Volume **3** (2) 2021 https://doi.org/10.5204/lthj.2012

To App or Not to App? Understanding Public Resistance to COVID-19 Digital Contact Tracing and its Criminological Relevance

Anita Lavorgna, Pamela Ugwudike, Leslie Carr, Yadira Sanchez Benitez and Gopala Sasie Rekha
University of Southampton, United Kingdom

Abstract

In the context of the COVID-19 pandemic, digital contact tracing has been developed and promoted in many countries as a valuable tool to help the fight against the virus, allowing health authorities to react quickly and limit contagion. Very often, however, these tracing apps have faced public resistance, making their use relatively sparse and ineffective. Our study relies on an interdisciplinary approach that brings together criminological and computational expertise to consider the key social dynamics underlying people's resistance to using the NHS contact-tracing app in England and Wales. The present study analyses a large Twitter dataset to investigate interactions between relevant user accounts and identify the main narrative frames (lack of trust and negative liberties) and mechanisms (polluted information, conspiratorial thinking and reactance) to explain resistance towards use of the NHS contact-tracing app. Our study builds on concepts of User eXperience (UX) and algorithm aversion and demonstrates the relevance of these elements to the key criminological problem of resistance to official technologies.

***Keywords**:* COVID-19; tracing app; algorithm aversion; user experience; public compliance; data-driven surveillance.

Introduction

In response to the COVID-19 pandemic, contact-tracing apps have been developed and released in several countries, including the UK, as a measure to combat the spread of COVID-19, speeding up the tracing of the contacts of individuals found to be infected.[1] At the core of this approach is the notion that, although the novel coronavirus spreads too rapidly to be contained by manual contact tracing, it can be controlled and contained through the use of automatised contact tracing via apps, if used by a sufficient number of people.[2] Such apps are generally based on practical hardware technologies (e.g., Bluetooth low energy and possibly GPS data), meaning they can be used by virtually anyone with a smartphone. In practice, however, these apps lack sufficient real-life testing. This represents a problem because their effectiveness, irrespective of the technology used, depends on socio-behavioural factors, such as public confidence and trust in the protection of privacy.[3]

As stated in a recent editorial in *Nature* (2020), despite the global nature of the pandemic, at present, there is no global standard for the development of COVID-19 tracing apps. This raises a series of concerns, particularly accuracy concerns (because incorrect information being sent could create severe harm) and privacy concerns (in terms of whether individuals can be identified from the aggregated datasets).[4] In light of this, it is arguably unsurprising that these apps—particularly in privacy-conscious countries—have faced strong public resistance, and their resulting use has made them relatively ineffective.

[1] Ada Lovelace Institute, Exit Through the App Store?
[2] Ferretti, "Quantifying SARS-CoV-2 Transmission," 6491.
[3] Sweeney, "Tracking the Debate on COVID-19 Surveillance Tools," 301–304; von Wyl, "A Research Agenda," 29.
[4] Among others, see Farronato, "How to Get People to Actually Use Contact-tracing Apps"; Rowe, "Contact Tracing Apps and Value Dilemmas."

Except where otherwise noted, content in this journal is licensed under a Creative Commons Attribution 4.0 International Licence. As an open access journal, articles are free to use with proper attribution. ISSN: 2652-4074 (Online)

© The Author/s 2021

The present study relies on an interdisciplinary approach that brings together criminological and computational expertise to investigate a large Twitter dataset as a means of unravelling the social dynamics underpinning people's resistance to the NHS contact-tracing app across England and Wales. This study focuses on the broader issue of resistance to governance strategies that, in most cases, may not or should not be explicitly defined as 'criminal' or 'deviant' acts but that has nevertheless attracted the attention of criminology, with cultural criminologists, for example, exploring public resistance to forms of power and authority that are perceived as harmful and unjust.[5] Our study focuses on a specific form of resistance: public resistance to the perceived harms of governance technologies (i.e., data-driven tools for surveillance and control). This crucial area of study has attracted limited criminological attention but has become increasingly topical. Our study brings criminology to the forefront of this fast-growing area by offering new insights into the issue of public resistance to the NHS tracing app, the underpinning mechanisms (particularly the perceived harms of surveillance through governance tools) and its implications. More broadly, our study builds on conceptual tools from tech-design studies and demonstrates their relevance to a key criminological problem which is resistance to official technologies. We focus on the concepts of User eXperience (UX) and algorithm aversion, both of which draw attention to the real-world contexts in which technology is deployed, to enhance criminological understandings of the factors underpinning the resistance to official technologies, such as digital-tracing apps and identity-remedial strategies. The rapid proliferation of such automated decision-making technologies across several western and non-western jurisdictions renders this enquiry essential.

Theoretical Framework

Data-driven technologies are increasingly used to automate key policy decisions in the public and private sectors, and research suggests that public buy in or acceptance of a technology is crucial for adoption. This is particularly true for technologies that, unlike coercive systems (e.g., electronic-surveillance devices deployed in justice systems), rely on voluntary adoption. Examples include the plethora of surveillance technologies that have emerged with the advent of recent technological advances. This paper focuses on the COVID-19 Track and Trace app that was introduced across England and Wales in 2020 to surveil individuals who tested positive for the virus to contain the pandemic. Research, however, has pointed to growing public resistance to this and similar apps.[6] Despite this, there is limited criminological insight into the mechanisms underpinning this resistance.

Contact-tracing apps are, in a broad sense, surveillance technologies that seek to govern and control human conduct. They differ substantially in nature and scope from technologies used traditionally in criminal justice settings, such as biometric surveillance technologies[7] and electronic monitoring devices.[8] Unlike criminal-justice technologies, tracing apps are (or should be) designed to reduce the risk of their use for mass surveillance and should have a defined purpose of promoting public health outcomes. Contact-tracing apps also occupy a very different space in public discussions on surveillance and, so far, appear to have received limited media and scholarly attention. However, although the technologies we focus on in this contribution are substantively different, there is a common denominator connecting them all to the currently proliferating smart technologies—they are all data driven and give rise to similar concerns of data injustice, privacy violations, opacity and other harms that erode public trust.[9]

Criminological studies of surveillance technologies focus mainly on coercive systems, such as electronic monitoring devices.[10] The paucity of criminological insight is surprising, not least because the problem of resistance to official, policy-driven technologies is of great relevance to the discipline and particularly to the fast-growing strand of criminology that focuses on the design and adoption of emerging data-driven technologies, some of which include the rapidly proliferating predictive algorithms. To address this dearth of criminological insights, the present study draws on sections of the artificial intelligence design literature that explores the UX of data-driven technologies. Originating in industry settings and initially used by organisations seeking to embed user feedback in tech designs, UX studies generate the information required to develop responsive, user-friendly systems. UX studies map people's perceptual and behavioural responses to an anticipated or already-deployed system.[11] While UX is dynamic and evolves in tandem with technological advances, a key discovery of UX research is that user endorsement of the functionality, utility, usability and efficiency of a system is necessary for tech adoption. Added to this, to encourage uptake—even in multi-stakeholder conditions—tech design should be responsive to broader concerns, such as the sociocultural contexts of use and users' entrenched beliefs and interests.[12] Tech design should also factor in the

[5] Ferrell, "In Defence of Resistance"; Smith, "Driving Politics."
[6] See, for instance, Abeler, Support in the UK.
[7] For instance, Fussey, "'Assisted' Facial Recognition."
[8] Nellis, "Surveillance-based Compliance."
[9] Denick, "Exploring Data Justice"; Lavorgna, "The Datafication Revolution."
[10] Nellis, Standards and Ethics in Electronic Monitoring.
[11] Hinderks, "Developing a UX KPI."
[12] Ferreira, "Universal UX Design."

extent to which a system could influence daily routines or even generate or exacerbate stressful conditions for users.[13] Related factors, such as public trust in the technologies[14] and the authority encouraging adoption (in this case, the government), are also relevant, not least because, as Devine and colleagues observed, 'high levels of trust are seen to be a necessary condition for the implementation of restrictive policies and for public compliance with them'.[15]

Studies investigating barriers to tech uptake also suggest that ignoring or paying insufficient attention to UX can foment 'algorithm aversion', a term that refers to the general reluctance of target users to adopt technologies designed to fully or partly automate tasks, instead preferring human judgement, particularly after observed or reported failures of the technologies.[16] Dietvorst and colleagues, however, found that uptake can be improved if users can modify what they consider to be flawed algorithms, demonstrating the importance of user input in tech design.[17] Insights from research into UX and algorithm aversion draw attention to the importance of exploring users' discourses about their experiences of new technologies to uncover mechanisms of resistance. Our study explores these issues, focusing on the digital-tracing app, the NHS Test and Trace, introduced in England and Wales in 2020.

