Unconsented Data Transfusions: Attitudes Towards Extracting Personal Device Data for Public Health Emergencies

Colin Watson
Open Lab
Newcastle University
Newcastle upon Tyne, UK
c.watson8@newcastle.ac.uk

Jan David Smeddinck
Open Lab
Newcastle University
Newcastle upon Tyne, UK
jan.smeddinck@newcastle.ac.uk

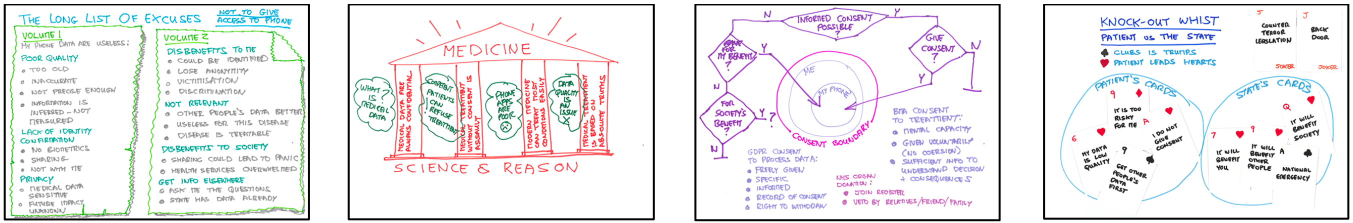

Figure 1: Four approaches to theme generation from coded data (see video figure). Left to right 1a) The long list of excuses, 1b) Medicine, 1c) Consent, 1d) Knock-out whist (card sorting).

ABSTRACT

Despite privacy and security concerns, personal data on smartphones could be of beneficial use to society, for example during national emergencies. User attitudes were collected through a small focus group approach to reveal what citizens' opinions may be towards extraction of medical data in the event of a public health incident. Thematic analysis revealed four themes with an overarching theme of "my phone is part of my body". This small-scale proof of concept study established individuals view smartphones akin to organs or limbs, where forced access, without consent, is assault. They consider the benefits to society of unconsented access to medical and other personal data on mobile devices must be overwhelming before such acquisition is considered acceptable. The analysis also points to the difficulty of gaining consent, a lack of knowledge about legal aspects, and a distrust about the state collecting data.

CCS CONCEPTS

• Security and privacy → Human and societal aspects of security and privacy → Social aspects of security and privacy • Information systems → Information systems applications → Mobile information processing systems

KEYWORDS

Privacy, security, remote access, data, sensing, qualitative study

1 Introduction

An increasing amount of personal data ("any information relating to an identified or identifiable natural person" [8]) is being recorded on smartphones. Some of this may be useful to assist in diagnosis and treatment of individuals and to mitigate adverse societal effects during public health emergencies. Despite debate about the balance between protecting and safeguarding privacy and delivering public services [21], little is known concerning citizens' views on NHS England, as an arm of the State and an exemplary public health institution, utilising such data *without freely expressed consent*, and consequently there has been a lack of information regarding attitude formation and public opinion [11]. Other work has focused on data sharing between health professionals, or use of health data for research and other secondary purposes [28]. Our work was conducted to inform policy about personal responsibilities within national public health plans and guidance, such as by NHS England [16,17]. The value of personal data varies depending upon the perspective [27] and privacy is contextual [26]. This pre-study informs a larger ongoing project on public health data policies and interaction, setting out to illicit citizens' attitudes to the State having direct access to their personal phone-stored medical data based around the question "how do citizens view forced unconsented access to their own smartphone data during medical emergency situations?", where data is accessed, extracted and used against the will of the individuals, and where consent is hard to gain [13].

The focus group we conducted to present participants with scenarios to elicit attitudes around different affliction and data access scenarios was executed before the impact of the coronavirus / Covid-19 pandemic and the resulting grave international impact became apparent. However, the current developments provide a timely relevance to our research, as it can be relevant to a) understanding the attitudes towards digital technologies being developed to support responses, such as contact-tracing applications, some of which are made mandatory in certain regions, as well as b) informing design implications or considerations for implementations of such technologies that are aware of user concerns around data access and consent.

