation for example. If I had to do something, I would mix between making the person understand and punishing him a little bit. There's also no point in punishing him if he doesn't understand what he did wrong.*"

4.1.3 Theme 3: The Inclusion of MPC Subjects is Crucial. Many participants underlined the importance of taking the MPC subjects into account in the process of addressing MPCs. The participants indicated that rehabilitation, incapacitation, retribution, and deterrence do not consider the MPC subject, the one who was exposed. In this regard, they found restoration useful, as it can involve MPC subjects and enables them to talk with MPC infringers, to receive an apology for their misbehavior. In turn, this could bring psychological benefits that could make MPC subjects feel better. [P1, male, 19 y.o.]: "*Restoration might be more of a relief for the victim because they can confront the person directly.*

[13] Recently, in some countries, some fines have been made proportionate to the income of the person who infringes the law (e.g., traffic tickets for speeding in Switzerland [97]).
[14] Note that even if harms can be mended, what has been seen cannot be unseen.

It enables the person who inflicted the harm to understand the pain of the victim. This might help avoid future cases" (in reply to P1) [P3, female, 21 y.o.]: "*Yes! It also enables the victim to be able to express themselves and confront the offender directly, and in some cases, it enables the creation of a dialog where everyone can understand each other, which can facilitate the healing process.*" According to participants, simply punishing MPC infringers is not sufficient to address MPCs.

4.1.4 The Pros and Cons of the Five Justice Strategies. The participants reported different advantages for ***incapacitation***, including protecting the society from MPC infringers, making MPC infringers understand that their misdeeds might have concrete consequences in their lives, and deterring people from committing future MPCs. In contrast, the participants highlighted two shortcomings of incapacitation: this approach might not concretely educate infringers about what they did wrong, and it might be considered excessive for minor offenses (e.g., an embarrassing photo of the MPC subject wearing an awful Christmas jumper is shared non-consensually [120]). For ***retribution***, participants reported that it affords proportionality (see Sec. 4.1.1 above), it could educate infringers (i.e., make MPC infringers understand exactly what they did to the MPC subject), and that MPC infringers could receive an actual punishment (see Sec. 4.1.2). As for the drawbacks, the participants mentioned that retribution can trigger retaliation, that it is not educative, that it does not involve MPC subjects in the process (see Sec. 4.1.3), and that it feels like a primitive form of justice. ***Deterrence*** was regarded as an excellent way to make people aware that their wrongdoing could have concrete consequences and make them think twice before sharing content portraying other people, without asking first. This strategy was perceived as an effective approach for prevention. The participants also felt that this approach could be easily adapted to the context of the MPCs. In terms of shortcomings, some participants reported that monetary-based approaches, such as those suggested by the deterrence approach, could be ineffective with wealthy MPC infringers. Finally, concerning the ***rehabilitation*** approach, participants felt this could support MPC infringers' growth by educating them and making them reflect on their misdeeds (see Sec. 4.1.2). The main reported advantage of ***restoration*** was that of involving MPC subjects in the process, by having the parties communicate about the situation (see Sec. 4.1.3). This communication could enable MPC infringers to understand the harm they caused and could support the MPC subjects in their recovery process. It was noted, however, that both rehabilitation and restoration require human resources to be implemented. Both approaches were also perceived as ineffective for malicious, insincere, and non-empathetic individuals.

In the following sections, we describe the six solutions designed by the MPC subjects (marked with `-S-`), and the four solutions designed by the MPC infringers (marked with `-I-`). Note that the designed solutions typically involve multiple independent steps. These could be easily decoupled and re-composed into more effective strategies. We will further discuss this in the discussion section.

4.2 Solution 1. Trick-then-Treat (TT) -S-

TT is an intelligent content analyzer that can detect sensitive content, such as nudity or sexual content, in a photo (or video) and warn the users before sharing it on OSNs (Figure 3a). The warning says: *"Your content has been judged offensive! It could hurt other people. Do you want to post it?"* The MPC infringer can accept or refuse the warning. If the MPC infringer refuses the warning and continues to share content that leads to MPCs, the OSN can block access to the account and report the IP address of the computer of the infringer to the authorities.[15] The MPC infringer is then asked to remain at home until that person receives a visit from a professional that could provide psychological support and discuss the reason that led to the misbehavior. This might help the infringer change their behavior and avoid giving rise to MPCs in the future. TT aims at dissuading MPC infringers by reminding them about the possible

[15]Note this is somehow naive because there are ways to hide an IP address by using proxies or Tor.

negative outcomes of their actions. This solution uses incapacitation by limiting access to the OSN and rehabilitation by providing psychological support after the MPC has occurred (cf. 4.1.2).

4.2.1 Participants' Feedback. The participants reported perceiving TT to be effective in countering the rise of MPCs, as it might prevent offensive content from being shared, and it might help MPC infringers to understand why their behavior falls below community standards. Participants also found TT preventive, as it could dissuade infringers who might be acting in good faith. A participant mentioned that TT should be applied to serial infringers. However, some participants reported that the punishment of this solution is not proportionate to the offense, and it should not be implemented in real life as the consequences are too severe. Participants mentioned that it is technically challenging to judge content as offensive as it depends on many criteria. For example, a work of art can be marked erroneously as offensive content.

4.3 Solution 2. Warning Of Legal Fallout (WOLF) -I-

Similar to TT, WOLF combines a sensitive-content detection with a consent reminder. However, it is different because it can report detected cases to law enforcement authorities (Figure 3b). This technique presents the MPC infringer with messages such as: *"We found nudity in this image. If you post it, you might be reported to the local police."* Our co-designers thought warning MPC infringers with tangible consequences could be enough of a deterrent to prevent MPCs (cf. 4.1.1). In summary, WOLF applies a dissuasive approach by using the deterrence strategy, but it does not involve MPC subjects in the process.

4.3.1 Participants' Feedback. The majority of the participants agreed that WOLF could help reduce MPCs as the warning could dissuade infringers and the consequences appear to be certain. The participants noted the solution could, in the future, effectively protect MPC subjects from being harassed or from revenge pornography. They also reported that WOLF could work for only severe MPCs when the content involves nudity or violence, and it would not be useful for mild cases (e.g., a picture in a bar where the MPC subject appears drunk). The participants mentioned that the solutions might be complex to implement because law enforcement authorities might not have enough resources to act on all the reports of MPCs. One participant mentioned nudity content is not always offensive, and it might be difficult to build an algorithm that distinguishes offensive from legitimate content. Finally, the participants suggested that the solution could detect other forms of offense, in addition to nudity or pornography (e.g. a picture where the MPC subject is picking his nose), and it should be implemented on all OSNs.

4.4 Solution 3. From Ban To Forgiveness (FBTF) -S-

FBTF, similar to TT and WOLF, reminds MPC infringers that, before sharing the co-owned content, they must obtain consent from the other parties. But different than TT and WOLF, FBTF uses face-recognition algorithms. If one of the detected MPC subjects flags the photo, FBTF locks the infringer's account on the OSN for a certain duration (e.g., 30 days). After this period, the MPC infringer receives a message on their smartphone (cf. 4.1.3); it requires the infringer to write an apology letter to the MPC subject (Figure 3c). The solution warns potential infringers by using a simple popup warning. It utilizes incapacitation to punish MPC infringers and restoration to repair the harm (cf. 4.1.2).

4.4.1 Participants' Feedback. Participants disagreed on whether FBTF could be effective in preventing MPCs. Some of them found the one-month ban sufficient to avoid MPC, whereas others found this time insufficient. Several participants described how banning accounts could be easily circumvented, as some MPC infringers could create accounts on other

OSN platforms. Additionally, some participants noted how dissuasive warnings could be a weak approach, as some MPC infringers could simply ignore the message. As for the idea of apologizing at the end of the ban, participants mentioned that some MPC infringers could be insincere and just pretend to be sorry.[16] The participants reported several suggestions to improve FBTF: by (i) replacing the punishment with a monetary fine, (ii) shortening the ban period or making it proportionate to the severity of the MPC, and (iii) including the solution on all OSNs, not only one.

4.5 Solution 4. Face-based Individual Consent Reminder (FICR) -I-

FICR combines a facial-recognition algorithm with a consent reminder similar to that of FBTF. The FBTF detects users who appear in the photo and who did not provide their consent. FICR reminds users to obtain their permission, before sharing the photo (Figure 3d). For each individual face in the photo, FICR asks the MPC infringers to confirm if they have already received consent. However, unlike FBTF, FICR lets the MPC infringers decide whether to share the picture without consent. This solution does not use a particular justice strategy. The designers of FICR found it difficult to conceive a technology-based restoration strategy in everyday social media use. Designers mentioned that users could solve their conflicts through in-person discussions.

4.5.1 Participants' Feedback. Although participants appreciated FICR, as it encourages consent collection, some reported that FICR does not impede MPC infringers from sharing. One participant mentioned that FICR is not helpful to MPC subjects as they could be alerted about the non-consensual content, but only after it would be shared. Participants noted some recommendations: (i) give more control to MPC subjects and notify them before the content gets shared, and (ii) add some legal pressure to the warning message.

4.6 Solution 5. Guardian Angel of Privacy (GAP) -I-

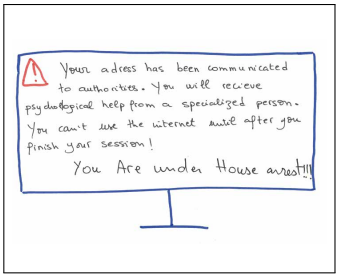
GAP is a tool that informs MPC subjects about their photo being published and enables them to remove the photo by explaining the reasons to the MPC infringer (Figure 3e). Similar to FBTF and FICR, GAP first recognizes the MPC subject's face, but it also notifies the MPC subject about the published content (cf. 4.1.3). If the MPC subjects are unhappy with the content, they can contact the MPC infringer by writing in a pop-up box why they do not agree that the picture should be published and how they would feel if it is published.[17] The OSN automatically removes the photo after the message has been seen by the MPC infringer.[18] In summary, GAP uses automatic face-recognition algorithms and lets the MPC infringers know the reason for the photo removal.

4.6.1 Participants' Feedback. All participants agreed that GAP is an appropriate solution for managing MPCs. Empowering MPC subjects by giving them the authority and control to remove unwanted content and enabling them to explain their motivation for the removed content are the two main reasons appreciated by the participants. Other participants reported that having an opportunity to explain their reasoning can also make MPC subjects feel better. They also noticed how GAP is a realistic solution that can be implemented on OSNs by using existing technologies. Finally, the

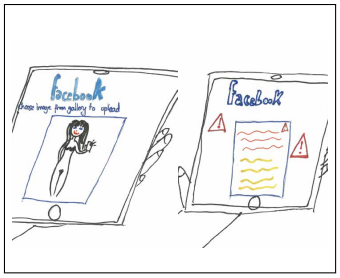
[16] Interestingly the participants did not notice the opportunities to game the solution with the reporting mechanisms. Essentially, to harm the uploader, users could give their consent while in person, then later pretend that they did not. Such solutions could be complemented with online consent collection systems.

[17] This part of the solution is in-line with a recently published work [88] that offers an explainable agent to manage MPCs. Further research is required to compare the effectiveness of receiving such explanations from virtual agents versus real MPC subjects. Furthermore, this solution follows a somewhat similar mechanism to what Facebook recently introduced in their privacy settings, where a user can ask for a picture to be removed and can explain why. See https://www.facebook.com/about/basics/manage-your-privacy/untagging (step 6), last accessed February 2021.