Tracing Apps, Public Concerns and Compliance

In the unfolding of the COVID-19 pandemic, contact-tracing apps have been developed and released in various countries worldwide, and their use has become a subject of public debate. In response to a degree of public resistance to these apps, researchers and media commentators (as exemplified below, and generally by relying on studies based on national surveys or expert interviews) have sought to explain the factors underpinning this resistance.[18] While the results of these contributions are difficult to generalise in the evolving COVID-19 situation (where people's opinions can easily change depending on the evolution of the pandemic and the health, social and economic crises it provokes) and across countries (as many factors behind people's resistance may be situational and culture specific), they nonetheless offer important insights into individual choices on this issue, allowing common patterns to be identified. From this literature, in line with Farronato and colleagues,[19] privacy concerns appear to be the main barrier to the adoption of tracing apps. Privacy, as appears in those studies, seem to be broadly intended and is mainly associated with an ideological commitment to avoid interference from governments or big tech companies; in any case, this concept is not discussed in detail. This could be symptomatic of the sociocultural contexts of use. According to UX research, users vary in their beliefs about the extent to which the authority encouraging use can be trusted to embed privacy protections in the system. Privacy concerns could also reflect the problem of algorithm aversion stemming from highly publicised data breaches in recent years.[20] Developers and proponents contend that the adoption of stricter privacy protections limits the effectiveness of the technology in controlling the spread of the virus. Nevertheless, the privacy concerns experienced by the public appear to outweigh the perceived benefits to an extent. For example, the value of tracing apps is not as immediately clear as it may have been if such apps had initially been implemented in small-sized communities before national rollout. This reinforces what UX studies have revealed about the importance of considering users' views on the utility of a new technology.

Concerns about privacy and data security are, unsurprisingly, also at the core of the debate in contexts in which minority groups risk persecution or where segments of the population are concerned that data leakages may lead to increased risk for and stigma against individuals who test positive for COVID-19. More generally, individuals may be reluctant to provide personal information when there is insufficient information and transparency about how an app works and how data are collected, protected, stored and shared.[21] In these cases, the concept of privacy appears to align with the defence of positive rights—such as freedom of expression and the conditions necessary for human flourishing—as well as with data protection rights. However, similar concerns have also been expressed in countries with stronger data-protection regulations (including the UK), with potential users concerned about privacy violations and the possibility that their personal data will be used to fuel data-driven surveillance by private companies or the government after the pandemic is over.[22]

[13] Tromp, "Design for Socially Responsible Behaviour."
[14] Consider, for instance, Shin, "User Perceptions of Algorithmic Decisions"; Shin, "Beyond User Experience."
[15] Devine, "Trust and the Coronavirus Pandemic."
[16] Berger, "Watch Me Improve"; Dietvorst, "Overcoming Algorithm Aversion."
[17] Dietvorst, "Algorithm Aversion."
[18] For instance, Farronato, "How to Get People to Actually Use Contact-tracing Apps."
[19] Farronato, "How to Get People to Actually Use Contact-tracing Apps."
[20] See, for instance, BBC News, "NHS Data Breach."
[21] Fitriani, "COVID-19 Apps."
[22] Farries, "Covid-tracing App may be Ineffective and Invasive of Privacy"; Garret, "A Representative Sample of Australian Participant's Attitudes"; O'Callaghan, "A National Survey of Attitudes"; Weaver, "Don't Coerce Public."

In line with the findings of UX studies that highlight perceived tech efficiency and trust in authorities are key concerns of the public, Panda Security's survey of nearly 2,000 members of the UK public found that the pandemic has brought issues of trust and its link to perceived competence to the fore.[23] In the survey, one-third of respondents had no trust in the government to successfully track and trace the virus through mobile apps at all. Similarly, using a 10-minute online survey administered in March 2020 (n = 1055) among British residents (asking hypothetical questions about future behaviour), Abeler and colleagues identified wide support for app-based contact tracing (with about three-quarters of respondents reporting that they would definitely or probably install the app—a figure that is comparatively higher compared with populations in other countries). However, respondents who lacked trust in the government were less favourable. Abeler and colleagues found that respondents' main reasons for not installing the app were a perceived increased risk of government surveillance after the epidemic, the fear that installing the app would lead to increased anxiety about the epidemic, and the fear of having your phone hacked. The same survey conducted in other western countries noted very similar results.[24] A number of other social and practical barriers to tracing app adoption have also been identified in UX research, including poverty, the inability to buy or use a smartphone, the inability to download the app, an unmet need for more information and support and concerns about phone-battery usage.[25]

However, in line with findings that perceived utility and efficiency can encourage user endorsement and adoption,[26] many individuals surveyed (with the precise proportion varying across countries from approximately 50% to 60% in most studies to higher in Abeler and colleagues' UK study) have recognised some benefit in downloading and using tracing apps, *in primis* for their potential to help family and friends, to engage in collective responsibility to the wider community and when the system is perceived as efficient, rigorous and reliable.[27] Lia and colleagues identified pro-socialness (i.e., voluntary actions a person conducts to help, take care of, assist or comfort others), COVID-19 risk perception, general privacy concerns, technology readiness and demographic factors as more important than app-design choices (e.g., decentralised design vs centralised design, location use and app providers) and the presentation of security risks as predictors of an individual's willingness to use tracing apps.[28]

Along with studies focusing on (potential) users' behaviours, conceptual, theoretical and systemic considerations surrounding contact-tracing apps have also been debated, with discussions on their system architecture, data management, privacy, security, proximity estimation and attack vulnerability.[29] Of particular interest are the concerns raised by Rowe, who, focusing on a tracing app launched in France after a heated public debate, took a critical stance.[30] Rowe stressed how the app—despite its short-term benefits—could create long-term concerns about a potential encroaching on civil liberties if the app induced significant risk to informational privacy, surveillance and habituation to security policies, potentially fomenting discrimination and public distrust. Others have also cast doubt on the necessity of tracing apps; for example, commenting on the situation in Singapore, Woo argued that it was the fiscal, operational and political capacities that were built up after the SARS crisis—rather than tracing apps—that contributed to Singapore's relatively low fatality rate (despite its high infection rate) and contact-tracing capabilities.[31] Indeed, it was likely a lack of technological literacy among some quarters of the population, though more likely concerns about data privacy and a lack of trust in the government's ability to safeguard individuals' personal data, behind the local TraceTogether app not being widely downloaded by the Singaporean population.

While the studies discussed so far reveal the key themes and issues—*in primis* privacy—affecting individuals' willingness to comply with the use of contact-tracing systems, they have some limitations. Methodologically, most of the studies used surveys administered over a limited timeframe, though public opinion on the pandemic likely changes as the pandemic evolves. Simko and colleagues longitudinally measured the evolving nature of public opinions in the US on the tension between effective technology-based contact tracing and the individuals' privacy using online surveys; however, the study's sample size of 100 participants per survey was very limited.[32] In addition, while UX studies suggest that exploring the willingness to comply with contact tracing (mostly in quantitative terms) can inform policy-making (as the effectiveness of an app largely depends on public willingness and the ability to support this type of measure), it is important to qualitatively consider the sociocultural and practical dynamics underlying public resistance to tracing apps or the socio-technical impediments to use them.

[23] Panda Security, "Apathy in the UK."
[24] Abeler, Support in the UK.
[25] Farries, "Covid-tracing App may be Ineffective and Invasive of Privacy"; Garret, "A Representative Sample of Australian Participant's Attitudes"; Megnin-Viggars, "Facilitators and Barriers to Engagement"; Tromp, "Design for Socially Responsible Behaviour."
[26] Ferreira, "Universal UX Design."
[27] O'Callaghan, "A National Survey of Attitudes"; Megnin-Viggars, "Facilitators and Barriers to Engagement"; Simko, "COVID-19 Contact Tracing and Privacy"; Walrave, "Adoption of a Contact Tracing App."
[28] Lia, "What Makes People Install a COVID-19 Contact-Tracing App?"
[29] Ahmed, "A Survey of COVID-19 Contact Tracing Apps"; Mbunge, "Integrating Emerging Technologies."
[30] Rowe, "Contact Tracing Apps and Values Dilemmas."
[31] Woo, "Policy Capacity and Singapore's Response to the COVID-19 Pandemic."
[32] Simko, "COVID-19 Contact Tracing and Privacy."

In our study, we offer an empirical, methodological and conceptual contribution that combines computational capacities to investigate a large social media dataset covering 10 months. We further offer qualitative expertise in criminology to reflect on emerging issues of public trust, governance and the use of personal data for public good. These issues are the basis of people's resistance to using tracing apps but are unlikely to peter out after the debate about COVID-19 contract tracing apps is over. From a criminological standpoint, our study uncovers new insights that can expand current understandings of resistance to the new data-driven surveillance technologies that are currently transforming the landscape of decision-making across the private and public sectors, including the justice system. While existing criminological literature has, to date, focused on coercive surveillance systems, such as electronic tags, generating highly useful insights,[33] our study expands the field by investigating a surveillance technology that relies on public acceptance and voluntary adoption for effective deployment.