This project provides insights into people's opinions by collecting views of a small number of United Kingdom citizens concerning the State accessing personal medical data stored on their own smartphones. The outcomes can inform follow-up work towards deriving design requirements for technologies and application procedures in the area of using personal-device data as data sources in the context of public health.

2 Background

Consent requirements in General Data Protection Regulations (GDPR) introduced additional protections for data subjects [8] which have implications in a healthcare context through the need to gain "informed consent" [20]. This has led to greater awareness of the need to implement universal usability and privacy by design principles ensuring consent is sufficient [18]. However, GDPR defines other bases for processing personal data lawfully including "processing is necessary in order to protect the vital interests of the data subject or of another natural person" and "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller".

It has been shown that people may be willing to share data from lifestyle and fitness apps for use in medical research [5], but personal-device derived data also has the potential to assist disease surveillance, preparation and response [12]. Pooling individual data by opportunistic sensing (without the data subject's intervention) risks leaking sensitive data [29]. Lack of trust has led to failures of national medical data-sharing projects [4] where it is necessary to also address the "social dimensions of sharing data, including citizens' expectations and concerns". Full regulatory compliance has been found to be inadequate [22], and both social and technical factors need to be considered together when developing such systems.

The recent coronavirus / Covid-19 pandemic underlines the relevance of considerations around consent and data access from private devices, as many digital technologies are being developed and deployed in a hurried manner that are meant to support the responses at local, national and international scales. While digital technologies, such as contact-tracing applications, promise crucial potential benefits, the public debate around privacy concerns, data ownership and potentials for misuse clearly evidence a need for research to better understand the nature of such concerns, as well as resulting implications for the design and application processes of technologies in this space. While early research is now looking into attitudes around the specifics of contact-tracing applications [30], this work provides a more general exploration of attitudes and values around data access of personal digital-device data for public health purposes and explores possible differences in attitudes based on the type of health concern that the data collection is intended to address.

3 Method

To facilitate an approach for interpretation of meaning in the data collected that is less predetermined or biased by questions, a focus group method was selected [2]. After ethical approval by Newcastle University, a single-participant pilot and a three-participant pre-study semi-structured discussion group, time-limited to 15 minutes each, were undertaken. The convenient subjects were self-selecting digitally literate trainee researchers from non-vulnerable groups attending a research event, aged 20-39 years old, living in England. Two identified as female (pseudonyms: Helen, Sue) and two as male (George, Miguel).

A conductor script detailed the structure and key talking points of the focus group.

The assisted discussion, moderated by the researcher, was framed to illicit a range of views, moving from a more general medical data consent topic regarding a heart condition, to more specific national emergency issues including a patient with tuberculosis and an influenza pandemic.

These scenarios were chosen to reflect an increase in severity with respect to the potential relevance of shielding the population beyond an individual patient and also to investigate the relationship between attitudes towards data access relative to how meaningful data from digital devices is likely to be with regard to different afflictions. To provoke open discussion, "personal data" or "medical data" were not further defined.

Each discussion was audio recorded. Following verbatim transcription by the research team, inductive thematic analysis [2] was performed using a social constructionist approach, set within a critical realist ontology. Following thorough reading and familiarisation with the transcripts when initial noticings were made, complete coding and theme identification were undertaken by the lead author using visually and textually supported creative mind-mapping, as illustrated in Figure 1 (a-d) – see also the accompanying video figure. The coding included both data-derived and researcher-derived codes. Subsequently, candidate themes were identified, reviewed and assessed by checking back to the original coding, re-listening to the audio recordings and through discussion with the co-author before selecting best-fitting final themes.

4 Findings

The reflexive "organic" thematic analysis of the coded data, generated themes which are more developed and tell a story about the data with a central unifying concept, instead of being domain summaries [6]. The analysis highlighted an overarching theme of *my phone is part of my body* comprising four themes: *the sanctity of medical science*; *consent trumps all …doesn't it?*; *data validity matters*; and *access is risky for individuals.* Two have subthemes as shown in Figure 2, on the following page.

Participants construct their view of smartphone data as an inherent part of their body, such that the phone is a vital organ leading to the overarching theme of *my phone is part of my body.* and the consequent metaphor used in the paper's title that taking data from a personal phone is the equivalent of transferring a vital matter like blood (transfusion).