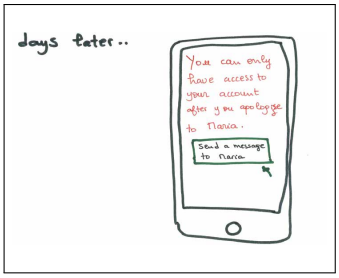
[18] However, this could also be done right after the MPC subject sends the message.



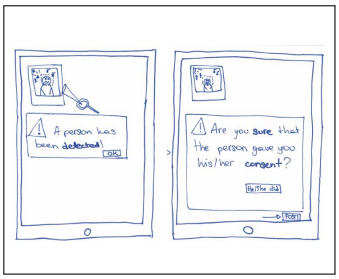
(a) TT; The intelligent content analyzer detects offensive content and warns an uploader.



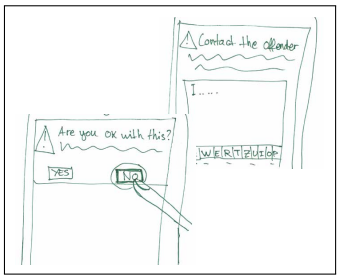
(b) WOLF; The app warns the MPC infringer that they can report the incident to law enforcement authorities.



(c) FBTF; After a 30-day account lock, the infringer has to write an apology letter to unlock the account.

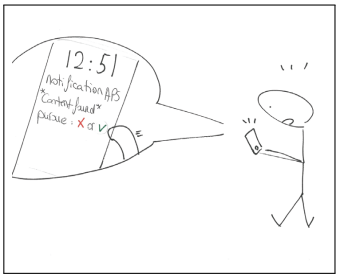


(d) FICR; The app reminds the uploader to obtain consent for every single face detected in the photo.

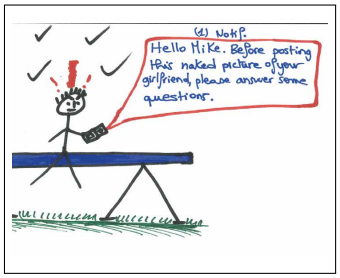


(e) GAP; The MPC subject writes in a pop-up box why they are not okay with the picture.

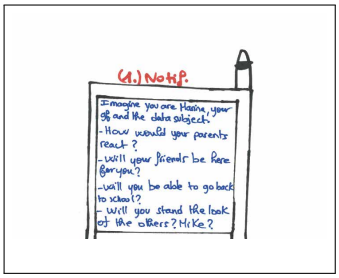
(f) APS (a); The app scans pornographic websites and seeks any content that features the MPC subject's face.



(g) APS (b); The MPC subject reviews a list of matches and double-checks the accuracy of the recognition.

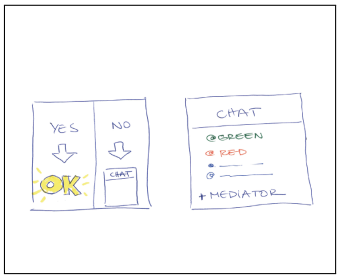


(h) ME (a); The app asks Mike to put himself in the shoes of his ex-girlfriend and answer a few questions.

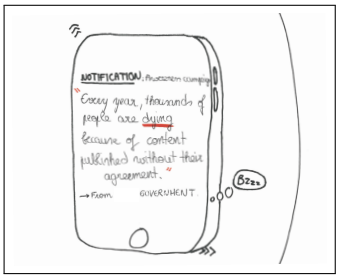


(i) ME (b); *"Imagine you are Marina! How would your parents react? Will you be able to go back to school?" etc.*

(j) MOOCIE; A lecturer teaches about the importance of obtaining consent. Next, the user should take a quiz.



(k) MeCoR; An expert mediator supports the MPC infringer and MPC subject(s) to solve the conflict.



(l) GAC; *"Every year, thousands of people die because of content published without their consent!"*

Fig. 3. Storyboards created for different solutions. All storyboards are available in the OSF repository.

participants mentioned that GAP could be improved by informing MPC subjects, before the content is shared. They also suggested extending the solution to multiple OSNs to prevent malicious infringers from circumventing the restriction.

4.7 Solution 6. Anti-Public Shaming (APS) -s-

APS is a Chrome plug-in [41]. Similar to FBTF, FICR, and GAP, APS uses face-recognition algorithms. But, contrary to these solutions, APS is a supportive approach. APS helps MPC subjects (cf. 4.1.3) who are suspicious or worried that their private videos could end up on pornographic websites. APS enables users to connect their OSN accounts to the plug-in and match their faces (from their shared photos) with pornographic websites (Figure 3f). APS scans multiple pornographic websites and seeks any content that features the MPC subject's face.[19] After the search is finished, MPC subjects receive a list of matches (if any). Then, they can review the content and double-check the accuracy of the recognition (Figure 3g). APS enables the MPC subject to use the results of the search to request removal and initiate legal action. If the judge finds the MPC infringer guilty, the infringer is obliged to remove the content and to pay a fine.

This solution uses the deterrence strategy to dissuade MPC infringers from giving rise to additional MPCs in the future.

4.7.1 Participants' Feedback. Most of the participants perceived APS to be a complementary solution to protecting MPC subjects. The participants found this solution supportive rather than preventive, as it helps remove unwanted content and track MPC infringers. Although, some participants reported that APS could also deter future MPCs, as MPC infringers might become more aware of the legal consequences of their actions. The participants mentioned that utilizing this solution requires a certain effort, such as installing the plug-in and synchronizing it with the OSN account. Hence, the solution could be difficult to use for novice technology users. Given the variety of pornographic websites and their large database, some participants mentioned that scanning all these repositories would not be feasible. Meanwhile, others suggested that crawling should be exhaustive and not limited to only pornographic websites.

4.8 Solution 7. Moment of Empathy (ME) -s-

ME is designed to address severe MPCs (Figure 3h). Identical to TT and WOLF, ME detects sensitive content. However, only ME attempts to create empathy on the part of MPC infringers towards MPC subjects. The app asks the MPC infringer to put herself in the shoes of the MPC subject and to answer a few questions such as *"How would your parents react?"*, *"Will you be able to go back to school?"*, *"How will you deal with the looks of others?"* (Figure 3i). ME gives the MPC infringer time to carefully consider sharing the content. These questions were designed to nudge MPC infringer to reflect and eventually refrain from sharing the content.[20]

4.8.1 Participants' Feedback. Overall, participants were positive and optimistic about ME. Most of the participants reported that ME would make MPC infringers aware of the consequences of their acts. The participants believed that ME could help them to remember that MPC subjects are human beings and to understand that, although these behaviors are commonplace on the Internet, there might be repercussions in real life. The participants reported that ME could prevent MPCs, as infringers could feel closer to MPC subjects. It would cause them to think twice, and to reconsider their decisions before sharing. However, some participants reported that low-empathy individuals could circumvent the solution by providing random and thoughtless answers. Some participants noted that it could be challenging to ask the

[19] Note that such content must be accessible and not behind paywalls, which could be the case with pornographic websites.
[20] Note that the use of empathy to dissuade people from enacting negative behavior has been studied in the past [110, 111]. However, its effectiveness in the MPC context is still under debate [6, 21]. Future research should investigate empathy-based strategies in real-usage settings.

right questions that would make the infringers reflect, and that the questions should be adapted for every case. The participants recommended improving the solution by (i) integrating a system to make sure the questions were read carefully by MPC infringers, (ii) exposing questions in the form of video messages instead of text to increase the impact, and (iii) notifying the MPC subjects about the sensitive content to be shared.

4.9 Solution 8. MOOC for Internet Education (MOOCIE) -s-

MOOCIE is a web-based pedagogical solution for mild MPCs (Figure 3j). It aims at educating MPC infringers who share non-consensual content in OSNs. Similar to FBTF, MOOCIE is activated if an MPC subject reports an MPC by triggering a specific flag on the OSN. However, MOOCIE is different because it immediately blocks the account of the MPC infringer and requires them to take—and pass—an online course on "cybersecurity and privacy awareness" (cf. 4.1.2). The course is designed to teach MPC infringers about being respectful of others' privacy and the importance of obtaining consent before sharing someone else's photo. The course is followed by a short quiz. Access to the account is restored only after the right answers are submitted. MOOCIE uses incapacitation to force MPC infringers to participate in rehabilitative sessions, and it aims at preventing infringers from giving rise to other MPCs in the future.

4.9.1 Participants' Feedback. Overall, participants found MOOCIE effective. However, some participants underlined the fact that when an MPC subject flags content, it is already too late as the intervention occurs after the picture or video has been published and might already has been seen by others. Consequently, MOOCIE might not stop ongoing MPC but could reduce the rate of future MPCs. The participants found the solution feasible and thought it would work in real-life scenarios. However, some mentioned it could not deter malicious users. The participants suggested that the course content should not be generic and should be tailored for different cases. They also mentioned changing the content of the course to prevent habituation. Finally, some suggested deploying the solution across all OSNs, thus making it hard for MPC infringers to circumvent the ban by creating new accounts or sharing on other OSNs.

4.10 Solution 9. Mediation for Conflict Resolution (MeCoR) -s-

MeCoR is a collaborative solution that enforces the consent collection for mild MPCs (Figure 3k). Similar to TT, WOLF, FBTF, FICR, and ME, MeCoR reminds the MPC infringer to ask for consent before sharing. It also requires the MPC infringer to tag all MPC subjects depicted in the photo. Next, MeCoR sends notifications to all MPC subjects asking for their consent before the photo is published (cf. 4.1.3). The photo is published if and only if all MPC subjects give their consent. For MPC subjects who do not consent, the app opens a chat box for the MPC infringer, MPC subject(s), and a mediator from the OSN company. The mediator, who is an expert of the terms and conditions of the OSN, guides the conversation and supports the users in solving the conflict. To avoid potential future conflicts between users, this method applies the restoration strategy, before the content is shared.

4.10.1 Participants' Feedback. Most of the participants described MeCoR as a preventive solution. They also noted that the prevention would be effective only if MeCoR enforces MPC infringers to tag MPC subjects or if it uses an automatic-detection technique. The participants reported that they would feel secure with MeCoR because nothing can be published without their consent. Another positive point of the design is the opportunity for the users to explain their motives and to negotiate the final sharing decision. Participants also noticed that it might be infeasible for OSNs to put a real mediator in chat groups for every single conflict. They suggested the use of AI technology and chatbots to

overcome this issue. Finally, participants noted that the solution does not work for those who do not own an account on the same OSN where the content is being shared.[21]

4.11 Solution 10. Government Awareness Campaign (GAC) -I-

GAC reminds the content uploaders in advance, similar to TT, WOLF, FBTF, FICR, ME, and MeCoR. However, GAC is a novel OSN function, as it was developed through the collaboration of the OSN platform and local government (Figure 3l). The initiative begins with a social awareness campaign against MPCs and is sponsored by the local government. Designers provided an example of such messages: *"Every year, thousands of people die because of content published without their consent! (Interagency Working Group, U.S. Government)"*[22] The warnings appear in the form of a pop-up message at the moment of sharing a photo on an OSN. GAC aims to dissuade the MPC infringers, before they share non-consensual content, or to persuade them to delete the photo, immediately after it has been shared. In summary, GAC uses the deterrence strategy by informing MPC infringers about the potentially serious consequences of their behavior.

