Lavorgna A, Carr L, Ugwudike P, Sanchez Benitez Y e Rekha SG (2021) To app or not to app? Understanding public resistance in using COVID-19 digital contact tracing. *Law, Technology & Humans* – confidential (in press)

To app or not to app? Understanding public resistance in using COVID-19 digital contact tracing and its criminological relevance

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 been facing public resistance, making their use relatively sparse and ineffective. Our study, which relies on an interdisciplinary approach bringing together criminological and computational expertise, unpacks this issue by looking at key social dynamics at the basis of people resistance in using the NHS contact tracing app in England and Wales. It analyses a large Twitter dataset to investigate interactions between relevant user accounts, and to identify the main narrative frames (lack of trust; negative liberties) and mechanisms (polluted information; conspiratorial thinking; reactance) explaining and enabling people's resistance in using the NHS contact tracing app. Our study builds on concepts of User eXperience (UX) and algorithm aversion and demonstrates their relevance to a key criminological problem which is resistance to official technologies.

Keywords

COVID-19; tracing app; algorithm aversion; user experience; public compliance; data-driven surveillance

Introduction

In the context of the COVID-19 pandemic, contact tracing apps have been developed and released in several countries, including the United Kingdom, as an additional measure to combat COVID-19, speeding up the tracing of contacts of people found to be infected[1]. At the core of this approach is the fact that, although the new coronavirus spreads too fast to be contained by manual contact tracing, it could be controlled through the use of automatised contact-tracing (via an app), if used by enough people, which would help contain the pandemic[2]. These apps are generally based on practical hardware technologies (e.g., Bluetooth low energy, possibly GPS data), so basically anyone with a smartphone can use and implement their use. In practice, however, these type of apps lack sufficient real-life testing, which is problematic as their effectiveness, regardless of the technology used, depends as much as on socio-behavioural factors, such as public confidence and trust in the protection of privacy[3].

As lamented in a recent editorial in *Nature* (2020), despite the global nature of the pandemic, there are at the moment no global standards for the development of COVID-19 tracing apps, which raises a series of concerns, particularly accuracy concerns (if incorrect information is sent, this could create severe harms) and privacy concerns (if individuals can be identified from the aggregated datasets)[4]. Hence, it may not be surprising that these apps – especially in privacy-conscious countries – have been facing strong public resistance, with the consequence that their sparse use has made them relatively ineffective.

Our study, which relies on an interdisciplinary approach bringing together criminological and computational expertise, aims to unpack this issue from a novel standpoint – that is, by investigating a large Twitter dataset to unravel the social dynamics underpinning people's resistance to the NHS contact tracing app across England and Wales. As such, it focuses on the

[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 also Farronato, "How to get people to actually use contact-tracing apps"; Rowe, "Contact tracing apps and value dilemmas".

broader issue of resistance to governance strategies which, in most cases, may/should not be explicitly defined as ‘criminal’ or ‘deviant’ acts, but has nevertheless attracted the attention of criminology, with cultural criminologists for example exploring public resistance to forms of power and authority perceived as harmful and unjust[5]. Our study focuses on a specific form of resistance which is public resistance to the perceived harms of governance technologies (i.e., data-driven tools for surveillance and control). This is a crucial area of study which has attracted limited criminological attention but has become increasingly topical. Our study brings criminology to the forefront of this fast-growing area by creating 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 techs are deployed. Both concepts are relevant to the current study which seeks to enhance criminological understandings of the factors underpinning resistance to official techs such as digital tracing apps and identify remedial strategies. The rapid proliferation of such automated decision-making techs across several western and non-western jurisdictions renders this enquiry essential.

Theoretical framework

Data-driven technologies are increasingly automating key policy decisions in public and private sectors and studies suggest that pubic “buy in” or acceptance of the techs is crucial for adoption. This is particularly the case with techs which, unlike coercive systems such as electronic surveillance devices deployed in justice systems, rely on voluntary adoption. Examples include the plethora of surveillance techs that have emerged with the advent of recent technological advances. This paper focuses on the COVID-19 “track and trace” app which was introduced across England and Wales in 2020 to surveil people who test positive and contain the pandemic. Studies,

[5] Ferrell, “In Defence of Resistance”; Smith, “Driving Politics”.

however, point to growing public resistance to such apps[6]. Yet, there is limited criminological insight into the mechanisms underpinning this resistance.

Contact tracing apps are, in a broad sense, surveillance technologies which seek to govern and control human conduct. Of course, we recognise that they are very different in nature and scope from those used traditionally in criminal justice settings, for example, 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 have a defined purpose of promoting public health outcomes. Also, we recognise that contact tracing apps occupy a very different space in public discussions about surveillance, or at least have so far received less media and scholarly attention on this aspect. However, although the technologies we are focusing on in this contribution are substantively different, it is important to recognise that there is a common denominator that connects all the currently proliferating "smart technologies" – *i.e.*, they are all data-driven and give rise to similar concerns such as data injustice, privacy violations, opacity, and other harms that erode public trust[9].

Existing criminological studies of surveillance techs 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 techs is of great relevance to the discipline, 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 the dearth of criminological insights, the study draws on sections of the AI design literature that explore UX of data-driven technologies. Originating initially in industry settings and used by organisations seeking to embed user feedback in tech design, UX studies generate information required for developing responsive user-friendly systems. The studies map people's

[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".

perceptual and behavioural responses to an anticipated or already deployed system[11]. Whilst UX is dynamic and evolves in tandem with technological advances, a clear and broad theme that emerges from UX studies is the fact 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, including users' entrenched beliefs and interests[12]. Tech design should also factor in the extent to which the system could impact on daily routines or even generate or exacerbate stressful conditions for potential users[13]. Related factors such as public trust in the techs[14] and the authority encouraging adoption, in this case the government, are also relevant, not least because as Devine and colleagues observe, "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 which refers to the general reluctance of target users to adopt techs designed to fully or partly automate tasks, preferring human judgement instead, particularly after observed or reported failures of the techs[16]. A study by Dietvorst and colleagues, however, found that uptake can be improved if users are able to modify what they consider to be flawed algorithms, highlighting the importance of user input in tech design[17]. These insights from studies of UX and algorithm aversion draw attention to the importance of exploring user's discourses about their experiences of new tech, to uncover mechanisms of resistance. Our study explores these issues, with a focus on the digital tracing app introduced in England and Wales in 2020.