4.1 The sanctity of medical science

Participants perceived medicine as a hard science where the truth exists and only needs to be revealed. The theme *the sanctity of medical science* captures their assumptions, where formal rules exist to evaluate data evidence to inform diagnosis, prognosis, therapy and clinical and health care issues. Medical data as evidence is given a high value, considered sensitive and therefore very confidential.

Participants stated the direct link between quality of medical data with good diagnosis and were concerned that smartphone data is not up to this high standard *"how can you make a diagnosis with that – it is just false information... I don't think they will trust it" (George).* This demonstrates a presumption that medicine primarily uses a scientific evidence-based approach, using a combination of clinical evidence, clinical research and patient values [14]. There was no challenge of medical efficacy indicating a belief that medical professionals can be trusted and also that most conditions are *"treatable" (George).*

Like other medical data, smartphone data are sensitive requiring a high degree of confidentiality which is a societal norm:

> *"Yeah, because we have reached this point where we consider data to be confidential right, even medical records" (George)*

Throughout the discussion phone data in general is treated like medical data – something which is personal, inherent, private and not to be touched by others without permission.

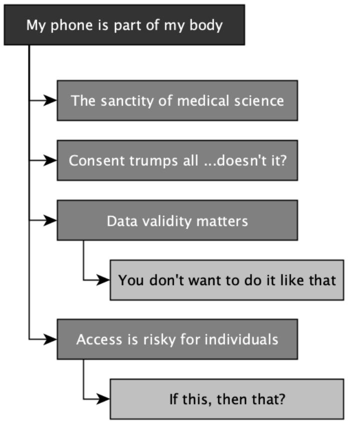
My phone is part of my body
The sanctity of medical science
Consent trumps all ...doesn't it?
Data validity matters
You don't want to do it like that
Access is risky for individuals
If this, then that?

Figure 2: Overarching theme, themes and subthemes.

4.2 Consent trumps all ...doesn't it?

This theme brings together views mainly relating to consent for use of data, but also touches on consent for medical treatment. This theme captures an assumed agreed underlying principle, held by all participants, that informed consent is a prerequisite for data access, extraction and use.

Helen pronounced that accessing medical data from a phone without permission was "*like an invasion of privacy*". Everyone stated that if consent were given to access phone data, *"there is no controversy there... why not?" (George),* but there was a strong view that access against a capable person's wishes must never occur *"I don't think they should" (Helen), "I think not" (George), "(pause, intakes of breath and gasps)", "definitely not" (George), "no" (Sue).* It was also believed that people must be allowed to make their own decisions and should have the right to refuse:

> *"...that's his choice... much like it's a Jehova's Witness's choice not to receive a blood transfusion erm... even if the medical... the staff think that's the most appropriate treatment, they can still refuse that... erm... and I guess it's the same scenario here that personal choice overrides however much we might disagree..." (Helen)*

This illustrates how refusal to permit data access is equated with the situation where patients can refuse medical treatment:

> *"...conscious responsive patients have a right to refuse treatment..." (Helen)*

As Helen alluded to guidance for health practitioners and explained how this can be overruled in an emergency situation by medical practitioners if the person is unable or incapable of providing consent at the time [3,15]. This comparison with medical treatment reinforces the idea that phones are metaphorically an organ or limb of a person's body.

There was a realisation amongst some of the participants that more serious emergencies could tip the balance for access towards the needs of society. However, there were reservations from both Sue *"I think it's okay, but..."* and Helen *"I still have big reservations about it".* This continued lack of acceptance in the worst cases occurs even when nothing can be done about forced access. It is difficult to see how in such circumstances consent can be freely given, specific and informed [9].

During the analysis phase, it was realised that there had been no discussion of what constitutes medical data. The contagious disease scenarios alluded to location data primarily, but in other contexts this alone would not be classified as personal health data. Health data is a type of special category data under GDPR.