4.11.1 Participants' Feedback. Most of the participants found GAC helpful as it encourages OSN users to think twice before posting content that might hurt other people. GAC was seen as a reminder that could nudge MPC infringers to cease their sharing or to seek consent. Some participants mentioned that GAC could educate infringers by making them more aware of what MPC subjects might experience as a consequence of their actions. The participants also highlighted that "government-issued warnings" could be effective, as the source is typically seen as authoritative. Some mentioned that, even though GAC is not targeted directly at MPC subjects, it could still give them a feeling that their problems have been heard. However, most participants reported that GAC would not work for malicious MPC infringers who intentionally want to harm others and it might be ignored by users who share frequently (due to habituation). The participants recommended that (i) GAC should add a punishment for those who do not delete the content judged offensive, and (ii) it should send notifications to MPC subjects, letting them know about the non-consensual content being shared.

4.12 The Summary of Solutions

The overall summary of the ten solutions is presented in Table 2. Most solutions were designed primarily for the MPC infringers, to make them aware of the consequences of their actions and to dissuade them from sharing without collecting consent from others. Only one solution was designed primarily for MPC subjects, to help them uncover content where they appear and for which they did not provide consent (APS). Two solutions also provided active roles for the MPC subjects (GAP and MeCoR); these solutions involved the MPC subjects in the interaction process of resolving the MPCs. A number of other solutions involved MPC subjects as secondary stakeholders (TT, WOLF, FBTF, FICR, ME, MOOCIE, and GAC); these solutions do not prescribe the involvement of the MPC subject, as they consider it optional. In terms of severity, about half of the solutions addressed MPCs that could produce severe consequences such as cyberbullying, cyberstalking, and revenge porn (TT, WOLF, GAP, APS, and ME). The remaining solutions addressed MPCs that could have mild consequences, such as endangering the public image of the MPC subjects (FBTF, FICR, MOOCIE, MeCoR, and GAC).

[21] This is not necessarily the case as the OSN might allow co-owners without an account to review publication of content, even without being registered on their service.
[22] Here, our participants used fictitious data instead of real data. Given the ethical implications of using fictitious data [81], when implementing such solutions, designers should prefer data-driven approaches (i.e., real data).

Table 2. The summary of the solutions in terms of (i) the stakeholders involved in storyboards and whether they reap benefits, (ii) the severity of the MPC addressed, (iii) the expected impact of each solution, (iv) the types of support, (v) the use of the justice strategies, and (vi) the types of mechanisms. The top row shows the acronym of each solution. ∘ indicates the stakeholders who were not actively involved in the storyboards, but who reaped secondary benefits from the solutions.

		TT -S-	WOLF -I-	FBTF -S-	FICR -I-	GAP -I-	APS -S-	ME -S-	MOOCIE -S-	MeCoR -S-	GAC -I-
Stakeholders	MPC infringer	✓	✓	✓	✓	✓	∘	✓	✓	✓	✓
	MPC subject	∘	∘	∘	∘	✓	✓	∘	∘	✓	∘
Severity	Addressing severe MPC	✓	✓	-	-	✓	✓	✓	-	-	-
Impact	Preventive	-	-	-	-	✓	-	-	-	✓	-
	Dissuasive	✓	✓	✓	✓	-	-	✓	-	-	✓
	Corrective	-	-	-	-	-	✓	-	✓	-	-
Support	Psychological	✓	-	✓	-	-	-	-	-	-	-
	Legal	-	-	-	-	-	✓	-	-	✓	-
	Educational	-	-	-	-	-	-	-	✓	-	-
Strategies	Deterrence	-	✓	-	-	-	✓	-	-	-	✓
	Incapacitation	✓	-	✓	-	-	-	-	✓	-	-
	Rehabilitation	✓	-	-	-	-	-	-	✓	-	-
	Restoration	-	-	✓	-	-	-	-	-	✓	-
	Retribution	-	-	-	-	-	-	-	-	-	-
Mechanisms	Face Detection	-	-	✓	✓	✓	✓	-	-	-	-
	Content Detection	✓	✓	-	-	-	-	✓	-	-	-
	Manual Flagging	-	-	✓	-	-	-	-	✓	-	-
	Consent Reminder	✓	✓	✓	✓	-	-	✓	-	✓	✓
	Mediator	✓	-	-	-	-	-	-	-	✓	-
	OSN Integration	✓‡	✓‡	✓	✓	✓	-	✓	✓	✓	✓‡

The last six rows explain the type of mechanisms used in the solutions. These mechanisms are automatic detection mechanisms (e.g., detecting a face or sensitive content), manually flagging an item by MPC subjects, mechanisms using reminders (i.e., to obtain consent), and the mechanisms involving mediators (e.g., to resolve the conflict). The last row indicates if a solution should be implemented in an OSN platform. ✓‡ shows the solutions that OSN company should work together with a third-party organization.

In terms of the impact on the occurrence of MPCs, two solutions provided absolute prevention by enforcing MPC infringers to ask for consent before they could be allowed to publish the content (GAP and MeCoR). We refer to these as 'preventive' solutions in Table 2. In these solutions, the MPC subjects were able to approve or reject the sharing of the content where they appeared. Note that though MeCoR prevents the photo from being shared, GAP removes the photo right after the MPC subject expresses disagreement with the content being published. The former prevents side leakages, but the latter might not provide full protection. Six storyboards used dissuasive strategies to deter MPC infringers from giving rise to MPC (TT, WOLF, FBTF, FICR, ME, and GAC). Designers used distinct strategies with the infringers: informing them about the legal consequences (WOLF); warning them with statistical facts and authority (GAC); persuading them through empathy (TT and ME). The remaining two solutions provided damage-control support, but only after the MPC occurs (APS and MOOCIE). We refer to these solutions as 'corrective' in Table 2.

Reviewing the different solutions, we identified three forms of support that could help in the conflict resolutions related to MPCs: psychological (helping stakeholders reflect, empathize and elaborate), legal (helping stakeholders collect consent or produce legal evidence), and educational (helping stakeholders through training). Specifically, two solutions provided psychological support (TT and FBTF). Two solutions provided legal support (APS and MeCoR). And, one solution provided MPC infringers with educational support (MOOCIE).

In terms of the use of the aforementioned justice framework, three solutions integrated two justice strategies (TT, FBTF, and MOOCIE). These solutions combined incapacitation with either rehabilitation or restoration. Four of the solutions used a single strategy in their design: deterrence (WOLF, APS, and GAC), and restoration (MeCoR). The other solutions did not use any of the justice strategies introduced during the design sessions (FICR, GAP, and ME). Instead, these solutions used a psychological approach to elicit an empathic response (ME), or simply technological approaches to persuade users to seek consent (FICR) or to remove the photo (GAP). Three solutions used the principle of deterrence for the MPC infringers: informing them about the legal consequences of MPCs (GAC), threatening to report MPC infringers to law enforcement authorities before posting the content (WOLF), and threatening to use 'fines' (APS). Three storyboards used incapacitation that limits MPC infringers' access to OSN: until the infringer attends a psychological session (TT), for a fixed amount of days and only after the infringer apologizes (FBTF), and after the infringer succeeds in an online training course (MOOCIE). Two storyboards used the principle of rehabilitation: through in-person psychological support (TT), and by using an online training course and exam (MOOCIE). Finally, three solutions used the principle of restoration: by requiring that both sides resolve the conflict in advance through a mediator (MeCoR), without a mediator (GAP), and by encouraging MPC infringers to make an apology to the MPC subject (FBTF). None of the design groups used retribution. Our participants noted that retribution could create more problems than it solves. They perceived retribution as equal to the law of retaliation or the "lex talionis" [56] in the Bible, and mentioned retribution could incite hatred and create endless circles of anger. [P2, female, 21 y.o.]: "*It can encourage feelings of hatred like you did this to me, I'm doing this to you. So it never stops!*"

In terms of technology, most of the solutions used automatic recognition algorithms such as image-processing and computer-vision-based algorithms (e.g., content detection, face detection/recognition) to detect MPCs.[23] These solutions propose detecting: for nudity or sexual content (TT, WOLF, GAP, and ME), for content published on porn websites (APS), and simply for any kind of content published without consent (FBTF and FICR). Other techniques relied on non-automatic strategies including compulsory tagging (MeCoR) and a report-based flagging of non-consensual content (MOOCIE). Two solutions enabled the MPC subjects to report non-consensual sharing (FBTF and MOOCIE). Furthermore, several solutions proposed to deter the infringer through warning messages that would pop up during the sharing flow (TT, WOLF, FBTF, FICR, ME, MeCoR, and GAC). Two of the designed solutions require either a human mediator or an agent-based mediator (TT and MeCoR). Finally, almost all solutions require integration with online social networks. However, in several cases, this is not deemed sufficient and the designed solution would require integration with a third-party organization (TT, WOLF, and GAC).

5 DISCUSSION

Our participants co-designed ten solutions to address the problem of MPCs. In this section, we first provide an answer to our two research questions. Later, we discuss several aspects of these solutions, such as their technical feasibility.

[23]Note that such techniques do exist [1], yet they are not fully reliable. Also, any solutions relying on this technology should not allow reverse tagging, specifically the identity of the people in the content should not be revealed to the uploader to protect the privacy of the users.

We conclude this section by discussing future directions for research and design with regards to the development of concrete solutions to address MPCs.

5.1 What Solutions Would Young OSN Users, who have Experienced MPCs, Co-design to Address the Problem of MPCs?

The solutions designed by participants were mostly targeted at MPC infringers. However, in several cases, participants recognized the importance of involving MPC subjects in resolving the conflict. This was seen as providing psychological benefits to both sides (cf. 4.1.3). The recent literature on restorative approaches in the justice system has also reported the positive benefits of enabling the involved parties to communicate about what led to the conflict and to discuss the way to amend the situation [112]. Henceforth, the design and research community should look for ways of involving MPC subjects in the conflict resolution process. This can take place in multiple ways. For instance, by enabling a communication channel where MPC infringers can explain themselves and possibly apologize, and where MPC subjects can explain how they feel with regard to the non-consensual sharing.

Half of the designed solutions aimed at addressing severe MPCs. Namely, designers thought that for the most mundane cases, the solutions already in place in most OSNs for reporting conflicts would be sufficient (e.g., reporting a post on Instagram for abuse). Note, however, that the distinction between severe and non-severe is somewhat arbitrary and non-objective. An MPC, which might start as a trivial oversight, might spiral into a severe case of cyberbullying, once the conflictual content becomes known to the wider public. For instance, in a recent survey [31], 61% of teens reported being bullied about their appearance, whereas only 15% of them reported sexuality as the reason for cyberbullying. A safer approach would be to treat all conflicts the same, by automating detection, processing, and mitigating the conflict (see Sec. 5.3 below).

Only two designed solutions provide full protection against MPCs (i.e., prevention). The other solutions attempt to dissuade MPC infringers (i.e., discouraging non-compliant behavior) or to correct the MPC after the non-consensual content has become known to the public. Note that corrective approaches do not offer protection to MPCs because, as the content becomes known to the public, it can already be too late to avoid serious harm. Both preventive and dissuasive approaches have positive and negative aspects, as discussed in a recent study [21]. Although dissuasive solutions might be simpler to implement, they might not offer full protection to vulnerable users. Thus, we recommend that the design and research community test the effectiveness of these solutions on existing OSNs.