Research Design

Inspired by insights from UX and algorithm-aversion studies, as well as other studies on public reactions to digital-tracing apps, we analysed a relatively large dataset of tweets to examine public discourse on the NHS COVID Track and Trace app in England and Wales and identify mechanisms of resistance. We identified and analysed relevant accounts and the interactions between them to understand the drivers of this national conversation and to identify the main narrative frames and mechanisms explaining and enabling people's resistance to using the tracing app. Tweets were collected retrospectively, starting with the oldest relevant tweet being published on 6 March 2020 and continuing until 31 December 2020. Tweets were collected if they included any combinations of the keywords and phrases (track and trace NHS; track and trace app; no to track and trace; track and trace I refuse; not use track and trace; against track and trace), which were chosen after preliminary manual searches to determine the most frequently occurring terms in this context. We identified relevant tweets *post hoc* from searches on the Twitter Web app (https://twitter.com/search-advanced) using the Web Data Research Assistant software developed by one of the present study's authors.[34] The search yielded a total of 54,941 tweets (including 4,269 hashtags) tweeted from 38,713 Twitter accounts over the 10 months considered.[35]

We adopted a sociotechnical approach, developed through a sequence of five main iterative stages: (1) developing keywords and hashtag lists, (2) automatised data collection through a computational tool, (3) identification of relevant hashtags and keywords in the dataset, (4) information extraction and qualitative analyses (through the use of keywords-in-context displays, sentiment analysis with n-grams, development and refinement of a qualitative conceptual map, and social network analyses) and (5) qualitative checks for bias minimisation. The methodological process is described in detail in the project report.[36] Though we used computational tools for the analysis (often associated with positivistic research approaches), we mainly relied on a constructivist epistemology. As such, this research did not aim to identify ultimate laws but rather to offer meanings that are relevant through interpretation.

Data Analyses and Results

Interactions Between Accounts and Conversation Drivers

First, we sought to understand the interactions between the accounts to identify the drivers behind relevant conversations. To do so, we mapped the conversational network obtained by connecting two accounts where one replied to or mentioned the other. We considered only those accounts that contributed a tweet in our collection—not the 18,351 other accounts that were mentioned—but that did not otherwise participate in the conversation by tweeting on the topic. The network was plotted in Gephi using the Force Atlas layout (see Figure 1). As Figure 1 shows, we identified (1) an outer ring consisting of 26,140 isolated individuals who tweeted but received no replies to their tweets; (2) a middle ring of 1,107 small disconnected groups (ranging from 2 to 99 accounts each) that replied to each other, accounting for 2,832 accounts in total; and (3) a strongly connected central core of 9,741 accounts. In other words, the outer ring consisted of just over two-thirds of the accounts, the central core of just over a quarter and the middle ring of the remaining 7%.[37] The network was coloured according to Gephi's

[33] Nellis, Standards and Ethics in Electronic Monitoring.
[34] Available for download at http://bit.ly/WebDataRA. The software is a Chrome browser extension that monitors pages that the researcher browses (e.g., social media timelines and search results) and saves relevant data and metadata as a spreadsheet.
[35] Of 38,713 accounts, 2,530 were considered 'dormant' (i.e., they were used to tweet on any subject less than once per week) and 1,437 were probably automated (as they tweeted more than 50 times per day).
[36] See Lavorgna, Understanding Public Resistance.
[37] The existence of the rings and their placement is an artefact of the Force Atlas network layout algorithm, determined by the balance of attractive forces configured between linked accounts and the repulsive forces between non-linked nodes. The network is coloured according to its partition/modularity/cliques and the node sizes are related to the number of inlinks (that is, the number of times that other accounts have contacted that account).

modularity calculations, which identify the parts of a network that are highly modular in the sense that they are internally linked or well-connected clusters located in the central core and correspond to the appearance of 'clumps' in the layout.

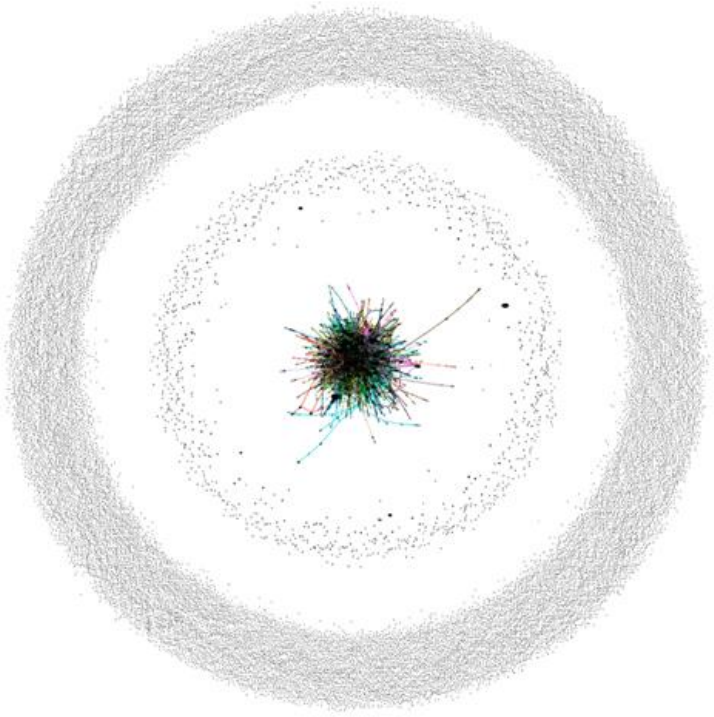

Figure 1. Network of interactions (full)

The majority of users we observed (isolated individuals) outside the core cluster were, therefore, 'shouting into the void': they were not part of any joined-up conversation, but their voices—as is further explored in the next section—were still relevant to our analysis. Through tweeting, they raised a number of themes that offered valuable insight into their feelings on the topic of interest.

Next, to understand the sociocultural and other key drivers at play, as identified in the UX and algorithm-aversion literature,[38] we sought to identify the conversation drivers (i.e., the type of social media actor setting the tone in the conversations observed). When focusing only on the connected core of the network (see Figure 2) in which most of the conversations occurred, we noticed that this was dominated by large clumps of nodes, with long threads emerging from the clumps. The clumps were centred around high-status public broadcasters (e.g., Sky and the BBC) and political institutions (e.g., Downing Street). Clumps formed when many individuals responded only to a single account (a network hub) but did not interact with others. The threads that emerged from these clumps were chains of commentators that responded to each other's contributions. Occasionally, the discussants took part in multiple chains and hence created the 'tangles' shown in Figure 2. This central interaction consisted mainly of individuals responding to journalists and prominent politicians, as well as to the official account for the NHS app (as detailed in Table 1 in the Appendix, which lists accounts with more than 150 replies [indegree > 150]), suggesting that much of the visible conversation was driven by tweets initiating responses from broadcasters and political accounts.

[38] Consider, for instance, Royal Statistic Society, Trust in Data; Dietvorst, "Algorithm Aversion"; Hartman, "Public Perceptions of Good Data Management"; Steedman, "Complex Ecologies."

Figure 2. At the core of the network

High-status Twitter accounts with many followers tended to generate more engagement in a conversation because a greater number of individuals saw their tweets. However, when considering the 25 highest-status organisations (with 1M+ followers) in our dataset (see Table 2 in the Appendix), we observed that many of them (e.g., the Economist) obtained almost no response to those of their tweets that were relevant to the scope of this study. Further, there was a notable absence of health organisations and professionals[39]: overall, it appeared that health organisations did not participate significantly in Twitter debates about the use of the NHS app.

Frames and Mechanisms of Resistance

Having clarified the structural aspects of our social network of interest and identified the conversation drivers, we then looked more in-depth and qualitatively at our dataset to unpack the key dynamics underlying people's resistance to using the NHS contact-tracing app.

Analytical Approach

To understand the prevailing themes underlying Twitter users' resistance to the use of the NHS tracing app, we first focused on their language and built a concept map. Frequency tables were created based on hashtags, keywords and n-grams (i.e., phrases of two or more words) present in the full dataset. Two researchers began by looking manually at hashtags, beginning with the most frequently used hashtags. Though only a minority of tweets (15%) used hashtags, we interpreted their use as a way of deliberately and explicitly entering the public discourse on our topic of interest on Twitter. The researchers then considered keywords and n-grams to expand and refine their conceptualisations until thematic saturation was reached (after approximately 800–1,000 words per table). Though overall frequency was a useful indicator of the 'value' of a keyword in our analysis, we decided to avoid setting a predefined frequency threshold, as less frequently used words could still be valuable for

[39] While no health organisations fall into the category of high-status organisations (the most-followed NHS account was Public Health England, with over 452,000 followers), we identified eight official NHS accounts in our dataset (NHSProviders, NHSCumbriaCCG, PublicHealth_NE, NTeesHpoolNHSFT, NHSX, NHSELRCCG, NHSDigital and LPFTNHS), together responsible for 14 tweets.

illuminating relevant themes. We used the concordance tool to analyse the context in which useful words emerged, as it allowed us to highlight the keyword in its original context[40] (see Figure 3).