Tracing apps, public concerns and compliance

[11] Hinderks, "Developing a UX KPI".
[12] Ferreira, "Universal UX Design".
[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".

In the unfolding of the COVID-19 pandemic, contact tracing apps have, as already noted, been developed or released in several countries, and their use has entered public debates. It appears, however, that there has been a degree of public resistance to the apps and, in response, a number of academic studies and media commentaries across the globe (exemplified below, and generally based on national surveys or expert interviews) have tried to understand the factors underpinning resistance to the apps where available[18]. While the results of these contributions might be difficult to generalize in such an evolving situation (where people's opinions might easily change depending on the evolution of the pandemic and the health, social and economic crises it provoked) and across countries (as many factors behind people's resistance might be situational and culture specific), they nonetheless offer important insights into individual choices on this issue, allowing us to start identifying common patterns. From this literature, in line with Farronato and colleagues[19], privacy concerns seem to be the main barrier to tracing apps adoption. Privacy, as appears in those studies, seem to be broadly intended, and mainly associated with an ideological commitment to avoid interference from the government or big tech companies; in any case, this concept is not discussed in detail. This could be symptomatic of the sociocultural contexts of use to which UX studies allude, in this case, users' beliefs about the extent to which the authority encouraging use can be trusted to embed privacy protections in the system. It 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 tool in tracing the spread of the virus. Nevertheless, privacy concerns among the public appear to outweigh perceived benefits for a number of reasons. To cite one example, the value of the apps is not as readily visible as it would have been if the apps had, for instance, been initially implemented in small-sized communities before national roll-out. This reinforces what, as noted earlier, UX studies reveal about the importance of considering users' views about the utility of a new tech.

Concerns about privacy and data security are, not surprisingly, also at the core of the debate in contexts where minority groups risk persecution, where whole segments of the population are

[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".

concerned that data leakages might lead to increased risks and stigma for people who test positive for COVID-19, or – more in general – they may be reluctant to provide personal information when there is insufficient information and transparency about how the app works, and how data are collected, protected, stored and shared[21]. In these cases, the concept of privacy seems to be aligned also with the defence of positive rights, such as freedom of expression and the conditions necessary for human flourishing, but also with data protection rights. Similar concerns, however, have also been expressed in countries with stronger data protection regulations (including the United Kingdom), with potential users concerned about privacy violations and the possibility that their personal data will fuel data-driven surveillance by private companies or the government after the pandemic[22].

In the United Kingdom more specifically, and in line with insights from UX studies that highlight perceived tech efficiency and trust in authorities as key concerns, Panda Security's survey of nearly 2,000 people found that the pandemic has brought to the fore issues of trust and its link to perceived competence[23]. One third of the respondents had no trust at all in the government to successfully track and trace the virus through mobile apps. In line with those findings, based on a 10-minute online survey in March 2020 (N=1055) to British residents (asking hypothetical questions about future behaviour), Abeler and colleagues found out that there is wide support for app-based contact tracing (with about three-quarters of respondents saying that they would definitely or probably install the app, so comparatively higher than in other countries). But respondents who lack trust in the government are less favourable. According to the study, the main reasons against installing the app are a perceived increased risk of government surveillance after the epidemic, fear that one's anxiety about the epidemic would increase, and fear of one's phone being hacked. The same survey conducted in other western countries found very similar results[24]. A number of other barriers – issues about poverty, inability to buy or use a smartphone, inability to download the app, unmet need for more information and support – and concerns – worries about the battery usage in their

[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".
[23] Panda Security, Apathy in the UK.
[24] Abeler, Support in the UK.

phone – were also reported across the globe[25]. These represent social and practical problems which UX studies also identify as barriers to tech adoption[26].

In is important to note, however, that in line with insights from UX studies which show that perceived utility and efficiency can encourage user endorsement and adoption[27], many individuals surveyed (with numbers varying across countries, approximately 50-60% in most studies reported, but higher in Abeler et al.'s study on the United Kingdom, as reported above) recognised some benefit in downloading and using the app, *in primis* for its potential to help family members and friends, for a sense of collective responsibility to the wider community, and when they perceived the system as efficient, rigorous and reliable[28]. Lia and colleagues identified prosocialness (i.e., the set of voluntary actions one may adopt to help, take care of, assist, or comfort others), COVID-19 risk perceptions, general privacy concerns, technology readiness, and demographic factors as more important than app design choices (such as decentralized design vs. centralized design, location use, app providers) and the presentation of security risks as predictors of the willingness to use tracing apps[29].

Apart from studies focusing on (potential) users' behaviours, there have been also debates based on more conceptual, theoretical or systemic considerations around the contact tracing apps, with discussions pivoting around their system architecture, data management, privacy, security, proximity estimation, and attack vulnerability[30]. Among those, of particular interest are the concerns raised by Rowe who, focusing on the tracing app launched in France after a heated public debate, takes a critical stance[31]. He stresses how the app – despite the short term benefits – might create long-terms concerns about the potential encroaching on civil liberties. This can occur if the app induces significant risks to informational privacy, surveillance and habituation to security

[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".
[26] For instance, Tromp, "Design for Socially Responsible Behaviour".
[27] Ferreira, "Universal UX Design".
[28] 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".
[29] Lia, "What Makes People Install a COVID-19 Contact-Tracing App?"
[30] Ahmed, " A survey of COVID-19 contact tracing apps"; Mbunge, "Integrating emerging technologies".
[31] Rowe, "Contact tracing apps and values dilemmas".

policies, potentially fomenting discrimination and public distrust. Doubts about the necessity of the app itself were also raised: for instance, commenting the situation in Singapore, Woo arguments that it was the presence of fiscal, operational and political capacities that were built up after the SARS crisis – rather than the use of tracing apps – that contributed to Singapore's relatively low fatality rate (despite the high infection rates) and contact tracing capabilities[32]. Indeed, probably also because of a lack of technological literacy among some quarters of the population, but more likely for concerns over data privacy and a lack of trust in the government's ability to safeguard individuals' personal data, the local TraceTogether app was not widely downloaded by the Singaporean population.