In terms of support, the participants proposed three forms of support: psychological (e.g., mediating the conflict between MPC infringers and subjects), legal (e.g., supporting consent collection), and educational (e.g., providing training on the community norms). Note that though these forms of supports are embedded in separate solutions, they might be concurrently provided to OSN users to address multiple facets of the MPC conflict. To date, few solutions have been developed in these three areas, which calls for future design exploration. The concept of the accountable-consent collection, in particular, has recently been demonstrated through a design concept [95].

In terms of the five justice strategies presented in Sec. 3.3, our participants implemented deterrence and incapacitation, most often by blocking MPC infringers' access to their OSN accounts or by threatening to block them. Rehabilitation was implemented in a minority of solutions, via counseling and teaching about the community standards. Finally, restoration was implemented by asking the MPC infringer to apologize or by enabling the MPC subject and the MPC infringer to discuss the conflict and to negotiate the amendments under the supervision of a mediator. Future work could focus on solutions that enable mediation and conflict resolution in OSNs. Next, we discuss the differences between solutions designed by MPC infringers and MPC subjects.

5.2 What Are the Differences Between Solutions Designed by MPC Infringers and MPC Subjects?

Overall, we found that, in a single solution, MPC subjects referred to justice strategies (cf. 3.3) more than MPC infringers did (S *median* = 1.5 vs. I *median* = 1).[24] As suggested by previous studies, referring to a lower number of justice strategies might indicate the need for MPC infringers to disengage morally to justify their negative behavior, and to deactivate moral controls and personal sanctions [11, 84]. These proportions could also be due to the MPC subjects being more motivated to find a solution. This increased motivation could also explain why MPC subjects proposed more *restrictive* solutions. They used the 'incapacitation' strategy in half of their solutions, perhaps as an intuitive emotional response, whereas the same strategy was never used by MPC infringers. MPC subjects, unlike MPC infringers, also provided more forms of support in their solutions (S *median* = 1 vs. I *median* = 0) and included 'third-parties' in two solutions; this could be a way to involve external authorities in the conflict-resolution process.

In terms of technical mechanisms (e.g., face detection/recognition, content detection), we found again that MPC subjects applied more techniques in their solutions than MPC infringers did (S *median* = 2 vs. I *median* = 1.5). This could be due to the fact that the MPC subjects need a backup mechanism to address the MPC in case the primary mechanisms should fail.

MPC infringers designed, overall, interventions with milder consequences. They resorted to deterrence more than MPC subjects did (S *median* = 0 vs. I *median* = 0.5), and they resorted to incapacitation less than MPC subjects did (S *median* = 0.5 vs. I *median* = 0), thus supporting the idea that MPC infringers might not fully realize the possible consequences of severe MPCs. An emotional mechanism might also explain this result. In contrast with the responsibility felt by victims, the feelings of pride and indifference might fuel disengagement for these users [84]. Taken together, these results suggest that a safer approach should be adopted to protect the most vulnerable users, given that MPC infringers might not fully realize (or might not be willing to evaluate) the impact of their actions on the lives of others. Next, we discuss the technical feasibility of the implementation of these solutions.

5.3 Technical Implementation of the Designed Solutions

All solutions designed by our participants are based on a workflow comprising three main steps: the detection of an MPC event, the processing during which dissuasive or preventive actions can be triggered, and the outcome step during which specific actions can be taken to address, mitigate [8], or resolve the conflict (see Figure 4).

Most of the designed solutions refer to automatic computer-vision-based algorithms for detecting content that is likely to cause an MPC (e.g., photos with nudity, photos with multiple individuals). Examples of these algorithms have already been proposed in the prior state-of-the-art, e.g., previous literature focused on face detection [1, 55], bystander detection [45], and nudity detection [39]. These previous studies provide the technical foundations to build the solutions identified by our participants. Note that, such methods could fall short of detecting people without an OSN account [75]. Also, with deepfakes [126], malicious users can modify the content before sharing it to bypass any detection mechanism. More research on this form of intentional misbehavior is required [65]. In addition to automatic detection, our participants also identified manual flagging of conflicting content as a mechanism to trigger the MPC workflow. In this regard, note that (i) options for reporting offending content already exist in most OSNs (see for example [33]); (ii) reporting offending content when it has already been published might be too late to avoid consequences; (iii) the mechanisms currently in place have been shown to be insufficient to counter the rise of MPCs, as reported by recent studies [117]; and (iv) the option for reporting offending content could be weaponized by malicious

[24] Note that though the study was not intended to quantitatively compare MPC infringers and MPC subjects, we observed some potential differences between these two categories of users; this needs to be confirmed by future research.

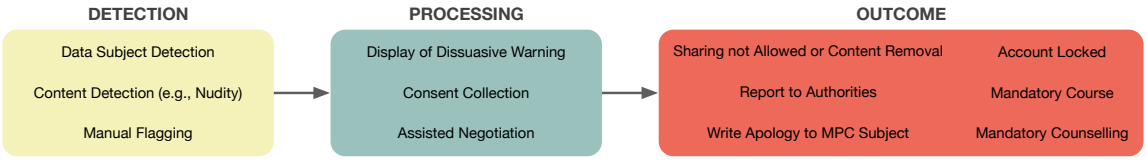


Fig. 4. Workflow of the designed solutions: for each main step, the main mechanisms identified by the participants are listed.

users to unduly punish other users [38]. In order to function, most of the designed solutions require integration with the OSN. The OSN provider acts as a content-delivery platform and as an identity manager. Recent work also proposes to decouple these two functions to further protect the privacy of the OSN users [95].

After an MPC event is detected (or reported), the designed solutions differ in terms of how to address the conflict. Many solutions move directly to the outcome step, addressing false-positives post-facto. Several solutions prompt the MPC infringer with dissuasive warnings. These have been researched in previous privacy research [6, 21, 81]. Using a different approach, two of the solutions designed by our participants suggest using consent collection from all parties appearing in the content as a precondition to publishing it. Earlier studies developed different techniques for consent collection [77, 95]. Whereas previous work suggests the use of negotiation algorithms to help stakeholders reach consensus on publishing conflicting content [115, 118], two other solutions, presented here, recommend the inclusion of mediators to help resolve the conflict between MPC infringers and subjects. Given the logistic requirements of such interventions (i.e., human mediators can be scarce and expensive), building these solutions might seem infeasible. However, the recent advances in the fields of natural-language processing [40] and conversational agents [26, 44, 72] could enable solutions to be built, where chatbots could mediate the discussion between the parties, and they could provide the information on the conditions of use of the OSN or information on the specific legislation in the country where the MPC took place, or support the users in expressing their feelings about the event. Henceforth, these solutions can be further researched and tested. One point of concern, highlighted in prior research, is about the delay required to secure consent from all MPC subjects depicted in the content [21]. In specific circumstances, this might render the delay unmanageable (e.g., bystanders in the picture). None of the designed solutions included item or audience modification (cf. Section 2.2). It is noteworthy this result contrasts with the fact that these two solutions were actually found in [117], where few participants reported using them in practice when confronted with MPC.

Finally, the designed solutions differ also in terms of the way to address the MPC, once the event is detected and possibly after a preventive phase. Several solutions simply do not permit the MPC infringers to continue with their sharing intent, others remove the content post-facto. Other solutions lock the account of the MPC infringer, or require mandatory counseling or training, as a means of preventing the same users from causing conflicts in the future. Other solutions suggest reporting the conflict to the authorities, so that they will pursue the MPC infringer in the real world. Finally, one solution requires the MPC infringer to write an apology letter. Whereas removing content or locking an account would be simple to implement for OSN providers (e.g., [34]), human-based counseling can be expensive, hence infeasible, especially on the scale of the users of the Internet. Online training or other forms of automated interventions might be easier to scale up. Future work can study these approaches.

5.4 Which Way Forward to Assist Users in the case of MPCs?

Our participants designed solutions that encourage MPC infringers to negotiate or to apologize, and this enables subjects to explain why they were unhappy with the content and requested its removal. These practices, in a minority of MPCs, were already identified in prior research as a way OSN users spontaneously handle conflicts [113]. The results of the participatory design presented here confirm that these practices are considered, by users who have experienced MPCs, as appropriate for addressing the problem. Furthermore, the solutions suggest that, if these were integrated into the main functionalities of OSNs, some of these approaches could be used more widely to support users during conflicts. Unfortunately, taken one by one, none of the presented solutions is ideal. For instance, MeCoR does not include any automatic recognition system in the detection step, thus permitting malicious users to purposefully omit tagging the content in order to circumvent the verification mechanisms that would involve the data subjects. Yet, the steps required by these solutions can be decoupled and re-combined into novel solutions to provide optimal support and protection to both MPC infringers and MPC subjects.

For example, we sketched a possible recombination of these steps named Dissuasion-Mediation-Training, or DiMeTra (see Figure 5). This solution is triggered by an algorithm that recognizes multiple people in the content being shared. In a first processing step, the solution displays a dissuasive warning to remind the user that the community standards require obtaining consent from other subjects portrayed in the content. If the warning is ignored, then the MPC subject(s) are notified. If they agree with the content, then the content is published on the OSN. Otherwise, both the MPC infringer and the subject are required to discuss in a chat window, which could be moderated by a chatbot. At this stage, several options are possible: either the MPC infringer ceases the sharing intent, or the content is edited to mask (or remove) the appearance of the MPC subject [95].[25] If the MPC infringer disagrees with these two options, the solution continues with a number of steps designed to mitigate the conflict: first, the sharing and viewing rights on the OSN of the MPC infringer are revoked; then the user is required to take an online course. The sharing and viewing rights are restored only upon successful completion of the online course evaluation. The advantages of this solution are multiple. Simple cases of non-conflictual content can be managed with little friction: either the MPC infringer desists or the content is immediately approved by the MPC subject(s). And blatant privacy infringements can be easily ruled out. For fringe cases, the feature offers the opportunity to both MPC infringer and subject to communicate with each other and to reach an agreement. Eventually, persistent negative behavior of the MPC infringer leads to mandatory training that can help the MPC infringers rehabilitate their misconduct and become better members of the OSN community.

Of course, *productizing* any of the solutions presented in this paper requires further work. Many details about these solutions require additional design and testing. For instance, the mediation component of DiMeTra relies on a linguistic model to support OSN users during the discussion. Further research is necessary to identify the most common communication intents that users will utilize to discuss MPCs. Henceforth, researchers could implement a minimal viable version of a chatbot designed to address MPCs. This prototype could be tested through a lab study involving participants who have experienced and/or caused MPCs. We plan to pursue this line of research in our future work.

5.5 Limitations of the Participatory Design Sessions

Our approach has some limitations. The study participants were young adults who experienced MPCs. Other age groups, such as teenagers or older adults, might have contributed different perspectives and needs with regard to these types of conflicts. Future studies could also include these additional age groups. Also, half of our participants experienced MPCs

[25] Prior work investigated various masking techniques for privacy protection [46, 47, 64, 79, 92].