/of Keep Our NHS Publi\nFresh concerns over	privacy	and profit in NHS COVID data deals
Some people have legitimate concerns over	privacy	and safety of the govt app.\n\nStarter: well./
/and trace app has huge question marks about	privacy	and security and doubtful functionality
app until I_m convinced that there are no	privacy	and security concerns /Track and Trace
/Director,_, shares some insights into the	privacy	and security dilemmas that a track and trace/
/with Huawei 5G than deeply invasive,	privacy	and security flawed gov't track and trace app
So what_s the latest with the data	privacy	and security implications of installing the/
/VoteLeave malware data-harvester app with	privacy	and security issues and dubious functionality/
/app for Covid\nNo thanks. I'm not making my	privacy	and security more vulnerable.\nI know I don't/
trace app/ If you are worried about	privacy	and security then don't download track and
/will boycott this crude attempt to invade our	privacy	and sell our data to unethical organisations.\n/
/'s track and trace app, questioning its	privacy	and suggesting potential alternatives
/app? Are you satisfied that it respects	privacy	and that the process for awarding the contract/
Great listening to talking about data	privacy	and the COVID-19 track and trace app
/or not it smacks of a gross invasion of	privacy	and the data collection element has Cummings_/
/allows tells you about the importance of	privacy	and the measures the app has put in place to/
/good articles from the last week about data,	privacy	and the NHS Track and Trace app, and all that/
/the Track and Trace app. I appreciate my	privacy	and there is plenty of information about me and/

Figure 3. Example of the keyword-in-context display for 'privacy'

This approach was used initially for the complete dataset and again for the frequency tables that were built separately for each part of the network, as described above (isolated individuals, disconnected small groups and connected core) to identify whether there were differences among these parts.

To conceptualise the data, notes were individually taken and then shared, discussed and integrated, drawing from insights from UX literature and algorithm-aversion studies, as well as their links to tech resistance, into the qualitative conceptual map shown in Figure 4. For the purpose of clarity, this map only the main connections identified, as well as highlighting the main themes and showing how they are connected.

[40] Ross, "Discursive Deflection."

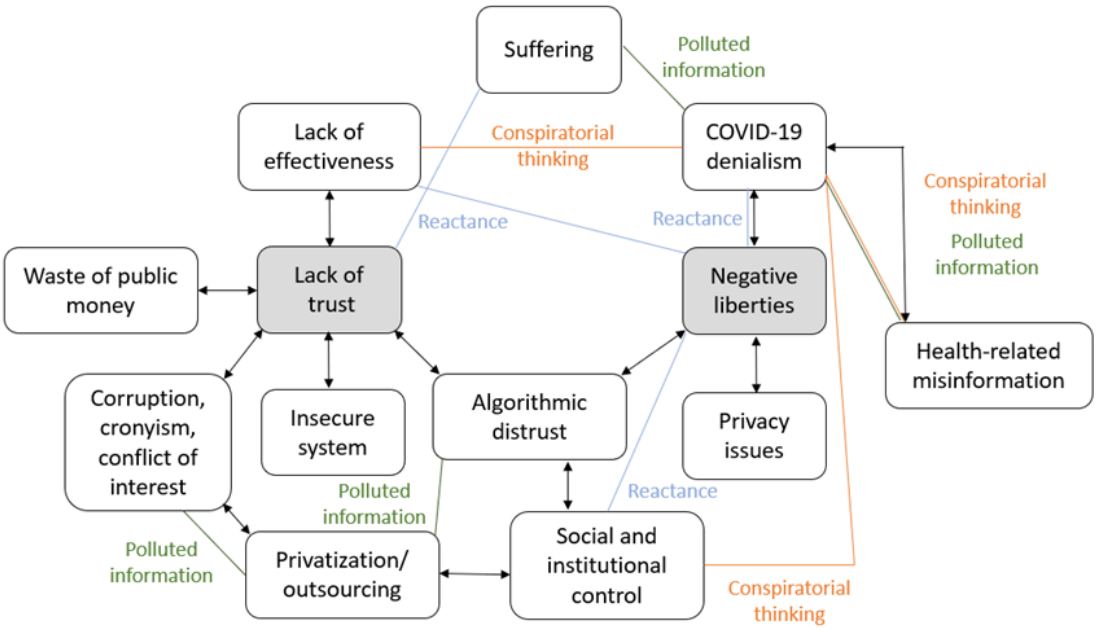

Figure 4. Conceptual map

Through this conceptual map, we identified two main narrative frames (lack of trust and negative liberties), reinforcing the findings of algorithm-aversion studies on public distrust or a 'data trust deficit' as being central to public resistance to data-driven technologies.[41] We also identified three main mechanisms (polluted information, conspiratorial thinking and reactance) underlying people's resistance to using the NHS contact-tracing app, which are discussed in the following subsections.

While all these frames and mechanisms were identified in all the parts of the networks, from the frequency tables that were separately built for each part of the network, certain differences emerged. For example, the isolated individuals were predominantly oppositional to the Conservative government and its members, indicating an entrenched lack of trust in the government and suggesting that, to understand UX, algorithm aversion and their links to tech resistance, consideration should be given to sociocultural contexts of new tech deployment (e.g., the level of trust in the authority encouraging adoption). Lack of trust can manifest in many different ways, and future research should further examine its relationship with different sociocultural features to better understand its nuances and ideate ad hoc interventions to restore public trust, which is fundamental in public health contexts.[42] We also noted the presence of unsubstantiated, imprecise or misleading claims on the more scientific aspects of the pandemic (e.g., herd immunity). Only in the disconnected small groups did the theme of 'suffering' (which included a broad range of sub-themes on a number of harms suffered, ranging from suicide and domestic violence to trauma and injustice) emerge as prevalent. As previously noted, UX research has shown that practical concerns about the capacity of technologies to generate or exacerbate stressful conditions for users should be considered during design and deployment to avoid resistance. In the connected core, discussions also appeared to pivot around issues of privacy and alleged/perceived corruption, reinforcing the findings of UX research on the importance of sociocultural contexts in tech design, as well as findings from algorithm-aversion research, which has cited privacy violations as a factor fuelling public resistance. The UX literature also suggests that users' beliefs and values can provoke resistance. The finding of the link between alleged and perceived corruption and resistance also reflected a lack of trust in the government and formed part of the sociocultural milieu from which resistance emerged. This reinforces previous findings from the algorithm-aversion scholarship on the inextricable link between lack of trust in government and resistance.[43]

[41] Royal Statistic Society, Trust in Data; Hartman, "Public Perceptions of Good Data Management."
[42] Consider, for instance, Gille, "Why Public Trust in Health Care Systems Matters"; Schwartz, "Evaluating and Deploying Covid-19 Vaccines."
[43] Devine, "Trust and the Coronavirus Pandemic."

Frames of Resistance

Though the themes identified in our manual analysis were varied and heterogeneous, we traced them back to two main narrative frames: lack of trust and negative liberties.

In the tweets examined, 'Trust' was declined in many different ways (e.g., *lack of trust* towards the Conservative government, towards a private company considered involved in the NHS app, towards the security and the effectiveness of the app and towards societal trends increasing datafication). The various declinations of trust were linked to diverse types of concerns (which are beyond the scope of this contribution) but that nonetheless appeared interrelated, as suggested by previously cited studies. Prior research has emphasised how various factors intersect to fuel public distrust and resistance. Future studies should further delineate the precise impact of each of these factors. Our study provides new insights into a range of factors and illuminates how the unique libertarian opportunities provided by Twitter and other social media platforms allow users of various sociocultural, socioeconomic and political backgrounds to broadcast their distrust and resistance to the new smart technologies of surveillance and governance—in this case, COVID-19 digital-tracing apps. The diverse but possibly intersecting narratives of distrust are "pushed through" via a large number of sites for engagement, hence being able to attract the interest of diverse populations of individuals.[44]

At the heart of individuals' lack of trust is the perceived incompetence of the actors involved, who are seen as flawed, corrupt, hypocritical and unaccountable for their actions or inaction. This mistrust is pivotal to understanding why, in some of the tweets observed, users appeared to be unencumbered by the social norm of protecting themselves, those at risk and, consequently, society at large and the economy, with their beliefs and behaviours becoming dependent on situational factors. This is in line with the 'drift' and 'digital drift' approaches in criminology, according to which the perceived lack of legitimacy or effectiveness of the criminal justice system can lead to delinquency, creating a 'sense of injustice' towards authorities; here, individuals feel they are freed from social norms, and their behaviours become dependent on transient opportunities and preferences.[45]

Further, tech scepticism—including algorithm distrust—appeared to play a key role. Techno-scepticism and public distrust of algorithms, which typically manifest as claims about the purpose and effectiveness of technological solutionism and automated processes, as well as the decisions algorithms make, have been fuelled in part by highly publicised cases highlighting the harms of certain data-driven algorithms (e.g., biases in areas such as criminal justice decision-making[46] and the distribution of healthcare resources[47]). Tech scepticism is also reinforced by the growing awareness of ethical issues, such as privacy violations, and the interrelated problems of poor explanability, transparency and accountability.[48] In the context of contact-tracing apps, concerns have been raised about the potential for widespread techno-surveillance, the outsourcing of expertise and sensitive (including health) data to tech giants and the consequent infringement of citizens' rights during times of emergency politics.[49]