While the studies here presented have been very useful in identifying key themes and issues – *in primis* privacy – affecting people's willingness to comply with the use of contact tracing systems, they have some limitations: methodologically, most of the reported studies were based on surveys administered over a limited timeframe, while discourses around the pandemic likely changed over its unfolding. The study by Simko and colleagues is measuring longitudinally, through a sequence of online surveys, the evolving nature of public opinions in the United States about the tensions between effective technology-based contact tracing and the privacy of individuals, but the sample (100 participants per survey) is very limited[33]. Additionally, while as UX studies suggest, exploring the willingness to comply with contact tracing (mostly in quantitative terms) can inform policy-making (as the effectiveness of the app largely depends on the public willingness and ability to support this type of measure), we believe it is important to further 'unpack' this puzzle to look, also qualitatively, at the socio-cultural and practical dynamics at the basis of public resistance and/or inability to use these apps.

In our study, we offer an empirical, methodological and conceptual contribution which combines computational capacities to investigate a large social media dataset expanding over 10 months and qualitative expertise in criminology to offer a new angle to reflect on emerging issues of public trust, governance, and the use of personal data for public good that are at the basis of people's resistance in using tracing apps, but that are unlikely to peter out after discussions on COVID-19

[32] Woo, "Policy capacity and Singapore's response to the COVID-19 pandemic".
[33] Simko, "COVID-19 contact tracing and privacy".

contract tracing apps will fade away. From a criminological standpoint, our study of the digital tracing app should uncover new insights that can expand current understandings of resistance to the new data-driven surveillance technologies currently transforming the landscape of decision making across the private and public sector, including the justice system. Whilst, as noted earlier, the extant criminological literature has to date focused on coercive surveillance systems such as electronic tags and generated very useful insights[34], our study expands the field by investigating a surveillance tech 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 of public reaction to digital tracing apps, we analysed a relatively large dataset of tweets to explore public discourse about the England and Wales' COVID track and trace app 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 6th March 2020 and continuing until 31st 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 had been chosen after preliminary manual searches to determine which ones were more used in this context. We identified relevant tweets *post hoc* from searches in the Twitter Web app (https://twitter.com/search-advanced) using the Web Data Research Assistant software developed by one of the authors[35]. This search produced a total number of 54,941 tweets (including a total of 4,269 hashtags) tweeted from 38,713 Twitter accounts over the 10 months considered[36].

[34] Nellis, Standards and ethics in electronic monitoring.

[35] 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.

36 It is worth noting that, of 38,713 accounts, 2,530 were considered "dormant" (that is, 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).

Overall, the study adopted a sociotechnical approach, developed though 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, the development and refinement of a qualitative conceptual map, and social network analyses); and (5) qualitative checks for bias minimisation. The methodological process can be found described in further detail in the project report[37]. It is worth noting that, even if our study made use of computational tools to aid our analyses (often associated to positivistic research approaches), our work mainly relies on a constructivist epistemology: as such, this research does not aim at identifying ultimate laws, but it rather aims to offer meanings that are relevant through interpretation.

Data analyses and results

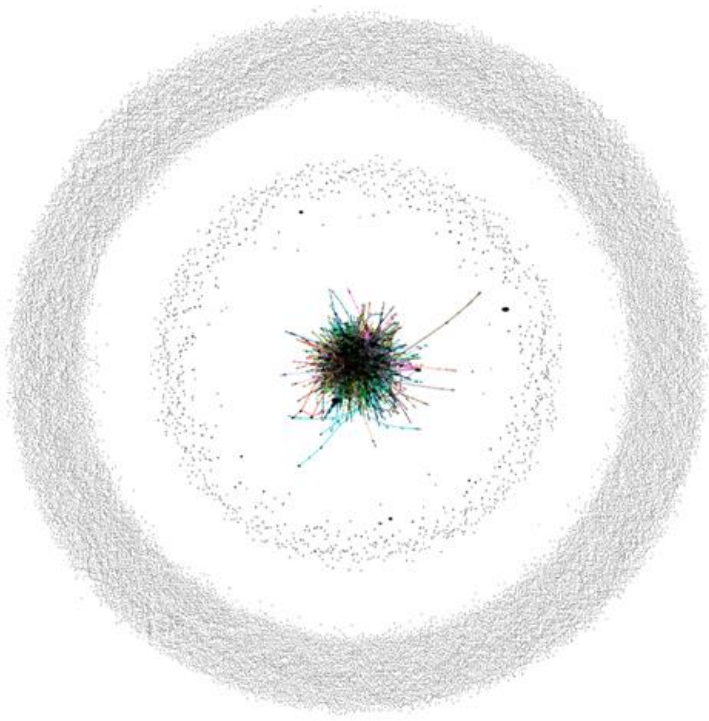
Interactions between accounts and conversation drivers

First, we were interested in understanding the interactions between the accounts to identify the drivers behind relevant conversations. To this end, we mapped the conversational network obtained by connecting two accounts where one replies to or mentions the other. We considered only those accounts that contributed a tweet in our collection, not the 18,351 other accounts that were mentioned, but did no otherwise participate in the conversation by tweeting on the topic. The network was plotted in Gephi using the Force Atlas layout [*Figure 1*]. As the Figure shows, we can identify (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 disconnected small groups (ranging from 2 to 99 accounts each) that replied to each other, and accounting for 2,832 accounts in total; and (3) a strongly connected central core of 9,741 accounts. In other words, the outer ring consists of just over two thirds of the accounts, the central core of just over a quarter, and the middle ring of the

[37] See Lavorgna, Understanding Public Resistance.

remaining 7%[38]. The network is coloured according to Gephi's modularity calculations which identifies the parts of a network that are highly modular in the sense that they are internally linked or well-connected clusters, which are located in the central core and correspond to the appearance of "clumps" in the layout.