Even though near the start of the discussion George asked *"first of all there is no requirement for him to do that? Right?",* and later reconfirmed *"and there is no requirement for him to do so",* knowledge about how data can be taken legally without consent did not otherwise surface. Subject to certain safeguards, GDPR allows for some usage without explicit consent including "protecting against serious cross-border threats to health..." [8,10]. Additionally, in the United Kingdom, devices can already be seized – and communications data harvested – under anti-terror legislation [24,25].

4.3 Data validity matters

A particular feature of the focus group data were the various and repeated reasons given why medical data on smartphones is invalid. The theme *data validity matters* gathers these strands, highlighting how the participants veered to find explanations of why the data is useless rather than defending their choices.

There was a concern that data is imprecise, has gaps, may relate to someone else and that phone sensors are not directly measuring the specific condition of interest:

> *"...or its, it's you know, it's not something accurate. It infers data from other things... it doesn't directly measure... so I don't think they will trust it." (George)*

A number of other reasons for not sharing data were also pronounced. These were considered to be a subtheme of *data validity matters* called *you don't want to do it like that,* which tried to capture further reasons why the data was no use. These encompass that the data sought do not exist, the data is too generic, but also wider reasons of inadmissibility (already treatable without this data, other people's data is of more use) and two reasons suggesting that alternative channels would be better (could be obtained from other sources, and conscious people could simply be asked for information *"without them needing to look at another source of information such as their phone" (Helen*). Lastly, this subtheme includes the realisation that if the State or other parties have access to the phone, the data could have been tampered with, thereby invalidating it.

4.4 Access is risky for individuals

The final theme brings together participants' concerns over potential negative impacts. Like medical interventions, phone data *access is risky for individuals*. This appeared in the later stages of discussion, where there is an increasing seriousness in scenario conditions and the argument for permitting access for the good of society gained weight. Discrimination and victimisation were the greatest concerns, so anonymity is raised as an important criteria for use of data: *"yes if it's kept anonymous" (Miguel).*

But the highest risks were captured in the subtheme *if this, then that?* when the implication of forced access by the State to phone data dawned on the participants:

> *"allowing a government organisation to have this access, means that there's… like a… you know… there's access… to your data, by …" (George)*
>
> *"Some sort of backdoor?" (Moderator) "Yeah, exactly." (George)*

If the State is able to access the data without consent, against the choice of people *"that's a bit of a slippery slope" (Helen).* Backdoors in software and hardware undermine trust, as they could be misused politically and are security vulnerabilities that can be exploited by other parties [23].

5 Discussion

As a limitation of this study, the scope of what is and is not considered medical data, and the purposes of use have not been sufficiently clarified. However, the findings support previous work [13] in the Ubicomp space which found that consent is a complex and multifaceted issue, and the proposed guidelines for Ubicomp do seem to be generally applicable in the problems raised in this study (see Figure 2).

The participants expressed how people construct meanings around technologies that clearly impact the way these are embedded in – and affect – daily living. They explicated the non-static nature of consent – how it changes over time and with circumstances, in a similar way to previous findings [1,19,26]. Concerns about data validity suggest further investigations to differentiate between those issues which are being used as excuses, and those which are reasons not to allow data access.

This work indicates that smartphones can be perceived as tools forming extensions to human bodies, not merely in a McLuhanian metaphorical sense, but quite directly with innate emotional relevance to the people using the technology. This underlines the relevance of very sensitive and considerate approaches towards data collection and harvesting from personal digital devices, placing the relevance of adequate consent procedures near considerations for human-subject studies or even medical procedures, if adverse impacts are to be avoided and critical levels of adherence are to be achieved.

This study underlines a need for greater understanding of the interaction between the State and individuals. People do not seem to be aware of how and when their devices and their data can be accessed legally, and this could mean that in the event of a national public emergency, when people's cooperation is most needed, conflict might occur, undermining efforts by national organisations, such as the NHS. The perceived close relationship between the NHS England and other parts of the State, such as security services, further erodes trust in such mechanisms.

In the light of the ongoing pandemic, lockdowns and deployments of digital technologies for data collection for public health purposes, such as contact-tracing applications, we are currently augmenting this work with follow-up studies to investigate the impact on attitudes and to also investigate the quantitative differences between the presented scenarios.