The propagation of polluted information (as discussed below) adds yet another vital dimension to the growing problem of tech scepticism. Researchers who explored how social media has been used to improve or reduce trust in scientific expertise during the COVID-19 pandemic, for example, have highlighted the capacity of social media to be deployed as a mechanism of misinformation to undermine public trust in scientific expertise and accompanying systems, such as algorithms.[50] Such problems can trigger algorithm aversion which, as we have seen, refers to resistance to technologies designed to automate tasks and a preference for human judgement or intervention.[51]

In line with recent reports in the literature on the resistance to tracing apps, the value of privacy (broadly intended), and more generally, the importance of protecting personal data from unwanted surveillance or control from the government or big tech companies, appears to be an important concern. There is a desire to contrast perceived unwelcome incursions and attacks that hinder the right to privacy with dimensions of vertical (institutional) privacy being of greater concern in the tweets observed than dimensions of horizontal privacy (i.e., privacy between users of social media).[52] From this perspective, it is important to contextualise privacy issues, as well as other issues observed in the analysis, such as COVID-19 denialism and algorithmic distrust, in the broader frame of negative liberties (i.e., a specific type of individualistic freedom that manifests in the absence of constraints, as opposed to ideas of collective freedoms and liberties, focusing on the possibility of acting to realise one's

[44] For instance, Johnson, "The Online Competition"; Lavorgna, "To Wear or Not to Wear."
[45] See Matza, Delinquency and Drift; Holt, "Digital Drift"; Lavorgna, "Information Pollution as Social Harm."
[46] For instance, Angwin, "Bias in Criminal Risk Scores."
[47] For instance, Price, "Hospital 'Risk Scores'."
[48] Pasquale, The Black Box Society.
[49] Csernatoni, "New States of Emergency."
[50] Clayton, "Real Solutions for Fake News?"; Llewellyn, "COVID-19: How to be Careful with Trust."
[51] Dietvorst, "Overcoming Algorithm Aversion."
[52] In line with Lavorgna, Information Pollution as Social Harm.

fundamental purpose). This is in line with populist libertarian views and ideas of self-reliance (and, often, minimal government).[53] These systems of beliefs and worldviews have an important role in science denialism,[54] as scientific evidence is rejected when it is perceived as a threat to personal freedom, in line with the psychological mechanisms of reactance[55] discussed below; in the context of the pandemic, these systems have played a fundamental role in the opposition to preventive measures, such as lockdowns, limitations to travelling and gathering and the use of masks, which are seen as undue interferences into individual and group liberties.[56]

Mechanisms of Resistance

Besides the narrative frames that inform individuals' resistance to using the NHS contact-tracing app discussed above, from the conceptual map, we identified three main mechanisms of resistance (polluted information, conspiratorial thinking and reactance) to illuminate the factors that breed high levels of public distrust. These factors are primarily sociocultural in that they reflect the current social and cultural climate of app deployment. As the previously discussed UX studies suggest, these factors should be considered during design and subsequent deployment to enhance responsiveness and minimise resistance.

'Polluted information' is an umbrella term that encompasses misinformation (i.e., false information that is shared without the intent of harm), disinformation (i.e., false information that is knowingly shared to cause harm) and mal-information (i.e., genuine information that is shared to cause harm).[57] Polluted information began to be studied in cyberspace as a particularly devious variant of information warfare that can be propagated via countless platforms and cause great social harm by making individuals less knowledgeable, sharpening existing sociocultural divisions and fomenting scepticism towards legitimate news producers and accurate reporting.[58] In the context of public health, the phenomenon of polluted information has received criminological attention in recent times as an important enabler of the propagation and success of medical misinformation, causing major social harm.[59] This study revealed that polluted information has facilitated a wealth of misleading health-related information (e.g., enabling antimask and antivax views and questioning the importance of physical distancing) and—together with conspiratorial thinking—has also fostered COVID-19 denialism and foregrounded discourses that minimise the health risks of COVID-19 (meaning that fewer people download and use the app, as they do not believe there is a real or serious health problem). A strand of polluted information has also propagated false and misleading information on the role of public companies in the NHS app; notable in this sense are the tweets focusing on Serco linked to negative themes, such as corruption, conflict of interest and cronyism and a lack of trust. Serco is a private company contracted to provide a range of public services in the UK (including in the Test and Trace process, as it manages some facilities and call centres). However, the company played no role in the creation of the NHS Test and Trace app and is not processing its data.[60]

The term 'conspiratorial thinking' conjures images of a group of agents working together in secret, often for a sinister purpose.[61] In the present study, conspiratorial thinking was mostly observed as the driving force behind COVID-19 denialism and appeared to be behind the idea that the NHS Test and Trace app is part of a clandestine plan for mass control. Similar to what was recently observed in ethnographic studies grounded in criminology that looked at online communities during the pandemic,[62] while some concerns over the use of mechanisms of social and institutional control may be legitimate, conspiratorial thinking manifests in the fact that the existence of a clear direction is assumed, and science-fiction elements end up overshadowing realistic concerns about the potential for extreme dataveillance. It is not surprising to encounter conspiratorial thinking in the context of the pandemic: conspiracy theories are often adopted defensively, as they offer individuals a compensatory sense of control and help them feel a sense of power by rejecting official narratives,[63] particularly when there is a need to overcome feelings of alienation or anxiety in times of large-scale social change.[64] Importantly, conspiratorial thinking should not be dismissed as a weird or fringe belief, as such thinking can drive majorities to act in political, health, and social decision-making.[65]

[53] Boaz, The Politics of Freedom.
[54] See, for instance, Massa, "Don't Trust the Experts!"
[55] Prot, "Science Denial."
[56] Lavorgna, Information Pollution as Social Harm.
[57] Wardle, Information Disorder.
[58] Allcott, "Social Media and Fake News"; Lavorgna, Information Pollution as Social Harm.
[59] Lavorgna, Information Pollution as Social Harm.
[60] Krishna, "Serco Didn't Build."
[61] Coday, "An Introduction."
[62] Lavorgna, Information Pollution as Social Harm; Lavorgna, "Science Denial and Medical Misinformation."
[63] Douglas, "Motivations, Emotions and Belief."
[64] Bangerter, "How Conspiracy Theories Spread."
[65] Uscinski, Conspiracy Theories; Pierre, "Mistrust and Misinformation."

'Reactance' refers to how individuals tend to be averse to having their freedom or ability to act in a particular way restricted. When this happens, they tend to reject evidence that is perceived as a threat to their ability to act (or not act) in a certain way.[66] The NHS app is, in a way (and similarly to other preventive and mitigative measures imposed or suggested during the pandemic, such as physical distancing, the use of masks and lockdowns), seen as undue interference with individual liberties, with official recommendations, at times, being disregarded or opposed

Discussion and Conclusion

In our study, we combined criminological expertise and qualitative approaches with computational capacities to investigate people's resistance to using the NHS Test and Trace app. We identified three main parts of the network (isolated individuals, disconnected small groups and a connected core), with some differences in the type of accounts involved and themes discussed. The prevailing narrative frames (lack of trust and negative liberties) and mechanisms (polluted information, conspiratorial thinking and reactance) underlying people's resistance to using the app were also discussed. Our interdisciplinary research team adopted an exploratory and iterative process that aimed to make larger (and more complex) datasets better accessible for qualitative investigation and untangle our research puzzle in a more comprehensive way. The interaction between the computer scientist managing the data collection and quantitative aspects of network analyses with the subject-matter expertise and theoretical oversight provided by the social scientists enabled us to observe general trends and zoom in and analyse more in-depth subsets of relevant data.[67] We aimed to uncover insights based on the language contained in the tweets, the context of the authors of the tweets and the interactions between those authors who contributed to a national conversation (because the content of the tweets analysed was likely relevant to a broad segment of the population, as it related to a behaviour that the entire adult population of England and Wales was expected to engage in. While this discussion played out across other social platforms, not just Twitter alone, including in offline spaces, focusing on Twitter allowed us to examine aspects of these wider conversational engagements.

The conversations (and the lack thereof) that took place in our dataset suggested some avenues of further research and had practical implications. For example, our results invite the question of whether health organisations (that, as we have seen, rarely entered Twitter debates about the use of the NHS app) could be more active online to encourage better-informed discussions. Further, as most conversations centred around tweets by broadcasters and other significant accounts, could a more informative and less provocative use of tweets by traditional media outlets and journalists help avoid the online polarisation of health-sensitive topics? From a strictly criminological perspective, our findings reinforce insights from the UX literature, highlighting key dynamics that should be integrated into frameworks for understanding public resistance to new digital technologies, particularly surveillance systems, such as digital-tracing apps. One such mechanism is the recognition of the sociocultural context (i.e., the accepted beliefs, norms and practices that prevail among target users) in which the tech design and adoption takes place. Indeed, criminological studies exploring how frontline criminal justice practitioners deploy data-driven technologies, such as risk-prediction algorithms, have found that sociocultural resistance can discourage deployment and even trigger algorithm aversion. Such resistance can be provoked by perceived conflicts between the technologies and practice cultures, doubts about the social utility and technical efficiency of the technologies and lack of trust in their fairness.[68] Evidence also suggests that some police officers doubt the utility of predictive-policing algorithms and express concern and distrust about their fairness for socially marginal communities.[69] Interestingly, our study similarly uncovered sociocultural mechanisms of resistance, albeit in a different context of tech usage, and characterised by different intersecting factors, such as polluted information, conspiratorial thinking and ontological insecurity. This suggests that, even if their manifestations change across different contexts, the sociocultural dynamics prevailing at any one time and in any context should inform policy strategies that aim to address resistance to vital technologies, such as apps that can improve public health.