Figure 1: Network of interactions (full)



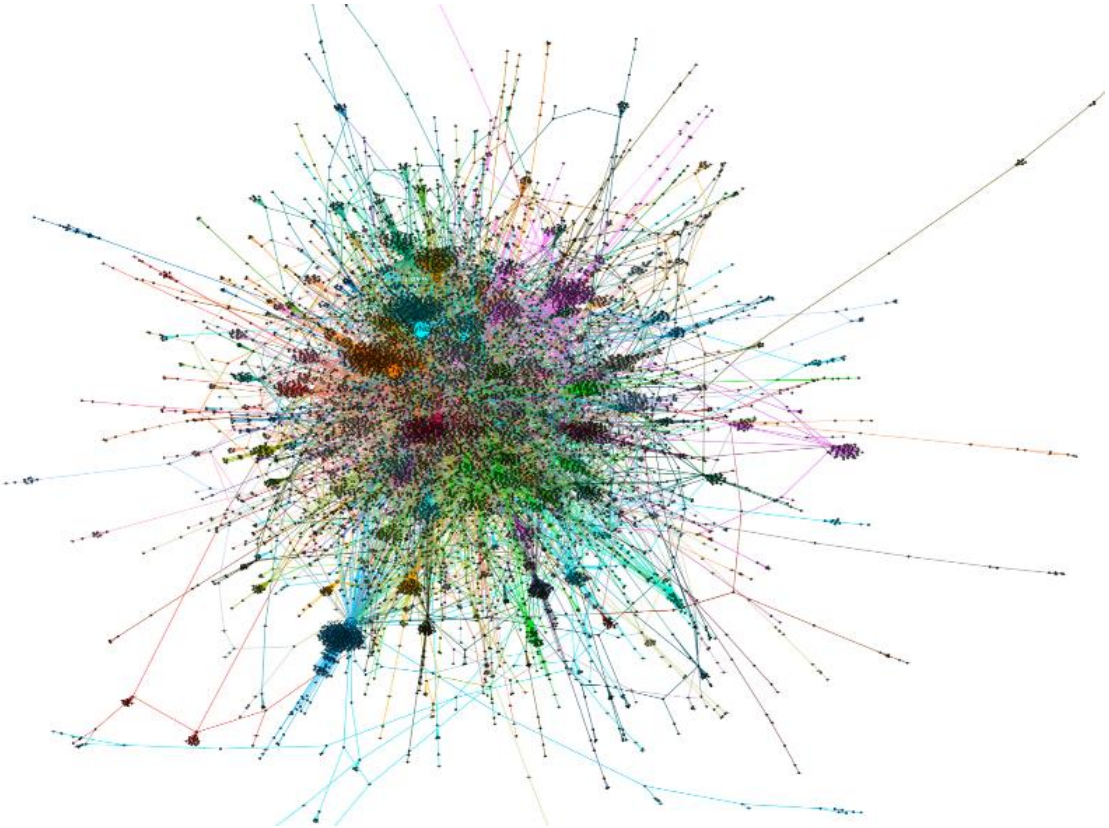
The majority of the users we observed (isolated individuals) outside the core cluster are therefore "shouting into the void": they are not part of any joined-up conversation on this topic, but their voices – as we will see in the next section – are still relevant to our analysis: by tweeting, they raise a number of themes that can offer valuable insight into their feelings about our topic of interest.

[38] 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).

Second, to understand the sociocultural and other key drivers at play as identified by the UX and algorithm aversion literature as well as algorithm aversion studies[39], we wanted to identify the conversation drivers. In other words, the type of social media actor setting the tone in the conversations observed. If we focus only on the connected core of the network [*Figure 2*], where most of the conversations occur, we can notice that this is dominated by large “clumps” of nodes and long “threads” emerging from those clumps. The clumps are centred around high status public broadcasters (like Sky and BBC), and political organisations (like Downing Street). Clumps form when many individuals respond only to a single account (a network hub) and do not share their attention with others. The threads that emerge from these clumps are chains of commentators that respond to each other’s contributions. Occasionally the discussants take part in multiple chains and hence create the “tangles” that are visible in Figure 2. This central interaction consists mainly of people responding to the journalists and prominent politicians, plus to the official account for the NHS app (as detailed in *Table 1* in the Appendix, presenting the accounts with more than 150 replies (indegree>150)), suggesting that much of the visible conversation is driven by tweets initiating responses from broadcasters and political accounts.

Figure 2: At the core of the network

[39] Consider, for instance, Royal Statistic Society, *Trust in data*; Dietvorst, *Algorithm Aversion*; Hartman, “Public perceptions of good data management”; Steedman, “Complex ecologies”.



High status Twitter accounts with many followers tend to generate more engagement in a conversation because they have a greater number of people seeing their tweets. However, if we look at the 25 highest-status organisations (with 1M+ followers) in our dataset (see *Table 2* in the Appendix), we can notice that many of these (e.g., the Economist) obtained almost no response to their (relevant, for the scope of this study) tweets. Furthermore, there is a notable absence of health organizations and professionals[40]: overall, it appears that health organization were not participating significantly in Twitter debates about the use of the NHS app.

Frames and mechanisms of resistance

[40] While no health organisations fall into the category of high status organisations (the most-followed NHS account is Public Health England, with 452K followers), we found 8 official NHS accounts in our dataset (NHSProviders; NHSCumbriaCCG; PublicHealth_NE; NTeesHpoolNHSFT; NHSX; NHSELRCCG; NHSDigital; LPFTNHS), together responsible for 14 tweets.

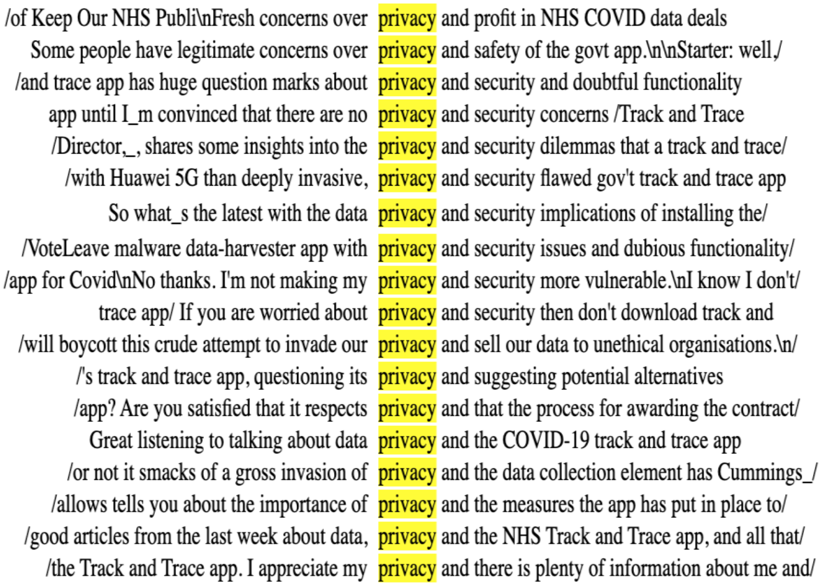
Having clarified the structural aspects of our social network of interest, and identified the conversation drivers, we were then ready to "zoom in" and look more in-depth, qualitatively, at our dataset, in order to unpack the key dynamics at the basis of people resistance in using the NHS contact tracing app.