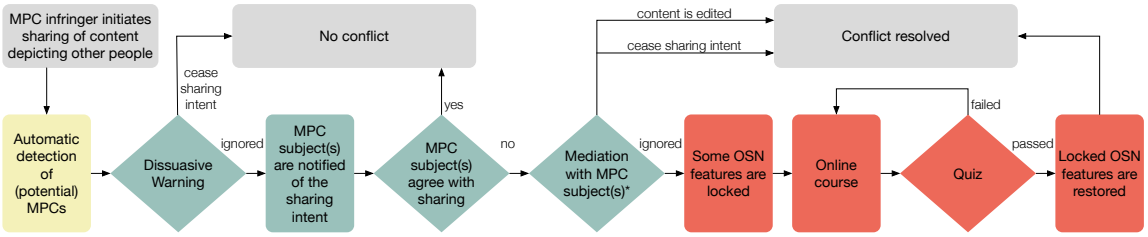


Fig. 5. DiMeTra Solution. The colors of the steps refer to Figure 4.

with severe consequences. However, none of them experienced MPCs with *extreme* consequences, such as revenge pornography. Conducting research with this population of users might require additional care and consideration. However, their perspective and experience could reveal additional aspects of MPCs that we have not yet considered in this study. Finally, we conducted our study in Switzerland. OSN users with different cultural backgrounds might have different attitudes and opinions about MPCs. Future research could replicate the current study with participants from different cultural backgrounds.

6 CONCLUSION

In this article, to develop practical solutions to the problem of MPCs, we have presented the outcome of participatory design sessions. To the best of our knowledge, this study is the first to involve young OSN users—who have experienced MPCs—in the design process. In this work, we have contributed user-centric designs that inform the future privacy-preserving techniques in OSNs. Although we cannot implement these ten solutions in their current state, they reveal constituting steps (or processes) that can be re-purposed to further the development of practical implementations. For a possible embodiment of these processes, we have contributed DiMeTra, a solution to MPCs requiring further development and testing. In the future, we can only expect our digital life to grow in complexity and pervasiveness. Privacy solutions need to quickly adapt to this fast-moving landscape. In this regard, we suggest an exciting research direction of using chatbots to provide support during conflicts that people experience online. We plan to pursue this avenue in our future work. Implementing refined versions of the approaches presented in this paper in existing OSNs can help limit the incidence of interdependent privacy conflicts and promote a safer online environment.

ACKNOWLEDGMENTS

This work was partially funded by the Swiss National Science Foundation with Grant #CRSK-2_190762. We sincerely thank Manon Jendly and Camille Perrier Depeursinge for their advice regarding the justice strategies. We thank Jose M. Such for providing precious feedback on the article. We thank Lahari Goswami for her valuable comments on our participatory design. We also thank Holly Cogliati, James Tyler, and Vincent Vandersluis for proofreading this article. Last, we thank all the participants who contributed to the design sessions.

REFERENCES

[1] Paarijaat Aditya, Rijurekha Sen, Peter Druschel, Seong Joon Oh, Rodrigo Benenson, Mario Fritz, Bernt Schiele, Bobby Bhattacharjee, and Tong Tong Wu. 2016. I-Pic: A Platform for Privacy-Compliant Image Capture. In *Proc. of the Annual Int. Conf. on Mobile Sys., Applications, and Services (MobiSys)*. Assoc. for Comp. Mach. (ACM), Singapore, Singapore, 235–248. https://doi.org/10.1145/2906388.2906412

[2] Gulsum Akkuzu, Benjamin Aziz, and Mo Adda. 2020. Towards consensus-based group decision making for co-owned data sharing in online social networks. *IEEE Access* 8 (2020), 91311–91325. https://doi.org/10.1109/ACCESS.2020.2994408

[3] Albert W Alschuler. 2003. The changing purposes of criminal punishment: A retrospective on the past century and some thoughts about the next. *The University of Chicago Law Rev.* 70, 1 (2003), 1–22. https://chicagounbound.uchicago.edu/uclrev/vol70/iss1/1/

[4] Büşra Altın and Songül Aksoy. 2020. Investigation of the Effects of Cognitive Tasks on Balance Performance in Young Adults. *American Jour. of Otolaryngology* 41, 6 (Nov. 2020), 102663. https://doi.org/10.1016/j.amjoto.2020.102663

[5] Irwin. Altman. 1975. *The environment and social behavior: privacy, personal space, territory, crowding.* Brooks/Cole Pub. Co., Monterey, California, USA. https://eric.ed.gov/?id=ED131515

[6] Mary Jean Amon, Rakibul Hasan, Kurt Hugenberg, Bennett I Bertenthal, and Apu Kapadia. 2020. Influencing Photo Sharing Decisions on Social Media: A Case of Paradoxical Findings. In *2020 IEEE Symp. on Secu. and Privacy (SP).* IEEE, San Francisco, California, USA, 79–95. https://doi.org/10.1109/SP40000.2020.00006

[7] Reza Anaraky, Tahereh Nabizadeh, Bart Knijnenburg, and Marten Risius. 2018. Reducing Default and Framing Effects in Privacy Decision-Making. In *SIGHCI 2018 Proc.* Assoc. for Info. Sys. (AIS), Atlanta, GA, USA, 7. https://aisel.aisnet.org/sighci2018/19

[8] Zahra Ashktorab. 2016. A Study of Cyberbullying Detection and Mitigation on Instagram. In *Proc. of the ACM Conf. on Comp. Supported Cooperative Work & Social Comp. (CSCW Companion'16).* Assoc. for Comp. Mach. (ACM), New York, NY, USA, 126–130. https://doi.org/10.1145/2818052.2874346

[9] Zahra Ashktorab and Jessica Vitak. 2016. Designing Cyberbullying Mitigation and Prevention Solutions through Participatory Design With Teenagers. In *Proc. of the ACM Conf. on Human Factors in Comp. Sys. (CHI'16).* Assoc. for Comp. Mach. (ACM), New York, NY, USA, 3895–3905. https://doi.org/10.1145/2858036.2858548

[10] Hedy Bach. 2007. Composing a visual narrative inquiry. *Handbook of narrative inquiry: Mapping a methodology* 280 (2007), 307. https://methods.sagepub.com/book/handbook-of-narrative-inquiry/n11.xml

[11] Albert Bandura, Claudio Barbaranelli, Gian Vittorio Caprara, and Concetta Pastorelli. 1996. Mechanisms of Moral Disengagement in the Exercise of Moral Agency. *Jour. of Personality and Social Psychology* 71, 2 (1996), 364–374. https://doi.org/10.1037/0022-3514.71.2.364

[12] Filipe Beato and Roel Peeters. 2014. Collaborative joint content sharing for online social networks. In *Proc. of the Int. Conf. on Pervasive Comp. and Comm. Workshops (PERCOM Workshops).* IEEE, Budapest, Hungary, 616–621. https://doi.org/10.1109/PerComW.2014.6815277

[13] Andrew Besmer and Heather Richter Lipford. 2010. Moving beyond untagging: photo privacy in a tagged world. In *Proc. of the ACM Conf. on Human Factors in Comp. Sys. (CHI'10).* Assoc. for Comp. Mach. (ACM), Atlanta, GA, USA, 1563. https://doi.org/10.1145/1753326.1753560

[14] Leanne Bowler, Cory Knobel, and Eleanor Mattern. 2015. From Cyberbullying to Well-Being: A Narrative-Based Participatory Approach to Values-Oriented Design for Social Media. *Jour. Assoc. Info. Science Tech.* 66, 6 (June 2015), 1274–1293. https://dl.acm.org/doi/10.5555/3150797.3150812

[15] Leanne Bowler, Eleanor Mattern, and Cory Knobel. 2014. Developing design interventions for cyberbullying: A narrative-based participatory approach. In *iConf. Proceedings.* Ischools, Berlin, Germany, 153–162. https://doi.org/10.9776/14059

[16] John Braithwaite. 2004. Restorative justice and de-professionalization. *The good society* 13, 1 (2004), 28–31. https://doi.org/10.1353/gso.2004.0023

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

[18] Kevin M Carlsmith. 2006. The roles of retribution and utility in determining punishment. *Jour. of Experimental Social Psychology* 42, 4 (2006), 437–451. https://doi.org/10.1016/j.jesp.2005.06.007

[19] Barbara Carminati and Elena Ferrari. 2011. Collaborative Access Control in On-line Social Networks. In *Proc. of the Int. Conf. on Collaborative Comp.: Networking, Applications and Worksharing (CollaborateCom'11).* IEEE, Orlando, FL, USA, 231–240. https://doi.org/10.4108/icst.collaboratecom.2011.247109

[20] Michael Cavadino, James Dignan, and George Mair. 2007. *The penal system: An introduction.* Sage, London, UK. https://bit.ly/3669NgV

[21] Mauro Cherubini, Kavous Salehzadeh Niksirat, Marc-Olivier Boldi, Henri Keopraseuth, Jose M. Such, and Kévin Huguenin. 2021. When Forcing Collaboration is the Most Sensible Choice: Desirability of Precautionary and Dissuasive Mechanisms to Manage Multiparty Privacy Conflicts. *Proc. of the ACM Jour.: Human-Comp. Interaction; Comp. Supported Cooperative Work and Social Comp.* 5, CSCW1, Article 053 (April 2021), 36 pages. https://doi.org/10.1145/3449127

[22] Hichang Cho and Anna Filippova. 2016. Networked Privacy Management in Facebook: A Mixed-Methods and Multinational Study. In *Proc. of the ACM Conf. on Comp.-Supported Cooperative Work & Social Comp. (CSCW'16).* Assoc. for Comp. Mach. (ACM), San Francisco, CA, USA, 502–513. https://doi.org/10.1145/2818048.2819996

[23] Ben C. F. Choi, Zhenhui (Jack) Jiang, Bo Xiao, and Sung S. Kim. 2015. Embarrassing Exposures in Online Social Networks: An Integrated Perspective of Privacy Invasion and Relationship Bonding. *Info. Sys. Research* 26, 4 (Dec 2015), 675–694. https://doi.org/10.1287/isre.2015.0602

[24] Tae Rang Choi and Yongjun Sung. 2018. Instagram versus Snapchat: Self-Expression and Privacy Concern on Social Media. *Telematics and Informatics* 35, 8 (Dec. 2018), 2289–2298. https://doi.org/10.1016/j.tele.2018.09.009

[25] D Jean Clandinin and F Michael Connelly. 2000. Narrative inquiry. https://bit.ly/3adjJ9N

[26] Leigh Clark, Nadia Pantidi, Orla Cooney, Philip Doyle, Diego Garaialde, Justin Edwards, Brendan Spillane, Emer Gilmartin, Christine Murad, Cosmin Munteanu, Vincent Wade, and Benjamin R. Cowan. 2019. What Makes a Good Conversation? Challenges in Designing Truly Conversational Agents. In *Proc. of the ACM Conf. on Human Factors in Comp. Sys. (CHI'19).* Assoc. for Comp. Mach. (ACM), New York, NY, USA, 1–12. https://doi.org/10.1145/3290605.3300705

[27] Marshall B Clinard and Robert F Meier. 2015. *Sociology of deviant behavior.* Nelson Education, Andover, UK. https://bit.ly/3a23LyS

[28] Mauro Coletto, Luca Maria Aiello, Claudio Lucchese, and Fabrizio Silvestri. 2016. On the behaviour of deviant communities in online social networks. In *Int. AAAI Conf. on Web and Social Media.* AAAI Press, Cologne, Germany, 72–81.