Unfortunately, the mechanisms of resistance we identified are difficult to counter and mitigate. Polluted information, for example, touches on the very delicate equilibria needed to promote and protect the right to freedom of opinion and expression; polluted information can be enjoyable (as it is more pleasant for consumers to read partisan news in line with their system of beliefs), cheap to obtain and difficult to identify.[70] Conspiratorial thinking finds a very fertile ground in situations in which people's need to feel safe and secure and exert control over their existence are threatened; conspiratorial thinking can, in such circumstances, be highly successful, as it helps promote individuals' feelings of agency and power.[71] The phenomenology of

[66] Rosenberg, "A 50-year Review of Psychological Reactance Theory"; Prot, "Science Denial."
[67] In line with, among others: Tinati, "Mixing Methods and Theory to Explore Web Activity"; Tinati, "Big Data: Methodological"; Tinati, "Challenging Social Media Analytics"; Halford, "Understanding the Production and Circulation of Social Media Data."
[68] For instance, Lavorgna, "The Datafication Revolution."
[69] Babuta, Data Analytics and Algorithmic Bias.
[70] Allcott, "Social Media and Fake News."
[71] Imhoff, "Conspiracy Beliefs as Psycho-Political Reactions."

reactance, similar to other psychological mechanisms at the basis of science denialism,[72] reminds us why simply bombarding denialists with accurate scientific information does not lead to a change in attitudes. So far, interventions targeting these mechanisms have not been conducted in a coordinated way.[73] As recently discussed in the context of harmful polluted information online,[74] profound architectural changes have not occurred, and interventions from online intermediaries that targeting the source are proving relatively ineffective and have the potential to create serious tensions against individual rights. Further, debunking activities have often proved ineffective and potentially even counterproductive, increasing polarisation and facilitating displacement towards more protected social media. As is the case with other online harms, there is no single best strategy, and a sustained and multilayered effort between a wide range of institutions, individual actors and technology is, therefore, needed to meet a fundamental social challenge that goes well beyond convincing individuals to use an app; rather, this challenge has to do with improving public scientific literacy and critical thinking and restoring public trust. Such trust, however, must be earned, and this involves improving effectiveness and (institutional, political and algorithmic) transparency.

[72] Prot, "Science Denial."
[73] Kreko, "Countering Conspiracy Theories"; Larson, "Blocking Information."
[74] Lavorgna, Information Pollution as Social Harm.

Bibliography

Abeler, Johannes, Sam Altmann, Luke Milsom, Severine Toussaert and Hannah Zillessen. *Support in the UK for App-based Contact Tracing of COVID-19*. (Department of Economics, University of Oxford, 2020).

Ada Lovelace Institute. *Exit Through the App Store?* (2020). https://www.adalovelaceinstitute.org/wp-content/uploads/2020/04/Ada-Lovelace-Institute-RapidEvidence-Review-Exit-through-the-App-Store-April-2020-2.pdf

Angwin, Julia and Jeff Larson. "Bias in Criminal Risk Scores is Mathematically Inevitable, Researchers Say." December 30, 2016. https://www.propublica.org/article/bias-in-criminal-risk-scores-is-mathematically-inevitable-researchers-say

Allcott, Hunt and Matthew Gentzkow. "Social Media and Fake News in the 2016 Elections." *Journal of Economic Perspectives* 31, no 2 (2017): 211–236.

Ahmed, Nadeem, Regio A. Michelin, Wanli Xue, Sushmita Ruj, Robert Malaney, Salil S. Kanhere, Aruna Seneviratne, Wen Hui, Helge Janicke and Sanjay K. Jha. "A Survey of COVID-19 Contact Tracing Apps." *IEEE Access* 8 (2020): 134577–134601. https://doi.org/10.1109/ACCESS.2020.3010226

Anuradha, Nagaraj. "'Black Holes': India's Coronavirus Apps Raise Privacy Fears." August 26, 2020. https://www.reuters.com/article/us-health-coronavirus-india-tech-feature/black-holes-indias-coronavirus-apps-raise-privacy-fears-idUSKBN25M1KE

Babuta, Alexander and Marion Oswald. *Data Analytics and Algorithmic Bias in Policing*. (Royal United Services Institute Briefing Paper, 2019). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/831750/RUSI_Report_-_Algorithms_and_Bias_in_Policing.pdf

Bangerter, Adrian, Pascal Wagner-Egger and Sylvain Delouvee. "How Conspiracy Theories Spread." In *Routledge Handbook of Conspiracy Theories*, edited by Michael Butter and Peter Knight. London, UK: Routledge, 2020, pp. 206-219.

BBC News. "NHS Data Breach Involving 284 Patients Uncovered." November 26, 2020. https://www.bbc.co.uk/news/uk-scotland-highlands-islands-55085485

Berger, Benedikt, Martin Adam, Alexander Rühr, A. and Alexander Benlian. "Watch Me Improve—Algorithm Aversion and Demonstrating the Ability to Learn." *Business & Information Systems Engineering* 63, no 1 (2020): 55–68. https://doi.org/10.1007/s12599-020-00678-5

Boaz, David. *The Politics of Freedom: Taking on The Left, The Right and Threats to Our Liberties*. Washington, DC: Cato Institute, 2008.

Clayton, Katherine, Spencer Blair, Jonathan A. Busam, Samuel Forstner, John Glance, Guy Green, Anna Kawata, Akhila Kovvuri, Jonathan Martin, Evan Morgan, Morgan Sandhu, Rachel Sang, Rachel Scholz-Bright, Austin T. Welch, Andrew G. Wolff, Amanda Zhou and Brendan Nyhan. "Real Solutions for Fake News? Measuring the Effectiveness of General Warnings and Fact-check Tags in Reducing Belief in False Stories on Social Media." *Political Behavior* 42 (2019): 1073–1095. https://doi.org/10.1007/s11109-019-09533-0

Coday, David. "An Introduction to the Philosophical Debate about Conspiracy Theories." In *Conspiracy Theories. The Philosophical Debate*, edited by David Coday. London: Routledge, 2016, pp. 1-13.

Csernatoni¸ Raluca. "New States of Emergency: Normalizing Techno-surveillance in the time of COVID-19." *Global Affairs* 6, no 3 (2020): 301–310. https://doi.org/10.1080/23340460.2020.1825108

Dencik, Lina, Arne Hintz, Joanna Redden and Treré Emiliano. "Exploring Data Justice: Conceptions, Applications and Directions." *Information, Communication & Society* 22, no 7 (2019): 873–881. https://doi.org/10.1080/1369118X.2019.1606268

Devine, Daniel, Jennifer Gaskell, Will Jennings and Gerry Stoker. "Trust and the Coronavirus Pandemic: What are the Consequences of and for Trust? An Early Review of the Literature." *Political Studies Review* 19, no 2 (2020): 274–285. https://doi.org/10.1177/1478929920948684

Dietvorst, Berkeley, Joseph P. Simmons and Cade Massey. "Overcoming Algorithm Aversion: People will Use Imperfect Algorithms if They can (Even Slightly) Modify Them." *Management Science* 64, no 3 (2015): 983–1476. https://doi.org/10.1287/mnsc.2016.2643

Dietvorst, Berkeley. "Algorithm Aversion." PhD, University of Pennsylvania, 2016. https://repository.upenn.edu/edissertations/1686.

Dietvorst, Berkeley, Joseph P. Simmons and Cade Massey. "Algorithm Aversion: People Erroneously Avoid Algorithms after Seeing Them Err." *Journal of Experimental Psychology: General* 144, no 1 (2016): 114–126. https://psycnet.apa.org/doi/10.1037/xge0000033

Douglas, Karen M., Aleksandra Cichocka and Robbie M. Sutton. "Motivations, Emotions and Belief in Conspiracy Theories." In *Routledge Handbook of Conspiracy Theories*, edited by Michael Butter and Peter Knight. London: Routledge, 2020, pp. 181-192.

Farronato, Chiara, Marco Iansiti, Marcin Bartosiak, Stefano Denicolai, Luca Ferretti and Roberto Fontana. "How to Get People to Actually Use Contact-tracing Apps." *Harvard Business Review*, July 15, 2020.

Farries, Elizabeth. "Covid-tracing App may be Ineffective and Invasive of Privacy, Government Must be Transparent to Avoid Unintended Consequences." *The Irish Times*, May 5, 2020. https://www.irishtimes.com/opinion/covid-tracing-app-may-be-ineffective-and-invasive-of-privacy-1.4244638

Ferreira, Alberto. *Universal UX Design: Building Multicultural User Experience*. Massachusetts: Morgan Kaufmann, 2016.