Analytical approach

In order to understand the prevailing themes used by Twitter users "resisting" the use of the NHS tracing app, we first focused on the language used to build a concept map. Frequency tables were created of the hashtags, keywords and n-grams (i.e., phrases of 2 or more words) present in our full dataset. Two researchers started by looking manually at hashtags, starting from those more frequently used: indeed, even if only a minority of tweets (15%) used hashtags, we interpreted their use as a way to deliberately and explicitly enter the public discourses on Twitter on our topic of interest. The researchers then looked at keyword and n-grams to expand and refine their conceptualizations, until thematic saturation was reached (approximately after 800-1000 words per table). In fact, although the overall frequency was a useful indicator of the 'value' of a keyword for our analysis, we decided to avoid setting a predefined frequency threshold, as less frequently used words might still be valuable in pointing towards themes relevant for the scope of our analysis. In order to understand the context in which the words emerging as useful to identify the themes relevant for our study were used, we relied on the concordance tool – i.e., a way to present the data highlighting the keyword in its original context[41] [see *Figure 3*].

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

[41] Ross, "Discursive deflection".

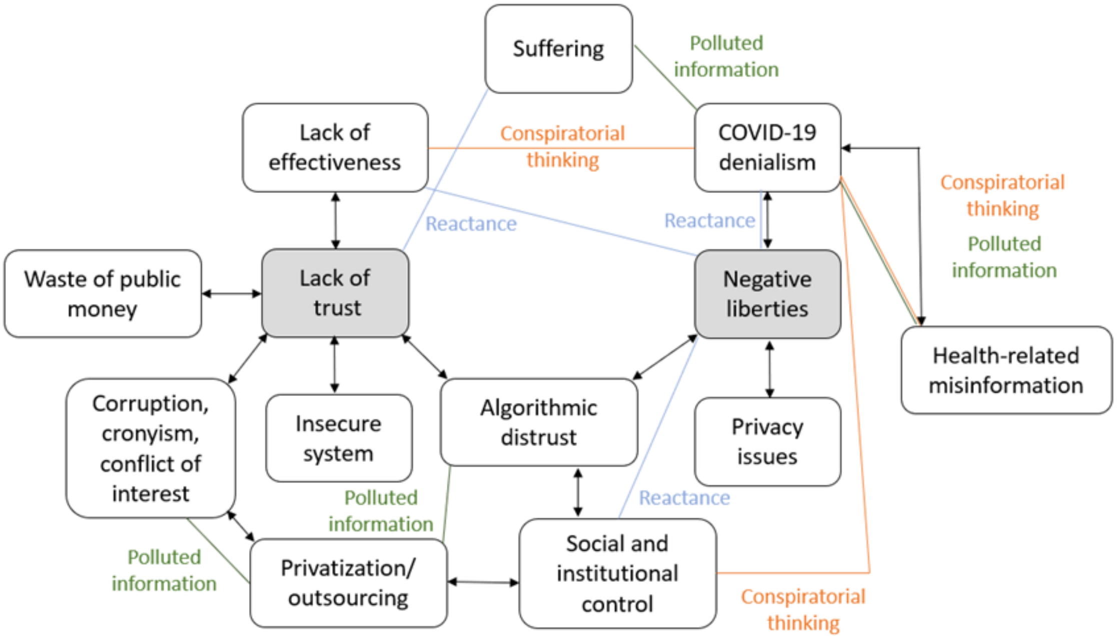


```
   /of Keep Our NHS Publi\nFresh concerns over privacy and profit in NHS COVID data deals
     Some people have legitimate concerns over privacy and safety of the govt app.\n\nStarter: well,/
  /and trace app has huge question marks about privacy and security and doubtful functionality
     app until 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/
```

This approach was used initially for the complete dataset, and then again on 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 see if differences emerged among these parts.

To facilitate a developing conceptualisation of the data, notes were individually taken and then shared, discussed and integrated drawing from insights from the UX literature and algorithm aversion studies, as well as their links to tech resistance into the following qualitative conceptual map [*Figure 4*, which indicates only the main connections identified for clarity purposes] highlighting the main themes and how they are connected.

Figure 4: Conceptual map



Through this conceptual map, we identified two main narrative frames (lack of trust; negative liberties), reinforcing insights from algorithm aversion studies which as noted earlier cite public distrust or a "data trust deficit" as central to public resistance to data-driven technologies[42]. We also identified three main mechanisms (polluted information; conspiratorial thinking; reactance) at the basis of people's resistance in using the of the NHS contact tracing app, which will be 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 built separately for each part of the network, some differences emerged. For instance, for the isolated individuals the focus was on being oppositional to the Conservative government and some of its members, indicating an entrenched lack of trust in the government and showing that to understand UX, algorithm aversion, and their links to tech resistance, consideration should be given to sociocultural contexts of new tech deployment such as the level of trust in the authority encouraging adoption. Lack of trust, indeed, can manifest itself in many different ways, and future research should further unpack how those relate to different

[42] Royal Statistic Society, *Trust in data*; Hartman, "Public perceptions of good data management".

sociocultural features, so to better understand its nuances, and better ideate *ad hoc* intervention to restore public trust, which remains fundamental in public health contexts[43]. There were also, unsubstantiated, imprecise or misleading claims on the more scientific aspects of the pandemic (e.g., herd immunity). It was only in the disconnected small groups that 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 traumas and injustice) emerged as prevalent. As already noted, UX studies show that practical concerns pertaining to the capacity of techs to generate or exacerbate stressful conditions for users should be taken into account during design and deployment, to avoid resistance. In the connected core, discussions also seemed to pivot around issues of privacy and alleged/perceived corruption, reinforcing UX studies of the sociocultural contexts of tech design as well as algorithm aversion studies which cite privacy violations as a factor fuelling public resistance. As noted earlier, the UX literature also suggests that users' beliefs, values, and so forth can provoke resistance. The finding regarding links between alleged/perceived corruption and resistance also reflect lack of trust in the government and forms part of the sociocultural milieu from which resistance emerges. It reinforces other findings from the algorithm aversion scholarship on the inextricable link between lack of trust in government and resistance[44].