[29] Simeon de Brouwer. 2020. Privacy Self-Management and the Issue of Privacy Externalities: of Thwarted Expectations, and Harmful Exploitation. *Internet Policy Rev.* 9, 4 (Dec. 2020), 29. https://doi.org/10.14763/2020.4.1537

[30] Jayati Dev, Sanchari Das, Yasmeen Rashidi, and L. Jean Camp. 2019. *Personalized WhatsApp Privacy: Demographic and Cultural Influences on Indian and Saudi Users.* SSRN Scholarly Paper ID 3391021. Social Science Research Network, Rochester, NY. https://doi.org/10.2139/ssrn.3391021

[31] Ogi Djuraskovic. 2021. Cyberbullying Statistics, Facts, and Trends (2021) with Charts. https://firstsiteguide.com/cyberbullying-stats/ Last accessed 28th of Jan 2021.

[32] Antony Duff and Zachary Hoskins. 2019. Legal Punishment. In *The Stanford Encyclopedia of Philosophy* (winter 2019 ed.), Edward N. Zalta (Ed.). Metaphysics Research Lab, Stanford University, Stanford, CA, US. https://plato.stanford.edu/archives/win2019/entries/legal-punishment/

[33] Facebook. 2021. How do I report inappropriate or abusive things on Facebook (example: nudity, hate speech, threats)? https://www.facebook.com/help/212722115425932 Last accessed 31st of January 2021.

[34] Facebook. 2021. Photos or Videos That Violate Your Privacy. https://www.facebook.com/help/428478523862899 Last accessed 31st of January 2021.

[35] Ricard L. Fogues, Pradeep K. Murukannaiah, Jose M. Such, and Munindar P. Singh. 2017. Sharing Policies in Multiuser Privacy Scenarios: Incorporating Context, Preferences, and Arguments in Decision Making. *ACM Trans. on Comp.-Human Interaction (TOCHI)* 24, 1 (Mar 2017), 1–29. https://doi.org/10.1145/3038920

[36] Ricard L. Fogues, Pradeep K. Murukannaiah, Jose M. Such, and Munindar P. Singh. 2017. SoSharP: Recommending Sharing Policies in Multiuser Privacy Scenarios. *IEEE Internet Comp.* 21, 6 (Nov 2017), 28–36. https://doi.org/10.1109/MIC.2017.4180836

[37] Ricard L Fogues, Pradeep Murukanniah, Jose M Such, Agustin Espinosa, Ana Garcia-Fornes, and Munindar Singh. 2015. Argumentation for multi-party privacy management. In *Proc. of the Int. Workshop on Agents and CyberSecu. (ACySe'15).* ACM Press, Istanbul, Turkey, 3–6. https://eprints.lancs.ac.uk/id/eprint/74191/

[38] David Mandell Freeman. 2017. Can You Spot the Fakes? On the Limitations of User Feedback in Online Social Networks. In *Proc. of the 26th Int. Conf. on World Wide Web (WWW'17).* Int. World Wide Web Conf.s Steering Committee, Republic and Canton of Geneva, CHE, 1093–1102. https://doi.org/10.1145/3038912.3052706

[39] M. B. Garcia, T. F. Revano, B. G. M. Habal, J. O. Contreras, and J. B. R. Enriquez. 2018. A Pornographic Image and Video Filtering Application Using Optimized Nudity Recognition and Detection Algorithm. In *IEEE Int. Conf. on Humanoid, Nanotechnology, Info. Tech., Comm. and Control, Environment and Management (HNICEM'18).* IEEE, Baguio City, Philippines, 1–5. https://doi.org/10.1109/HNICEM.2018.8666227

[40] Matt Gardner, Joel Grus, Mark Neumann, Oyvind Tafjord, Pradeep Dasigi, Nelson Liu, Matthew Peters, Michael Schmitz, and Luke Zettlemoyer. 2018. AllenNLP: A Deep Semantic Natural Language Processing Platform. In *Proc. of Workshop for NLP Open Source Software (NLP-OSS'18).* Assoc. for Computational Linguistics, Melbourne, Australia, 1–6. https://doi.org/10.18653/v1/W18-2501

[41] Google. 2021. Chrome Extensions. https://chrome.google.com/webstore/category/extensions Last accessed 15th of April 2021.

[42] Saul Greenberg, Sheelagh Carpendale, Nicolai Marquardt, and Bill Buxton. 2012. The Narrative Storyboard: Telling a Story about Use and Context over Time. *Interactions* 19, 1 (Jan. 2012), 64–69. https://doi.org/10.1145/2065327.2065340

[43] Ralph Gross and Alessandro Acquisti. 2005. Information revelation and privacy in online social networks. In *Proc. of the ACM Workshop on Priv. in the Electronic Society (WPES'05).* Assoc. for Comp. Mach. (ACM), Alexandria, VA, USA, 71–80. https://doi.org/10.1145/1102199.1102214

[44] Hamza Harkous, Kassem Fawaz, Kang G. Shin, and Karl Aberer. 2016. PriBots: Conversational Privacy with Chatbots. In *Proc. of the Symp.. on Usable Priv. and Secu. (SOUPS'16).* USENIX, Denver, CO, USA, 6. https://www.usenix.org/conference/soups2016/workshop-program/wfpn/presentation/harkous

[45] Rakibul Hasan, David Crandall, Mario Fritz, and Apu Kapadia. 2020. Automatically Detecting Bystanders in Photos to Reduce Privacy Risks. In *IEEE Symp. on Secu. and Priv. (S&P'20).* IEEE, Oakland, CA, USA, 318–335. https://doi.org/10.1109/SP40000.2020.00097

[46] Rakibul Hasan, Eman Hassan, Yifang Li, Kelly Caine, David J. Crandall, Roberto Hoyle, and Apu Kapadia. 2018. Viewer Experience of Obscuring Scene Elements in Photos to Enhance Privacy. In *Proc. of the ACM Conf. on Human Factors in Comp. Sys. (CHI'18).* Assoc. for Comp. Mach. (ACM), New York, NY, USA, 1–13. https://doi.org/10.1145/3173574.3173621

[47] Rakibul Hasan, Yifang Li, Eman Hassan, Kelly Caine, David J. Crandall, Roberto Hoyle, and Apu Kapadia. 2019. Can Privacy Be Satisfying? On Improving Viewer Satisfaction for Privacy-Enhanced Photos Using Aesthetic Transforms. In *Proc. of the ACM Conf. on Human Factors in Comp. Sys. (CHI'19).* Assoc. for Comp. Mach. (ACM), New York, NY, USA, 1–13. https://doi.org/10.1145/3290605.3300597

[48] Roberto Hoyle, Luke Stark, Qatrunnada Ismail, David Crandall, Apu Kapadia, and Denise Anthony. 2020. Privacy Norms and Preferences for Photos Posted Online. *ACM Trans. Comput.-Hum. Interact.* 0, ja (2020), 1. https://doi.org/10.1145/3380960

[49] Hongxin Hu and Gail-Joon Ahn. 2011. Multiparty Authorization Framework for Data Sharing in Online Social Networks. In *Proc. of the IFIP Annual Conf. on Data and Applications Secu. and Priv. (DBSec'11).* Springer, Richmond, VA, USA, 29–43. https://doi.org/10.1007/978-3-642-22348-8_5

[50] Hongxin Hu, Gail-Joon Ahn, and Jan Jorgensen. 2011. Detecting and resolving privacy conflicts for collaborative data sharing in online social networks. In *Proc. of the Annual Comp. Secu. Applications Conf. (ACSAC'11).* Assoc. for Comp. Mach. (ACM), Orlando, FL, USA, 103–112. https://doi.org/10.1145/2076732.2076747

[51] Hongxin Hu, Gail-Joon Ahn, and Jan Jorgensen. 2012. Enabling Collaborative data sharing in Google+. In *Proc. of the IEEE Global Comm. Conf. (GLOBECOM'12).* IEEE, Anaheim, CA, USA, 720–725. https://doi.org/10.1109/GLOCOM.2012.6503198

[52] Hongxin Hu, Gail-Joon Ahn, and Jan Jorgensen. 2013. Multiparty Access Control for Online Social Networks: Model and Mechanisms. *IEEE Trans. on Knowledge and Data Engineering* 25, 7 (Jul 2013), 1614–1627. https://doi.org/10.1109/TKDE.2012.97

[53] Mathias Humbert, Benjamin Trubert, and Kévin Huguenin. 2019. A Survey on Interdependent Privacy. *ACM Comp. Surv.* 52, 6, Article Article 122 (Oct. 2019), 40 pages. https://doi.org/10.1145/3360498

[54] Panagiotis Ilia, Barbara Carminati, Elena Ferrari, Paraskevi Fragopoulou, and Sotiris Ioannidis. 2017. SAMPAC: Socially-Aware Collaborative Multi-Party Access Control. In *Proc. of the ACM on Conf. on Data and Application Secu. and Priv. (CODASPY'17)*. ACM, Scottsdale, AZ, USA, 71–82. https://doi.org/10.1145/3029806.3029834

[55] Panagiotis Ilia, Iasonas Polakis, Elias Athanasopoulos, Federico Maggi, and Sotiris Ioannidis. 2015. Face/Off: Preventing Privacy Leakage From Photos in Social Networks. In *Proc. of the ACM SIGSAC Conf. on Comp. and Comm. Secu. (CCS'15)*. Assoc. for Comp. Mach. (ACM), Denver, CO, USA, 781–792. https://doi.org/10.1145/2810103.2813603

[56] Bernard S. Jackson. 2006. Lex Talionis in Early Judaism and the Exhortation of Jesus in Matthew 5.38–42. By James F. Davis. *The Jour. of Theological Stud.* 58, 1 (10 2006), 200–206. https://doi.org/10.1093/jts/fll096 arXiv:https://academic.oup.com/jts/article-pdf/58/1/200/9647630/fll096.pdf

[57] Adam N. Joinson. 2008. Looking at, Looking Up or Keeping Up with People?: Motives and Use of Facebook. In *Proc. of the ACM Conf. on Human Factors in Comp. Sys. (CHI'08)*. Assoc. for Comp. Mach. (ACM), Florence, Italy, 1027. https://doi.org/10.1145/1357054.1357213

[58] Dilara Kekulluoglu, Nadin Kokciyan, and Pinar Yolum. 2018. Preserving Privacy as Social Responsibility in Online Social Networks. *ACM Trans. on Internet Tech. (TOIT)* 18, 4 (Apr 2018), 1–22. https://doi.org/10.1145/3158373

[59] Dilara Keküllüoğlu, Nadin Kökciyan, and Pınar Yolum. 2016. Strategies for Privacy Negotiation in Online Social Networks. In *Proc. of the Int. Workshop on AI for Priv. and Secu. (PrAISe)*. Assoc. for Comp. Mach. (ACM), The Hague, The Netherlands, 1–8. https://doi.org/10.1145/2970030.2970035

[60] Simon Kemp. 2020. Digital 2020: Global Digital Overview. https://datareportal.com/reports/digital-2020-global-digital-overview Last accessed 13th of November 2020.