Ferrell, Jeff. "In Defense of Resistance." *Critical Criminology* (2019). https://doi.org/10.1007/s10612-019-09456-6

Ferretti, Luca, Chris Wymant, Michelle Kendall, Lele Zhao, Anel Nurtay, Lucie Abeler-Dörner, Michael Parker, David Bonsall and Christophe Fraser. "Quantifying SARS-CoV-2 Transmission Suggests Epidemic Control with Digital Contact Tracing." *Science* 368, no 6491 (2020). https://doi.org/10.1126/science.abb6936

Fitriani. "COVID-19 Apps: Fear of Tyranny by Data." *The Jakarta Post*, June 22, 2020. https://www.thejakartapost.com/academia/2020/06/22/covid-19-apps-fear-of-tyranny-by-data.html

Fussey, Pete, Davies, Bethan and Innes Martin. "'Assisted' Facial Recognition and the Reinvention of Suspicion and Discretion in Digital Policing." *The British Journal of Criminology* 61, no 2 (2021): 325–344. https://doi.org/10.1093/bjc/azaa068

Garrett, Paul, Joshua White, Daniel Little, Amy Perfors, Yoshihisa Kashima, Stephan Lewandowsky and Simon Dennis. "A Representative Sample of Australian Participant's Attitudes Towards the COVIDSafe App." Complex Human Data Hub, School of Psychological Sciences, The University of Melbourne, Australia, 2020.

Gille, Feliz, Sarah Smith and Nicholas Mays. "Why Public Trust in Health Care Systems Matters and Deserves Greater Research Attention." *Journal of Health Services Research & Policy* 20, no 1 (2015): 62–64. https://doi.org/10.1177/1355819614543161

Halford, Susan, Mark Weal, Ramine Tinati, Leslie Carr and Catherine Pope. "Understanding the Production and Circulation of Social Media Data: Towards Methodological Principles and Praxis." *New Media & Society* 20, no 9 (2018): 3341–3358. https://doi.org/10.1177%2F1461444817748953

Hartman, Todd, Helen Kennedy, Robin Steedman and Rhianne Jones. "Public Perceptions of Good Data Management: Findings from a UK-based Survey." *Big Data & Society* 7, no 1. https://doi.org/10.1177/2053951720935616

Hinderks, Andreas, Martin Schrepp, Francisco J. D. Mayo, Maria J. Escalona and Jorg Thomaschewski. "Developing a UX KPI Based on the User Experience Questionnaire." *Computer Standards & Interfaces* 65 (2019): 38–44.

Holt, Tom J., Russell Brewer and Andrew Goldsmith. "Digital Drift and the 'Sense of Injustice': Counter-Productive Policing of Youth Cybercrime." *Deviant Behavior* 40, no 9 (2019): 1144–1156. https://doi.org/10.1080/01639625.2018.1472927

Imhoff, Roland and Pia Lamberty. "Conspiracy Beliefs as Psycho-Political Reactions to Perceived Power." In *Routledge Handbook of Conspiracy Theories*, edited by Michael Butter and Peter Knight. Routledge, London, 2020, pp. 192-206.

Johnson, Neil F., Nicolas Velásquez, Nicholas J. Restrepo, Rhys Leahy, Nicholas Gabriel, Sara El Oud, Minzhang Zheng, Pedro Manrique, Stefan Wuchty and Yonatan Lupu. "The Online Competition between Pro- and Anti-vaccination Views." *Nature* 582 (2020): 230–233. https://doi.org/10.1038/s41586-020-2281-1

Krekó, Péter. "Countering Conspiracy Theories and Misinformation." In *Routledge Handbook of Conspiracy Theories*, edited by Michael Butter and Peter Knight. Routledge, London, 2020, pp. 242-256.

Krishna, Rachael. "Serco Didn't Build and Does Not Run the NHS Test and Trace App." Full Fact, September 30, 2020. https://fullfact.org/health/Serco-test-and-trace/

Larson, Heidi J. "Blocking Information on COVID-19 can Fuel the Spread of Misinformation." *Nature* 580 (2020): 306. https://doi.org/10.1038/d41586-020-00920-w

Lavorgna, Anita. *Information Pollution as Social Harm: Investigating the Digital Drift of Medical Misinformation in a Time of Crisis*. Emerald Publishing, 2021.

Lavorgna, Anita, Les Carr and Ashton Kingdon. "To Wear or Not to Wear? Unpacking the #NoMask Discourses and Conversations on Twitter" (under review).

Lavorgna, Anita and Heather Myles. "Science Denial and Medical Misinformation in Pandemic Times: A Micro-level Analysis of 'Alternative Lifestyle' Subcultural Groups." *European Journal of Criminology* (2021). https://doi.org/10.1177%2F1477370820988832

Lavorgna, Anita and Pamela Ugwudike. "The Datafication Revolution in Criminal Justice: An Empirical Exploration of Frames Portraying Data-driven Technologies for Crime Prevention and Control." *Big Data & Society* (2021, in press). https://eprints.soton.ac.uk/451344/

Lavorgna, Anita, Pamela Ugwudike, Yadira Sanchez Benitez and Les Carr. *Understanding Public Resistance in Using COVID-19 Digital Contact Tracing App: A Sociotechnical Analysis*. (Project report, University of Southampton, 2021).

Lia, Tianshi, Camille Cobba, Jackie J. Yangb, Sagar Baviskara, Yuvraj Agarwala, Beibei Lia, Lujo Bauera and Jason I. Honga. "What Makes People Install a COVID-19 Contact-Tracing App? Understanding the Influence of App Design and Individual Difference on Contact-tracing App Adoption Intention." 2020. https://arxiv.org/abs/2012.12415v3

Llewellyn, Sue. "COVID-19: How to be Careful with Trust and Expertise on Social Media." *British Medical Journal* 368 (2020). https://doi.org/10.1136/bmj.m1160

Massa, Ester. "'Don't Trust the Experts!': Analysing the Use of Populist Rhetoric in the Anti-vaxxers Discourse in Italy." In *Medical Misinformation and Social Harm in Non-Science-Based Health Practices: A Multidisciplinary Perspective*, edited by Anita Lavorgna and Anna D. Ronco, pp. 69-85. London: Routledge, 2019.

Matza, David. *Delinquency and Drift*. New York: Wiley, 1964.

Mbunge, Elliot. "Integrating Emerging Technologies into COVID-19 Contact Tracing: Opportunities, Challenges and Pitfalls." *Diabetes & Metabolic Syndrome: Clinical Research & Reviews* 14, no 6 (2020): 1631–1663. https://doi.org/10.1016/j.dsx.2020.08.029

Megnin-Viggars, Odette, Patrice Carter, G.J. Melendez-Torres, Dale Weston and Rubin G. James. "Facilitators and Barriers to Engagement with Contact Tracing during Infectious Disease Outbreaks: A Rapid Review of the Evidence." *PLoS ONE* 15, no 10 (2020). https://doi.org/10.1371/journal.pone.0241473

Nature. "COVID-19 Digital Apps Need Due Diligence." *The International Journal of Science* 5830, 563, no 30 (2020). https://media.nature.com/original/magazine-assets/d41586-020-01264-1/d41586-020-01264-1.pdf

Nellis, Mike. "Surveillance-Based Compliance using Electronic Monitoring." In *What Works in Offender Compliance*, edited by Pamela Ugwudike and Peter Raynor. London: Palgrave MacMillan, 2013.

Nellis, Mike. *Standards and Ethics in Electronic Monitoring. Handbook for Professionals Responsible for the Establishment and the Use of Electronic Monitoring*. Council of Europe, 2015. https://rm.coe.int/handbook-standards-ethics-in-electronic-monitoring-eng/16806ab9b0

O'Callaghan, Michael E., Jim Buckley, Brian Fitzgerald, Kevin Johnson, John Laffey, Bairbre McNicholas, Bashar Nuseibeh, Derek O'Keeffe, Ian O'Keeffe, Abdul Razzaq, Kaavya Rekanar, Ita Richardson, Andrew Simpkin, Jaynal Abedin, Cristiano Storni, Damyanka Tsvyatkova, Jane Walsh, Thomas Welsh and Liam Glynn. "A National Survey of Attitudes to COVID-19 Digital Contact Tracing in the Republic of Ireland." *Irish Journal of Medical Science* 190 (2021): 863–887. https://doi.org/10.1007/s11845-020-02389-y

Panda Security. "'Apathy in the UK': 80% of Brits Refuse to Download Covid Tracking Apps." July 15, 2020. https://www.pandasecurity.com/en/mediacenter/mobile-news/appathy-in-the-uk/.

Pasquale, Frank. *The Black Box Society: The Secret Algorithms That Control Money and Information.* Cambridge: Harvard University Press, 2016.

Pierre, Joseph M. "Mistrust and Misinformation: A Two-component, Socio-epistemic Model of Belief in Conspiracy Theories." *Journal of Social and Political Psychology* 8, no 2 (2020): 617–641.