Frames of resistance

Even if the themes identified in our manual analysis were very varied and heterogeneous, we could trace them back to two main narrative frames, which we summarized as *lack of trust* and *negative liberties*.

"Trust", in the tweets examined, 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/or the effectiveness of the app, towards societal trends increasing datafication). These various declinations of trust, of course, are linked to diverse types of concerns (which are beyond the scope of this contribution), but which nonetheless appear interrelated as

[43] Consider, for instance, Gille, "Why public trust in health care systems matters"; Schwartz, "Evaluating and Deploying Covid-19 vaccines".
[44] Devine, Trust and the Coronavirus Pandemic.

suggested by the previously cited studies. The existing research emphasises how various factors intersect to fuel public distrust and resistance. Future studies can further delineate the precise impact of each of these factors. Our study provides new insights into the range of factors and illuminates how the unique libertarian opportunities provided by Twitter and other social media 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 a diverse population of individuals[45].

At the heart of this lack of trust, is the perceived incompetence of the actors involved, who are seen as flawed, corrupt, hypocritical, and not accountable for their actions or inactions. This mistrust is pivotal to understand why, in some of the tweets observed, users seem 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 teachings of the “drift” and “digital drift” approaches in criminology, according to which the perceived lack of legitimacy or of effectiveness of the criminal justice system can lead towards delinquency, creating a “sense of injustice” towards authorities; individuals feel freed from social norms, and their behaviours will become dependent on transient opportunities and preferences[46].

Also, tech scepticism – including algorithm distrust – seemed to play a key role. Such techno-scepticism and public distrust of algorithms, which are typically targeted at the claims made about the purpose and effectiveness of technological solutionism and automated processes, and also at the decisions algorithms make, has been fuelled in part by highly published cases highlighting the harms of some data-driven algorithms (examples include biases in areas such as criminal justice decision making[47], and the distribution of healthcare resources[48]). Tech scepticism is also being

[45] For instance, Johnson, “The online competition”; and Lavorgna “To wear or not to wear”.
[46] See Matza, Delinquency and Drift; Holt, “Digital Drift”; and, more recently, Lavorgna, Information pollution as social harm.
[47] For instance, Angwin, “Bias in Criminal Risk Scores”.
[48] For instance, Price, Hospital “risk scores”.

reinforced by growing awareness of ethical issues such as privacy violations and the interrelated problems of poor explanability, transparency, and accountability[49]. In the context of contact tracing apps, concerns have been raised related to 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 a time of emergency politics[50].

The propagation of polluted information (as discussed below) adds yet another vital dimension to the growing problem of tech scepticism. Other scholars who have explored how social media have been used to improve or reduce trust in scientific expertise during the COVID-19 pandemic, for instance, have highlighted the capacity for social media to be deployed as mechanisms of misinformation, to undermine public trust in scientific expertise and accompanying systems such as algorithms[51]. These problems can trigger algorithm aversion which, as we have seen, refers to resistance to techs designed to automate tasks and a preference for human judgement or intervention[52].

In line with what has been reported in the recent literature on the resistance in using tracing apps, the value of privacy (broadly intended), and more in general the importance to protect personal data from unwanted surveillance or control from the government or big tech companies, seems to be an important matter of concern. There is a desire to contrast what are perceived as unwelcomed incursions and attacks hindering the right to privacy, with dimensions of vertical (institutional) privacy being of much more concern in the tweets observed than dimensions of horizontal privacy (that is, privacy between users of social media platforms)[53]. From this perspective, it is important to contextualize 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"* – that is, a specific type of individualistic freedom which manifests itself in the absence of constraints (as opposed to ideas of collectives' freedoms and liberties, focusing on the possibility of acting to realize one's fundamental purposes). This is in line with populist libertarian views and ideas of self-reliance

[49] Pasquale, The Black Box Society.
[50] Csernatoni, "New states of emergency".
[51] Clayton, "Real solutions for fake news?"; Llewellyn, "COVID-19: How to be careful with trust".
[52] Dietvorst, "Overcoming algorithm aversion".
[53] In line with Lavorgna, Information pollution as social harm.

(and often minimal government)[54]. These systems of beliefs and worldviews have an important role in science denialism[55], as scientific evidence is rejected when perceived as a threat to personal freedom in line with the psychological mechanisms of reactance[56] (discussed below); in the context of the pandemic, they are having a fundamental role in the opposition to preventive measures such as lockdowns, limitations to travelling and gathering, and the use of masks, which are here seen as an undue interference impacting individual and group liberties[57].

Mechanisms of resistance

Besides the narrative frames informing people's resistance in 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), shedding some light on the factors that are breeding high levels of public distrust. These are primarily sociocultural in that they reflect the current social and cultural climate of app deployment. As the UX studies cited earlier suggest, these should be considered during design and subsequent deployment to enhance responsiveness and minimise resistance.

Polluted information is a broader umbrella term that encompasses mis-information (when false information is shared, but no harm is meant), dis-information (when false information is knowingly shared to cause harm), and mal-information (when genuine information is shared to cause harm)[58]. Polluted information started to be studied in cyberspace as a particularly devious variant of information warfare, that can be propagated via countless platforms and that can cause great social harms by making people less knowledgeable, sharpening existing socio-cultural divisions, and making people more sceptical towards legitimate news producers and accurate reporting[59]. 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

[54] Boaz, The Politics of Freedom.
[55] See, for instance, Massa, "Don't trust the experts!".
[56] Prot, "Science denial".
[57] Lavorgna, Information pollution as social harm.
[58] Wardle, Information Disorder.
[59] Allcott, "Social media and fake news"; Lavorgna, Information pollution as social harm.

misinformation, causing major social harms[60]. From this study, it emerges that polluted information has allowed and facilitated not only a wealth of misleading health-related information (e.g., enabling antimask and antivax views, and questioning the importance of physical distancing), but – together with conspiratorial thinking – it has also fostered COVID-19 denialism and discourses minimizing the health risks related to COVID-19 (hence, people do not download and use the app as they believe there is no a real/serious health problem to be addressed). Moreover, a strand of polluted information has 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, all linked to negative themes such as corruption, conflict of interest and cronyism, and lack of trust. Serco is a private company that is 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, it played no role in the creation of the NHS Test and Trace app, and is not processing its data[61].