[61] Finn Kensing and Jeanette Blomberg. 1998. Participatory Design: Issues and Concerns. *Comp. Supported Cooperative Work (CSCW)* 7, 3 (Sept. 1998), 167–185. https://doi.org/10.1023/A:1008689307411

[62] Finn Kensing and Andreas Munk-Madsen. 1993. PD: Structure in the Toolbox. *Commun. ACM* 36, 6 (June 1993), 78–85. https://doi.org/10.1145/153571.163278

[63] Nadin Kökciyan, Nefise Yaglikci, and Pinar Yolum. 2017. An Argumentation Approach for Resolving Privacy Disputes in Online Social Networks. *ACM Trans. Internet Tech.* 17, 3, Article 27 (June 2017), 22 pages. https://doi.org/10.1145/3003434

[64] P. Korshunov and T. Ebrahimi. 2013. Using Face Morphing to Protect Privacy. In *IEEE Int. Conf. on Advanced Video and Signal Based Surveillance (AVSS'13)*. IEEE, Krakow, Poland, 208–213. https://doi.org/10.1109/AVSS.2013.6636641

[65] Pavel Korshunov and Sebastien Marcel. 2018. DeepFakes: A New Threat to Face Recognition? Assessment and Detection. *arXiv* 1812.08685 [cs] (Dec. 2018), 5. http://arxiv.org/abs/1812.08685

[66] Bert P. Krages. 2003. The Photographer's Right. http://www.krages.com/phoright.htm Last accessed 2nd of October 2020.

[67] Nicholas Kristof. 2020. The Children of Pornhub; Why does Canada allow this company to profit off videos of exploitation and assault? https://www.nytimes.com/2020/12/04/opinion/sunday/pornhub-rape-trafficking.html Last accessed 9th of December 2020.

[68] Richard A Krueger. 2014. *Focus groups: A practical guide for applied research.* Sage publications, California, USA. https://bit.ly/2XRwYao

[69] Justin Kruger, Cameron L. Gordon, and Jeff Kuban. 2006. Intentions in teasing: When "just kidding" just isn't good enough. *Jour. of Personality and Social Psychology* 90, 3 (Mar 2006), 412–425. https://doi.org/10.1037/0022-3514.90.3.412

[70] Airi Lampinen. 2015. Networked Privacy beyond the Individual: Four Perspectives to "Sharing". In *Proc. of The Fifth Decennial Aarhus Conf. on Critical Alternatives (CA'15)*. Aarhus University Press, Aarhus N, 25–28. https://doi.org/10.7146/aahcc.v1i1.21300

[71] Airi Lampinen, Vilma Lehtinen, Asko Lehmuskallio, and Sakari Tamminen. 2011. We're in it together: interpersonal management of disclosure in social network services. In *Proc. of the ACM Conf. on Human Factors in Comp. Sys. (CHI'11)*. Assoc. for Comp. Mach. (ACM), Vancouver, BC, Canada, 3217–3226. https://doi.org/10.1145/1978942.1979420

[72] Liliana Laranjo, Adam G Dunn, Huong Ly Tong, Ahmet Baki Kocaballi, Jessica Chen, Rabia Bashir, Didi Surian, Blanca Gallego, Farah Magrabi, Annie Y S Lau, and Enrico Coiera. 2018. Conversational agents in healthcare: a systematic review. *Jour. of the American Medical Info. Assoc.* 25, 9 (07 2018), 1248–1258. https://doi.org/10.1093/jamia/ocy072 arXiv:https://academic.oup.com/jamia/article-pdf/25/9/1248/34150600/ocy072.pdf

[73] Roxanne Leitão. 2019. Anticipating Smart Home Security and Privacy Threats with Survivors of Intimate Partner Abuse. In *Proc. of the ACM Conf. on Designing Interactive Sys. (DIS'19)*. Assoc. for Comp. Mach. (ACM), New York, NY, USA, 527–539. https://doi.org/10.1145/3322276.3322366

[74] David John Lemay, Tenzin Doleck, and Paul Bazelais. 2017. "Passion and Concern for Privacy" as Factors Affecting Snapchat Use: A Situated Perspective on Technology Acceptance. *Comp. in Human Behavior* 75 (Oct. 2017), 264–271. https://doi.org/10.1016/j.chb.2017.05.022

[75] Andrew Leonard. 2013. Why facial recognition failed. https://www.salon.com/2013/04/22/why_facial_recognition_failed/

[76] Karen Levy and Bruce Schneier. 2020. Privacy Threats in Intimate Relationships. *Jour. of Cybersecurity* 6, 1 (Jan. 2020), 1–13. https://doi.org/10.1093/cybsec/tyaa006

[77] Fenghua Li, Zhe Sun, Ang Li, Ben Niu, Hui Li, and Guohong Cao. 2019. HideMe: Privacy-Preserving Photo Sharing on Social Networks. In *Proc. of the IEEE Int. Conf. on Comp. Comm. (INFOCOM'19)*. IEEE, Paris, France, 154–162. https://doi.org/10.1109/INFOCOM.2019.8737466

[78] Yifang Li, Nishant Vishwamitra, Hongxin Hu, and Kelly Caine. 2020. Towards A Taxonomy of Content Sensitivity and Sharing Preferences for Photos. In *Proc. of the ACM Conf. on Human Factors in Comp. Sys. (CHI'20)*. Assoc. for Comp. Mach. (ACM), New York, NY, USA, 1–14. https://doi.org/10.1145/3313831.3376498

[79] Yifang Li, Nishant Vishwamitra, Bart P. Knijnenburg, Hongxin Hu, and Kelly Caine. 2017. Effectiveness and Users' Experience of Obfuscation as a Privacy-Enhancing Technology for Sharing Photos. *Proc. ACM Hum.-Comput. Interact.* 1, CSCW, Article 67 (Dec. 2017), 24 pages. https:

//doi.org/10.1145/3134702

[80] Yuhan Luo, Peiyi Liu, and Eun Kyoung Choe. 2019. Co-Designing Food Trackers with Dietitians: Identifying Design Opportunities for Food Tracker Customization. In *Proc. of the ACM Conf. on Human Factors in Comp. Sys. (CHI'19)*. Assoc. for Comp. Mach. (ACM), New York, NY, USA, 1–13. https://doi.org/10.1145/3290605.3300822

[81] Hiroaki Masaki, Kengo Shibata, Shui Hoshino, Takahiro Ishihama, Nagayuki Saito, and Koji Yatani. 2020. Exploring Nudge Designs to Help Adolescent SNS Users Avoid Privacy and Safety Threats. In *Proc. of the ACM Conf. on Human Factors in Comp. Sys. (CHI'20)*. Assoc. for Comp. Mach. (ACM), New York, NY, USA, 1–11. https://doi.org/10.1145/3313831.3376666

[82] Gillian M. McCarthy, Edgar R. Rodriguez Ramírez, and Brian J. Robinson. 2017. Participatory Design to Address Stigma with Adolescents with Type 1 Diabetes. In *Proc. of the ACM Conf. on Designing Interactive Sys. (DIS'17)*. Assoc. for Comp. Mach. (ACM), New York, NY, USA, 83–94. https://doi.org/10.1145/3064663.3064740

[83] Annette McDonough. 2009. The Experiences and Concerns of Young Adults (18-40 Years) Living with an Implanted Cardioverter Defibrillator (ICD). *European Jour. of Cardiovascular Nursing: Jour. of the Working Group on Cardiovascular Nursing of the European Society of Cardiology* 8, 4 (Oct. 2009), 274–280. https://doi.org/10.1016/j.ejcnurse.2009.03.002

[84] Ersilia Menesini, Virginia Sánchez, Ada Fonzi, Rosario Ortega-Ruiz, Angela Costabile, and Giorgio Feudo. 2003. Moral Emotions and Bullying: A Cross-National Comparison of Differences between Bullies, Victims and Outsiders. *Aggressive Behavior* 29 (Dec. 2003), 515–530. https://doi.org/10.1002/ab.10060

[85] Terance D Miethe, Hong Lu, et al. 2005. *Punishment: A comparative historical perspective*. Cambridge University Press, Cambridge, UK. https://books.google.ch/books/about/Punishment.html?id=o2ovr4ZzIXsC&redir_esc=y

[86] Andrew D. Miller and W. Keith Edwards. 2007. Give and take: a study of consumer photo-sharing culture and practice. In *Proc. of the ACM Conf. on Human Factors in Comp. Sys. (CHI'07)*. ACM Press, San Jose, California, USA, 347–356. https://doi.org/10.1145/1240624.1240682

[87] William Ian Miller. 2005. *Eye for an Eye*. Cambridge University Press, Cambridge, UK. https://bit.ly/2KFs4Km

[88] Francesca Mosca and Jose M Such. 2021. ELVIRA: an Explainable Agent for Value and Utility-driven Multiuser Privacy. In *20th Int. Conf. on Autonomous Agents and Multiagent Sys. (AAMAS'21)*. Int. Foundation for Autonomous Agents and Multiagent Sys., London, UK (virtual), In press.

[89] Francesca Mosca, Jose M Such, and Peter Mcburney. 2019. Value-driven Collaborative Privacy Decision Making. In *Proc. of the AAAI Spring Symp. on Priv.-Enhancing Artificial Intelligence and Language Tech. (PAL'19)*. CEUR Workshop Proc., Stanford, California, USA, 13–20. http://ceur-ws.org/Vol-2335/1st_PAL_paper_4.pdf

[90] Francesca Mosca, Jose M. Such, and Peter McBurney. 2020. Towards a Value-driven Explainable Agent for Collective Privacy. In *Proc. of the 19th Int. Conf. on Autonomous Agents and MultiAgent Sys. (AAMAS'20)*. Int. Foundation for Autonomous Agents and Multiagent Sys., Auckland, New Zealand, 1937–1939. https://doi.org/10.5555/3398761.3399033

[91] Daniel S Nagin. 1998. Criminal deterrence research at the outset of the twenty-first century. *Crime and Justice* 23 (1998), 1–42. https://doi.org/10.1086/449268

[92] Y. Nakashima, T. Koyama, N. Yokoya, and N. Babaguchi. 2015. Facial Expression Preserving Privacy Protection Using Image Melding. In *IEEE Int. Conf. on Multimedia and Expo (ICME'15)*. IEEE, Turin, Italy, 1–6. https://doi.org/10.1109/ICME.2015.7177394

[93] Helen Nissenbaum. 2009. *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press, Stanford, CA, USA. https://www.sup.org/books/title/?id=8862

[94] Abu Saleh Md Noman, Sanchari Das, and Sameer Patil. 2019. Techies Against Facebook: Understanding Negative Sentiment Toward Facebook via User Generated Content. In *Proc. of the ACM Conf. on Human Factors in Comp. Sys. (CHI'19)*. Assoc. for Comp. Mach. (ACM), New York, NY, USA, 1–15. https://doi.org/10.1145/3290605.3300698

[95] Alexandra-Mihaela Olteanu, Kévin Huguenin, Italo Dacosta, and Jean-Pierre Hubaux. 2018. Consensual and Privacy-Preserving Sharing of Multi-Subject and Interdependent Data. In *Proc. of the Symp. on Network and Distributed Sys. Secu. (NDSS'18)*. Internet Society, San Diego, CA, USA, 15. https://doi.org/10.14722/ndss.2018.23002

[96] Leysia Palen and Paul Dourish. 2003. Unpacking" privacy" for a networked world. In *Proc. of the ACM Conf. on Human Factors in Comp. Sys. (CHI'03)*. Assoc. for Comp. Mach. (ACM), New York, NY, USA, 129–136. https://doi.org/10.1145/642611.642635

[97] Jason Paur. 2010. Swiss Slap Speeder With $290K Fine. https://www.wired.com/2010/01/record-speeding-fine-dents-swiss-bank-account/ Last accessed 8th of January 2021.