Price, Michael. "Hospital 'Risk Scores' Prioritize White Patients." *Science*, October 24, 2019. https://www.sciencemag.org/news/2019/10/hospital-risk-scores-prioritize-white-patients

Prot, Sara and Craig A. Anderson. "Science Denial. Psychological Processes Underlying Denial of Science-based Medical Practices." In *Medical Misinformation and Social Harm in Non-Science-Based Health Practices: A Multidisciplinary Perspective*, edited by Anita Lavorgna and Anna D. Ronco. Routledge: London, 2019, pp. 24-38.

Rosenberg, Benjamin D. and Jason T. Siegel. "A 50-year Review of Psychological Reactance Theory: Do Not Read this Article." *Motivation Science* 4, no 4 (2018): 281–300. http://dx.doi.org/10.1037/mot0000091

Ross, Andrew S. and Damian J. Rivers. "Discursive Deflection: Accusation of 'Fake News' and the Spread of Mis- and Disinformation in the Tweets of President Trump." *Social Media + Society* 4, no 2 (2018). https://doi.org/10.1177/2056305118776010

Rowe, Frantz. "Contact Tracing Apps and Values Dilemmas: A Privacy Paradox in a Neo-liberal World." *International Journal of Information Management* 55 (2020). https://dx.doi.org/10.1016%2Fj.ijinfomgt.2020.102178

Royal Statistical Society. *Trust in Data and Attitudes Toward Data Use/Data Sharing*. 2014. https://doi.org/10.1016/j.ijinfomgt.2020.102178.

Schwartz, Jason L. "Evaluating and Deploying Covid-19 Vaccine. The Importance of Transparency, Scientific Integrity, and Public Trust." *The New England Journal of Medicine* 383 (2020): 1703–1705. https://doi.org/10.1056/NEJMp2026393

Shin, Donghee. "User Perceptions of Algorithmic Decisions in the Personalized AI System: Perceptual Evaluation of Fairness, Accountability, Transparency, and Explainability." *Journal of Broadcasting & Electronic Media* 64, no 4 (2020): 541–565. https://doi.org/10.1080/08838151.2020.1843357

Shin, Donghee, Bu Zhong and Frank A. Biocca. "Beyond User Experience: What Constitutes Algorithmic Experiences?" *International Journal of Information Management* 52 (2020). https://doi.org/10.1016/j.ijinfomgt.2019.102061

Simko, Lucy, Ryan Calo, Franziska Roesner and Tadayoshi Kohno. "COVID-19 Contact Tracing and Privacy: Studying Opinion and Preferences." 2020. https://arxiv.org/abs/2012.01553

Smith, Gavin D.J. and Pat O'Malley. "Driving Politics: Data-driven Governance and Resistance." *The British Journal of Criminology* 57, no 2 (2017): 275–298. https://doi.org/10.1093/bjc/azw075

Steedman, Robin, Helen Kennedy and Jones Rhianne. "Complex Ecologies of Trust in Data Practices and Data-driven Systems." *Information, Communication & Society* 23, no 6 (2020): 817–832. https://doi.org/10.1080/1369118X.2020.1748090

Sweeney, Yann. "Tracking the Debate on COVID-19 Surveillance Tools." *Nature Machine Intelligence* 2 (2020): 301–304. https://doi.org/10.1038/s42256-020-0194-1

Tinati, Ramine, Susan Halford, Leslie Carr and Catherine Pope. "Mixing Methods and Theory to Explore Web Activity." *Proceedings of the 2012 ACM Conference on Web Science* (2012): 308–316. https://doi.org/10.1145/2380718.2380758

Tinati, Ramine, Susan Halford, Leslie Carr and Catherine Pope. "Big Data: Methodological Challenges and Approaches for Sociological Analysis." *Sociology 48*, no 4 (2014): 663–681. https://doi.org/10.1177%2F0038038513511561

Tinati, Ramine, Oliver Philippe, Catherine Pope, Leslie Carr and Susan Halford. "Challenging Social Media Analytics: Web Science Perspectives." *Proceedings of the 2014 ACM Conference on Web Science* (2014): 177–181. https://doi.org/10.1145/2615569.2615690

Tromp, Nynke, Paul Hekkert and Peter P.C.C. Verbeek. "Design for Socially Responsible Behaviour: A Classification of Influence Based on Intended User Experience." *Design Issues* 27 (2011): 3–19.

UK Government. *Centre for Data Ethics and Innovation Independent Report: Review into Bias in Algorithmic Decision-Making*. (UK Government, 2020). https://www.gov.uk/government/publications/cdei-publishes-review-into-bias-in-algorithmic-decision-making/main-report-cdei-review-into-bias-in-algorithmic-decision-making

Uscinski, Joseph E. *Conspiracy Theories and the People Who Believe Them.* Oxford: Oxford University Press, 2018.

von Wyl Viktor, Sebastian Bonhoeffer, Edouard Bugnion, Alan M. Puhan, Marcel Salathé, Theresa Stadler, Carmela Troncoso, Effy Vayena and Nicola Low. "A Research Agenda for Digital Proximity Tracing Apps." *Swiss Medical Weekly* 150 (2020): 29–30. http://doi.org/10.4414/smw.2020.20324

Walrave, Michel, Cato Waeterloos and Koen Ponnet. "Adoption of a Contact Tracing App for Containing COVID-19: A Health Belief Model Approach." *JMIR Public Health Surveill* 6, no 3 (2020). https://doi.org/10.2196/20572

Wardle, Claire and Hossein Derakhshan. *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*. Strasbourg: Council of Europe, 2017.

Weaver, Matthew. "Don't Coerce Public Over Contact-tracing App, Say Campaigners." *The Guardian*, April 26, 2020. https://www.theguardian.com/law/2020/apr/26/dont-coerce-public-over-coronavirus-contract-tracing-app-say-campaigners

Woo, Jie. "Policy Capacity and Singapore's Response to the COVID-19 Pandemic." *Policy and Society* 39, no 3 (2020): 345–362. https://doi.org/10.1080/14494035.2020.1783789

Appendix

Table 1. Indegree > 150

Id	indegree	Description
SkyNews	577	We take you to the heart of the stories that shape our world. For breaking news, follow @SkyNewsBreak
BBCNews	527	News, features and analysis. For world news, follow @BBCWorld. Breaking news, follow @BBCBreaking. Latest sport news @BBCSport. Our Instagram: BBCNews
NHSCOVID19app	357	Official account for the latest #NHSCOVID19app news. Download now in England and Wales. We are here to help Mon-Fri 9am-6pm & Sat-Sun 9am-5pm.
LBC	306	Leading Britain's Conversation. For the latest news alerts, follow @LBCNews. Follow us on Instagram https://t.co/nAl9t58RmX
10DowningStreet	304	Official page for Prime Minister @BorisJohnson's office, based at 10 Downing Street
GMB	203	The UK's most talked about breakfast television show. Weekdays from 6am on @ITV. Replies & content may be used on air. See https://t.co/u4BYxXFfJq
KayBurley	177	More live TV than anyone else. Sky News founder member. Animal lover. Mountain climber. Impossibly proud mum. Enquiries: Wolfie@WolfieKutner.com
lewis_goodall	163	Policy Editor @BBCNewsnight. I cover politics, policy, economics and government in the UK and beyond | Author: Left for Dead. Buy here- https://t.co/5P5LrZxTl9
BethRigby	160	Political Editor, Sky News
BBCBreakfast	153	The UK's favourite morning news programme. Wake up with the most watched Breakfast show every day from 6am on BBC One ⏰☕

Table 2: High-status organisations

Organisation	Description
The Economist	News and analysis with a global perspective.
Reuters	Top and breaking news, pictures and videos from Reuters.
BBC News (UK)	News, features and analysis.
The Guardian	The need for independent journalism has never been greater.
Bloomberg	The first word in business news.
Sky News	We take you to the heart of the stories that shape our world.
The Hindu	News feeds from India's National Newspaper
10 Downing Street	UK Prime Minister Official page for Prime Minister @BorisJohnson's office, based at 10 Downing St
New Scientist	The best place to find out what's new in science—and why it matters.
The Independent	News, comment and features from The Independent.
The Telegraph	Think ahead with the latest news, comment, analysis and video.
Daily Mail Online	For the latest updates on breaking news visit our website
eNCA	eNCA is a 24-hour news channel focusing on news from across SA and Africa.
LADbible	Redefining entertainment & news! Follow now for the best viral videos, funny stories & latest news
ITV News	Breaking news and the biggest stories from the UK and around the world.
Republic	Official handle of the Republic Media Network. DIGITAL. TV. MEDIA
Reuters Business	Top business news around the world. Join us @Reuters, @breakingviews, @ReutersGMF
This Morning	Join us weekdays from 10am on ITV, STV and the ITV Hub! 🕙
The Sun	Never miss a story again. News, sport and entertainment, as it happens
TNW	The heart of tech
The Times	The best of our journalism
Bloomberg Quicktake	Live global news and original shows. Streaming free, 24/7.
Daily Mirror	The official Daily Mirror & Mirror Online Twitter account 📎 - real news in real time.
CNN Philippines	News you can trust • Free TV channel 9
The National	The official Twitter feed of The National, the UAE and Middle East's premier news source