The issue of how data might be accessed without consent, and the assumption of a technical backdoor, is not specific to medical data. It reflects a wider wariness of the State and other parties being able to undertake surveillance or extraction without user control – an invasion of the body as presented by the participants. A broader range of participants is needed to gather further evidence and draw fuller conclusions, and participant selection needs to avoid possible confounding variables such as participant's own health conditions or disabilities. Age, religious beliefs, and attitudes to organ donation and euthanasia may also be relevant factors where each participant's decision-making style and risk-taking attitudes such as these are known to affect views on privacy and security [7].

6 Conclusion

We presented results of a focus group discussion set up to illicit attitudes towards unconsented phone data access during public health emergencies. The findings highlight a high degree of reluctance by the participants to any form of unconsented access in the absence of overwhelming evidence of greater society-wide benefits. A key finding is that the *purpose* of use is considered a more important characteristic than the *type* of personal data.

Despite the results being drawn from a small sample, a noteworthy result from this explorative formative contribution is that health authorities need to ensure they earn and maintain the trust of the public, especially during national incidents. The participants regarded the close organisational proximity of NHS England with the State as a contaminating effect on trust, especially since they perceive personal phones as part of their bodies and Helen thought the extraction of data like an unconsented blood transfusion.

Although the participants were otherwise very digitally literate, there was a lack of knowledge of the State's legal powers, and their own obligations and rights. It has been discussed how policymakers should seek to gain further, wider viewpoints, using the current findings to advise that work. This can then be used to inform policy about personal responsibilities within national public health plans and guidance.

ACKNOWLEDGEMENT

This work was funded through the EPSRC Centre for Doctoral Training in Digital Civics at Newcastle University (EP/L016176/1).

REFERENCES

[1] Alex Bowyer, Kyle Montague, Stuart Wheater, Ruth McGovern, Raghu Lingam, and Madeline Balaam. 2018. Understanding the Family Perspective on the Storage, Sharing and Handling of Family Civic Data. In CHI '18. https://doi.org/10.1145/3173574.3173710

[2] Braun, Virginia and Clarke, Victoria. 2013. Successful Qualitative Research. Sage Publications Ltd. Retrieved November 3, 2018 from https://uk.sagepub.com/en-gb/eur/successful-qualitative-research/book233059

[3] British Medical Association. Consent to treatment - adults with capacity. Retrieved January 4, 2019 from https://www.bma.org.uk/advice/employment/ethics/medical-students-ethics-toolkit/6-consent-to-treatment-capacity

[4] Pam Carter, Graeme T Laurie, and Mary Dixon-Woods. 2015. The social licence for research: why care.data ran into trouble. Journal of Medical Ethics 41, 5: 404–409. https://doi.org/10.1136/medethics-2014-102374

[5] Juliana Chen, Adrian Bauman, and Margaret Allman-Farinelli. 2016. A Study to Determine the Most Popular Lifestyle Smartphone Applications and Willingness of the Public to Share Their Personal Data for Health Research. Telemedicine and e-Health 22, 8: 655–665. https://doi.org/10.1089/tmj.2015.0159

[6] Clarke, Victoria. 2017. What is thematic analysis, when is it useful, and what does "best practice" look like? Retrieved November 12, 2018 from https://www.youtube.com/watch?v=4voVhTiVydc

[7] Egelman, Serge and Peer Eyal. 2015. Predicting privacy and security attitudes. ACM SIGCAS Computers and Society 45, 1. Retrieved January 5, 2020 from https://dl.acm.org/doi/abs/10.1145/2738210.2738215

[8] European Parliament. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). eur-lex.europa.eu. Retrieved January 3, 2020 from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e40-1-1

[9] Information Commissioner's Office. Guide to Data Protection: GDPR: Lawful basis for processing: Consent. Retrieved January 4, 2019 from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/

[10] Information Commissioner's Office. Guide to Data Protection: GDPR: What are the conditions for processing? Retrieved January 4, 2019 from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-conditions-for-processing/

[11] Daniel Katz. 1966. Attitude Formation and Public Opinion. The ANNALS of the American Academy of Political and Social Science 367, 1: 150–162. https://doi.org/10.1177/000271626636700116