[98] Sandra Petronio. 2002. *Boundaries of privacy: Dialectics of disclosure*. State University of New York Press (series in communication studies), Albany, NY, US. https://bit.ly/3c9RtqX

[99] Sandra Petronio. 2010. Communication privacy management theory: What do we know about family privacy regulation? *Jour. of Family Theory & Rev.* 2, 3 (2010), 175–196. https://doi.org/10.1111/j.1756-2589.2010.00052.x

[100] William L Prosser. 1960. Privacy. *Cali. Law Rev.* 48, 3 (Aug. 1960), 383–423. https://web.archive.org/web/20131019050717/http://www.californialawreview.org/assets/pdfs/misc/prosser_privacy.pdf

[101] Sarah Rajtmajer, Anna Cinzia Squicciarini, Jose M. Such, Justin Semonsen, and Andrew Belmonte. 2017. An Ultimatum Game Model for the Evolution of Privacy in Jointly Managed Content. In *Proc. of the Int. Conf. on Decision and Game Theory for Secu. (GameSec'17)*. Springer, Vienna, Austria, 112–130. https://doi.org/10.1007/978-3-319-68711-7_7

[102] Yasmeen Rashidi, Tousif Ahmed, Felicia Patel, Emily Fath, Apu Kapadia, Christena Nippert-Eng, and Norman Makoto Su. 2018. "You Don't Want to Be the next Meme": College Students' Workarounds to Manage Privacy in the Era of Pervasive Photography. In *Proc. of the Symp. on Usable Priv.*

and Secu. (SOUPS'18). USENIX Assoc., USA, 143–157. https://www.usenix.org/conference/soups2018/presentation/rashidi

[103] Yasmeen Rashidi, Apu Kapadia, Christena Nippert-Eng, and Norman Makoto Su. 2020. "It's easier than causing confrontation": Sanctioning Strategies to Maintain Social Norms of Content Sharing and Privacy on Social Media. *Proc. of the ACM Jour.: Human-Comp. Interaction; Comp. Supported Cooperative Work and Social Comp.* 4, CSCW1 (May 2020), 23:1–23:25. https://doi.org/10.1145/3392827

[104] Arunee Ratikan and Mikifumi Shikida. 2014. Privacy Protection Based Privacy Conflict Detection and Solution in Online Social Networks. In *Proc. of the Int. Conf. on Human Aspects of Info. Secu., Priv., and Trust (HAS'14)*. Springer, Heraklion, Crete, Greece, 433–445. https://doi.org/10.1007/978-3-319-07620-1_38

[105] Edgardo Rotman. 1990. *Beyond punishment: A new view on the rehabilitation of criminal offenders*. Greenwood Press, Westport, CT, US. https://bit.ly/2MeasWu

[106] Robert AC Ruiter, Loes TE Kessels, Gjalt-Jorn Y Peters, and Gerjo Kok. 2014. Sixty years of fear appeal research: Current state of the evidence. *Int. Jour. of Psychology* 49, 2 (2014), 63–70. https://doi.org/10.1002/ijop.12042

[107] Elizabeth B.-N. Sanders and Pieter Jan Stappers. 2008. Co-Creation and the New Landscapes of Design. *CoDesign* 4, 1 (March 2008), 5–18. https://doi.org/10.1080/15710880701875068

[108] Raymond Scupin. 1997. The KJ Method: A Technique for Analyzing Data Derived from Japanese Ethnology. *Human Organization* 56, 2 (1997), 233–237. https://www.jstor.org/stable/44126786?seq=1#metadata_info_tab_contents

[109] Joanna Shapland. 2014. Implications of growth: Challenges for restorative justice. *Int. Rev. of Victimology* 20, 1 (2014), 111–127. https://doi.org/10.1177/0269758013510808

[110] Lijiang Shen. 2010. Mitigating psychological reactance: The role of message-induced empathy in persuasion. *Human Comm. Research* 36, 3 (2010), 397–422. https://doi.org/10.1111/j.1468-2958.2010.01381.x

[111] Lijiang Shen. 2011. The effectiveness of empathy-versus fear-arousing antismoking PSAs. *Health Comm.* 26, 5 (2011), 404–415. https://doi.org/10.1080/10410236.2011.552480

[112] Lawrence Sherman, Heather Strang, et al. 2007. *Restorative justice: The evidence*. Smith Institute, London, UK. https://www.iirp.edu/pdf/RJ_full_report.pdf

[113] Elizabeth Stowell, Teresa K. O'Leary, Everlyne Kimani, Michael K. Paasche-Orlow, Timothy Bickmore, and Andrea G. Parker. 2020. Investigating Opportunities for Crowdsourcing in Church-Based Health Interventions: A Participatory Design Study. In *Proc. of the ACM Conf. on Human Factors in Comp. Sys. (CHI'20)*. Assoc. for Comp. Mach. (ACM), New York, NY, USA, 1–12. https://doi.org/10.1145/3313831.3376833

[114] Jose M. Such and Natalia Criado. 2014. Adaptive Conflict Resolution Mechanism for Multi-party Privacy Management in Social Media. In *Proc. of the ACM Workshop on Priv. in the Electronic Society (WPES'14)*. Assoc. for Comp. Mach. (ACM), Scottsdale, AZ, USA, 69–72. https://doi.org/10.1145/2665943.2665964

[115] Jose M. Such and Natalia Criado. 2016. Resolving Multi-Party Privacy Conflicts in Social Media. *IEEE Trans. on Knowledge and Data Engineering* 28, 7 (Jul 2016), 1851–1863. https://doi.org/10.1109/TKDE.2016.2539165

[116] Jose M. Such and Natalia Criado. 2018. Multiparty privacy in social media. *Comm. of the ACM* 61, 8 (Jul 2018), 74–81. https://doi.org/10.1145/3208039

[117] Jose M. Such, Joel Porter, Sören Preibusch, and Adam Joinson. 2017. Photo Privacy Conflicts in Social Media: A Large-scale Empirical Study. In *Proc. of the ACM Conf. on Human Factors in Comp. Sys. (CHI'17)*. Assoc. for Comp. Mach. (ACM), Denver, CO, USA, 3821–3832. https://doi.org/10.1145/3025453.3025668

[118] Jose M. Such and Michael Rovatsos. 2016. Privacy Policy Negotiation in Social Media. *ACM Trans. on Autonomous and Adaptive Sys. (TAAS)* 11, 1 (Feb 2016), 1–29. https://doi.org/10.1145/2821512

[119] Kurt Thomas, Chris Grier, and David M. Nicol. 2010. unFriendly: Multi-party Privacy Risks in Social Networks. In *Priv. Enhancing Tech.* Springer, Berlin, Germany, 236–252. https://doi.org/10.1007/978-3-642-14527-8_14

[120] TIME. 2019. Justin Trudeau Wore Brownface at 2001 'Arabian Nights' Party While He Taught at a Private School. https://time.com/5680759/justin-trudeau-brownface-photo/ Last accessed 10th of February 2021.

[121] Suvi Uski and Airi Lampinen. 2016. Social norms and self-presentation on social network sites: Profile work in action. *New Media & Society* 18, 3 (2016), 447–464. https://doi.org/10.1177/1461444814543164

[122] Elham Vaziripour, Justin Wu, Reza Farahbakhsh, Kent Seamons, Mark O'Neill, and Daniel Zappala. 2018. A Survey of the Privacy Preferences and Practices of Iranian Users of Telegram. In *Proc. of the Symp. on Network and Distributed Sys. Secu., Workshop on Usable Secu. (USEC'18)*, Vol. 1. Internet Society, San Diego, CA, USA, 20. https://doi.org/10.14722/usec.2018.23033

[123] Nishant Vishwamitra, Yifang Li, Kevin Wang, Hongxin Hu, Kelly Caine, and Gail-Joon Ahn. 2017. Towards PII-based Multiparty Access Control for Photo Sharing in Online Social Networks. In *Proc. of the ACM on Symp. on Access Control Models and Tech. (SACMAT'17)*. Assoc. for Comp. Mach. (ACM), Indianapolis, IN, USA, 155–166. https://doi.org/10.1145/3078861.3078875

[124] Yang Wang, Gregory Norcie, Saranga Komanduri, Alessandro Acquisti, Pedro Giovanni Leon, and Lorrie Faith Cranor. 2011. "I regretted the minute I pressed share": a qualitative study of regrets on Facebook. In *Proc. of the Symp. on Usable Priv. and Secu. (SOUPS'11)*. Assoc. for Comp. Mach. (ACM), Pittsburgh, PA, USA, 1–16. https://doi.org/10.1145/2078827.2078841

[125] Frank W Weathers, Brett T Litz, Terence M Keane, Patrick A Palmieri, Brian P Marx, and Paula P Schnurr. 2013. The PTSD checklist for DSM-5 (PCL-5). https://www.ptsd.va.gov/ Scale available from the National Center for PTSD, Last accessed 17th of November 2020.

[126] Wikipedia. 2021. Deepfake. https://en.wikipedia.org/wiki/Deepfake Last accessed 10th of February 2021.

[127] Anders Wikström and Roberto Verganti. 2013. Exploring storyboarding in pre-brief activities. In *DS 75-7: Proc. of the Int. Conf. on Engineering Design, Design for Harmonies, Vol. 7: Human Behaviour in Design, Seoul, Korea (ICED'13)*. Design Society, Scotland, 11–22. https://www.designsociety.org/publication/34565/Exploring+storyboarding+in+pre-brief+activities

[128] Jakob Wirth, Christian Maier, Sven Laumer, and Tim Weitzel. 2019. Perceived Information Sensitivity and Interdependent Privacy Protection: A Quantitative Study. *Electronic Markets* 29, 3 (Sept. 2019), 359–378. https://doi.org/10.1007/s12525-019-00335-0

[129] Ryan Wishart, Domenico Corapi, Srdjan Marinovic, and Morris Sloman. 2010. Collaborative Privacy Policy Authoring in a Social Networking Context. In *Proc. of the IEEE Int. Symp. on Policies for Distributed Sys. and Networks (POLICY'10)*. IEEE, Fairfax, VA, USA, 1–8. https://doi.org/10.1109/POLICY.2010.13

[130] Pamela Wisniewski, Heather Lipford, and David Wilson. 2012. Fighting for my space: coping mechanisms for SNS boundary regulation. In *Proc. of the ACM Conf. on Human Factors in Comp. Sys. (CHI'12)*. Assoc. for Comp. Mach. (ACM), Austin, TX, USA, 609–618. https://doi.org/10.1145/2207676.2207761

[131] Pamela Wisniewski, Heng Xu, Heather Lipford, and Emmanuel Bello-Ogunu. 2015. Facebook apps and tagging: The trade-off between personal privacy and engaging with friends. *Jour. of the Assoc. for Info. Science and Tech.* 66, 9 (2015), 1883–1896. https://doi.org/10.1002/asi.23299

[132] Franklin E Zimring and Gordon Hawkins. 1995. *Incapacitation: Penal confinement and the restraint of crime.* Stud. in Crime and Public Policy, Oxford, UK. https://bit.ly/3pc9Qzn