Conspiratorial thinking postulates a group of agents working together in a secret, often, though perhaps not always, for a sinister purpose[62]. In the context of resting the use of the NHS app, conspiratorial thinking was mostly observed as the driving force behind COVID-19 denialism, and behind the idea that the app is part of a clandestine plan for mass control. Similarly to what has been recently observed in ethnographic studies grounded in criminology, looking at online communities during the pandemic[63], while some of the concerns over the use of mechanisms of social and institutional control can be legitimate, the conspiratorial element is to be found in the fact that the existence of a clear direction is assumed, and science-fiction elements end up overshadowing realistic alarms on the potential for extreme dataveillance. It is not surprising to encounter conspiratorial thinking as a key driver in the context of the pandemic: conspiracy theories are often adopted defensively as they offer people some compensatory sense of control, giving them the chance to feel they have some power by rejecting official narratives[64], especially when they need to overcome feelings of alienation or anxiety in times of large-scale social

[60] Lavorgna, Information pollution as social harm.
[61] Krishna, Serco didn't build.
[62] Coday, "An introduction".
[63] Lavorgna, Information pollution as social harm; Lavorgna, , "Science denial and medical misinformation".
[64] Douglas, "Motivations, emotions and belief".

change[65]. Importantly, we should not dismiss conspiratorial thinking as some weird, fringe beliefs, as it can drive majorities to act on them in political, health, and social decision-making[66].

Reactance refers to how people tend to be averse to having restricted freedom or ability to act in a particular way. When this happens, they tend to reject evidence that is perceived as a threat to their ability to act (or do not act) in a certain way[67]. The NHS app, 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) is seen as an undue interference impacting individual liberties, with official recommendations being disregarded or opposed.

Discussion and conclusion

In our study, we have combined criminological expertise and qualitative approaches with computational capacities to investigate people resistance in using the NHS tracing 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 the themes discussed. The prevailing narrative frames (lack of trust; negative liberties) and mechanisms (polluted information; conspiratorial thinking; reactance) at the basis of people's resistance in 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 to qualitative investigation, to 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 and the social scientists providing subject matter expertise and theoretical oversight enabled us to observe general trends and well as to "zoom in" and analyse more in-depth sub-sets of data of particular relevance[68]. We aimed to unravel the various insights available from (a) the

[65] Bangerter, "How conspiracy theories spread".
[66] Uscinki, Conspiracy Theories; Pierre, "Mistrust and misinformation".
[67] Rosenberg, "A 50-year review of psychological reactance theory"; Prot, "Science denial".
[68] 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".

language used in the tweets, (b) the context of the authors of the tweets, and (c) the interactions between the authors that contributed to a ‘national conversation’, as the topic at the core of the tweets analysed is likely to be relevant to a very broad segment of the population, as it is about a behaviour that the entire adult population of England and Wales was expected to engage in. While this discussion was played out in more social platforms than Twitter, and in more spaces than simply online, Twitter allowed us to examine some aspects of these wider conversational engagements.

The conversations (and the lack of conversations) taking place in our dataset suggest some avenues of further research, with practical implications. For instance, could health organizations (that, as we have seen, were almost not entering Twitter debates about the use of the NHS app) be more active online, prompting better informed discussions? As most conversations took place around tweets by broadcasters and other significant accounts, could a more informative and less provocative use of tweets by traditional media outlets and journalists be useful in avoiding online polarizations on health-sensitive topics? From a strictly criminological perspective, our findings reinforce insights from the UX literature, highlighting key dynamics that should be integrated into any framework for understanding public resistance to new digital technologies, particularly surveillance systems such as digital tracing apps. One such mechanism is a recognition of the sociocultural contexts of tech design and adoption. This concerns the accepted beliefs, norms, and practices that prevail amongst target users. 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 techs and practice cultures; doubts about the social utility and technical efficiency of the techs; and lack of trust in their fairness[69]. There is also evidence that some police officers doubt the utility of predictive policing algorithms and express concern and distrust about their fairness for socially marginal communities[70]. Interestingly, our study similarly uncovers 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 indicates that

[69] For instance, Lavorgna, “The datafication revolution”.
[70] Babuta, Data Analytics and Algorithmic Bias.

even if their manifestations change across different contexts, the sociocultural dynamics prevailing at any one time and in any context should inform policy strategies aiming to address resistance to vital technologies such as apps that can improve public health.

Unfortunately, all the mechanisms of resistance identified are very difficult to counter and mitigate. Polluted information, for instance, touches upon 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 a partisan news in line with their system of beliefs), cheap to obtain, and can also be very difficult to identify[71]. Conspiratorial thinking finds a very fertile ground in situations when people's need to feel safe and secure in their world and to exert control over their existence are threatened, and can become extremely successful as it helps individuals' feelings of agency and power[72]. The phenomenology of reactance, similar to other psychological mechanisms at the basis of science denialism[73], reminds us why simply bombarding denialists with accurate scientific information does not lead to attitude change. So far, interventions targeting these mechanisms have not taken place in a coordinated way[74]. As discussed Recently in the context of harmful polluted information online[75], in lack of more profound architectural changes, interventions from online intermediaries, targeting the source, are proving relatively ineffective, and can potentially create serious tensions against individual rights; debunking activities often proved to ineffective and potentially even counterproductive, increasing polarization 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 multi-layered effort between a wide range of institutions, individual actors and technology is therefore needed to meet a fundamental social challenge that clearly goes beyond convincing users to use an app: this challenge, indeed, has to do with improving public scientific literacy and critical thinking, and restoring public trust. This trust, however, needs to be earned, which involves improving effectiveness and (institutional, political, and algorithmic) transparency.

[71] Allcott, "Social media and fake news".
[72] Imhoff, "Conspiracy Beliefs as Psycho-Political Reactions".
[73] Prot, "Science denial".
[74] Kreko, "Countering Conspiracy Theories"; Larson, "Blocking information".
[75] 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 Economic, University of Oxford, United Kingdom, 2020.