[12] Patty Kostkova. 2015. Grand Challenges in Digital Health. Frontiers in Public Health 3. https://doi.org/10.3389/fpubh.2015.00134

[13] Ewa Luger and Tom Rodden. 2013. An informed view on consent for UbiComp. UbiComp 2013 - Proceedings of the 2013 ACM International Joint Conference on Pervasive and Ubiquitous Computing. https://doi.org/10.1145/2493432.2493446

[14] Izet Masic, Milan Miokovic, and Belma Muhamedagic. 2008. Evidence Based Medicine – New Approaches and Challenges. Acta Informatica Medica 16, 4: 219–225. https://doi.org/10.5455/aim.2008.16.219-225

[15] NHS Blood and Transplant. How is consent for organ donation established? www.organdonation.nhs.uk. Retrieved January 4, 2019 from /helping-you-to-decide/about-organ-donation/faq/consent/

[16] NHS England. 2017. Incident Response Plan (National). Retrieved December 8, 2018 from https://www.england.nhs.uk/publication/nhs-england-incident-response-plan-national/

[17] NHS England. Emergency Preparedness, Resilience and Response (EPRR). Retrieved December 8, 2018 from https://www.england.nhs.uk/ourwork/eprr/

[18] Yvonne O'Connor, Wendy Rowan, Laura Lynch, and Ciara Heavin. 2017. Privacy by Design: Informed Consent and Internet of Things for Smart Health. Procedia Computer Science 113: 653–658. https://doi.org/10.1016/j.procs.2017.08.329

[19] Aisling Ann O'Kane, Helena Mentis, and Eno Thereska. 2013. Non-static nature of patient consent: Shifting privacy perspectives in health information sharing. 553–562. https://doi.org/10.1145/2441776.2441838

[20] John Mark Michael Rumbold and Barbara Pierscionek. 2017. The Effect of the General Data Protection Regulation on Medical Research. Journal of Medical Internet Research 19, 2. https://doi.org/10.2196/jmir.7108

[21] Select Committee on the Constitution. Surveillance: Citizens and the State - Volume I: Report. House of Lords. Retrieved January 3, 2020 from https://publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/18.pdf

[22] Tejal Shah, Louise Wilson, Nick Booth, Olly Butters, Joe McDonald, Kathryn Common, Mike Martin, Joel Minion, Paul Burton, and Madeleine Murtagh. 2019. Information-sharing in health and social care: Lessons from a socio-technical initiative. Public Money & Management 39, 5: 359–363. https://doi.org/10.1080/09540962.2019.1583891

[23] Shannon Lear. 2018. The fight over encryption: Reasons why congress must block the government from compelling technology companies to create backdoors into their devices. Cleveland State Law Review.

[24] UK Government. 2000. Terrorism Act 2000. Retrieved January 4, 2020 from http://www.legislation.gov.uk/ukpga/2000/11/contents

[25] UK Government. 2016. Investigatory Powers Act 2016. Retrieved January 4, 2020 from http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted

[26] Yuhuai Wang, Huichuan Xia, Yaxing Yao, and Yun Huang. 2016. Flying Eyes and Hidden Controllers: A Qualitative Study of People's Privacy Perceptions of Civilian Drones in The US. Proceedings on Privacy Enhancing Technologies 2016: 172–190. https://doi.org/10.1515/popets-2016-0022

[27] Watson, Colin and Leach, John. 2010. The Privacy Dividend. Information Commissioner's Office. Retrieved from https://ico.org.uk/media/about-the-ico/documents/1042345/privacy-dividend.pdf

[28] Wellcome Trust. 2018. Understanding Patient Data, Public Attitudes to Patient Data Use. Retrieved from https://understandingpatientdata.org.uk/sites/default/files/2018-08/Public%20attitudes%20key%20themes_0.pdf

[29] Daqing Zhang, Bin Guo, and Zhiwen Yu. 2011. The Emergence of Social and Community Intelligence. Computer 44, 7: 21–28. https://doi.org/10.1109/MC.2011.65

[30] Lucy Simko, Ryan Calo, Franziska Roesner, and Tadayoshi Kohno. PRE-PUBLICATION. COVID-19 Contact Tracing and Privacy: Studying Opinion and Preferences. 32.