Ada Lovelace Institute. (2020). Exit Through the App Store? Retrieved from 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, 2016. Retrieved from 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. DOI:10.1109/ACCESS.2020.3010226.

Anuradha, Nagaraj. "Black holes": India's Coronavirus Apps Raise Privacy Fears, 2020. Retrieved from 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. Retrieved from 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 Michael Butter and Peter Knight (eds.) *Routledge Handbook of Conspiracy Theories*. London: Routledge, 2020.

BBC News. NHS data breach involving 284 patients uncovered, 2020. Retrieved from 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.

Boaz, David. *The Politics of Freedom: Taking on The Left, The Right and Threats to Our Liberties*. Cato Institute, Washington DC, 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. DOI:10.1007/s11109-019-09533-0.

Coday, David. "An introduction to the philosophical debate about conspiracy theories". In David Coday (ed.) *Conspiracy theories. The philosophical debate*. London: Routledge, 2016.

Csernatoni¸ Raluca (2020) New states of emergency: normalizing techno-surveillance in the time of COVID-19. *Global Affairs,* 6,3: 301-310. DOI: 10.1080/23340460.2020.1825108.

Dencik, Lina, Hintz, Arne, Redden, Joanna and Treré Emiliano. "Exploring Data Justice: Conceptions, Applications and Directions". *Information, Communication & Society,* 22, 7, (2019): 873-881. DOI: 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*, 0, no.0 (2020), 1478929920948684. doi: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).

Dietvorst, Berkeley, *Algorithm Aversion*, Publicly Accessible Penn Dissertations, 2016. Available at: 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.

Douglas, Karen M., Aleksandra Cichocka and Robbie M. Sutton. "Motivations, emotions and belief in conspiracy theories". In Michael Butter and Peter Knight (eds.) *Routledge Handbook of Conspiracy Theories*. London: Routledge, 2020.

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*, 15 July 2020.

Farries, Elizabeth. "Covid-tracing app may be ineffective and invasive of privacy, Government must be transparent to avoid unintended consequences". *The Irish Times*. 5 May 2020.

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, (2020): 6491:eabb6936. DOI: 10.1126/science.abb6936.

Fitriani. "COVID-19 Apps: Fear of Tyranny by Data". *The Jakarta Post*, 2020. Retrieved from 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 (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, Smith, Sarah and Mays, Nicholas. "Why public trust in health care systems matters and deserves greater research attention". *Journal of Health Services Research & Policy* 20, (2015):62-64. doi:10.1177/1355819614543161.

GOV.UK. Centre for Data Ethics and Innovation Independent Report: Review into Bias in Algorithmic Decision-Making. 2020. Retrieved from 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.

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.

Hartman, Todd, Kennedy, Helen, Steedman, Robin and Jones, Rhianne. "Public perceptions of good data management: Findings from a UK-based survey". *Big Data & Society*. 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.

Imhoff, Roland and Pia Lamberty. "Conspiracy Beliefs as Psycho-Political Reactions to Perceived

Power". In Michael Butter and Peter Knight (eds.) *Routledge Handbook of Conspiracy Theories*. Routledge, London, 2020.

Johnson, Neil F., Velásquez, Nicolas, Restrepo, Nicholas J. et al. (2020). "The online competition between pro- and anti-vaccination views". *Nature* 582 (2020): 230-233.

Krekó, Péter. "Countering Conspiracy Theories and Misinformation". In Michael Butter and Peter Knight (eds.) *Routledge Handbook of Conspiracy Theories*. Routledge, London, 2020.

Krishna, Rachael. "Serco didn't build and does not run the NHS test and trace app". Full Fact. 2020. Retrieved from 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.

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.

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.

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. arXiv preprint arXiv:2012.12415.

Llewellyn, Sue. "COVID-19: How to be careful with trust and expertise on social media". British Medical Journal, 368 (2020). Retrieved from https://www-bmj-com.proxy.library.uu.nl/content/368/bmj.m1160.long.

Massa, Ester. "Don't trust the experts!": Analysing the use of populist rhetoric in the anti-vaxxers discourse in Italy. In Anita Lavorgna and Anna D. Ronco (eds.). *Medical Misinformation and Social Harm in Non-Science-Based Health Practices: A Multidisciplinary Perspective*. Routledge, London, 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 (2020): 1631-1663.

Megnin-Viggars, Odette, Patrice Carter, Melendez-Torres G.J, 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): e0241473.

Nature. COVID-19 digital apps need due diligence. The International Journal of Science 5830, 563, 30 April 2020. doi:https://doi.org/10.1038/d41586-020-01264-1.

Nellis, Mike. Surveillance-Based Compliance using Electronic Monitoring. In Pamela Ugwudike and Peter Raynor (eds.) *What Works in Offender Compliance*. Palgrave MacMillan, London, 2013.

Nellis, Mike. *Standards and ethics in electronic monitoring. Handbook for professionals responsible for the establishment and the use of electronic monitoring*. 2015. Retrieved from 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*, 2020. DOI: doi.org/10.1007/s11845-020-02389-y.

Panda Security. “Apathy in the UK”: 80% of Brits Refuse to Download Covid Tracking Apps. 2020. Retrieved from 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.* Harvard University Press, Cambridge, 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. Social Sciences Technology, American Association for the Advancement of Science, Washington, DC, 2019. Retrieved from 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 Anita Lavorgna and Anna D. Ronco (eds.). *Medical Misinformation and Social Harm in Non-Science-Based Health Practices: A Multidisciplinary Perspective*. Routledge, London, 2019.

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.

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).

Royal Statistical Society. *Trust in data and attitudes toward data use/data sharing*, 2014. Available at: www.statslife.org.uk/images/pdf/rss-data-trust-data-sharing-attitudes-research-note.pdf.

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. DOI: 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*, 2020. DOI: 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*, 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. arXiv preprint arXiv:2005.06056.

Smith, Gavin DJ and O'Malley, Pat. "Driving Politics: Data-driven Governance and Resistance". *The British Journal of Criminology*, 57, no. 2 (2017): 275-298.

Steedman, Robin, Kennedy, Helen and Jones Rhianne. "Complex ecologies of trust in data practices and data-driven systems". *Information, Communication & Society*, 23, 6, (2020), 817-832. DOI: 10.1080/1369118X.2020.1748090.

Sweeney, Yann. "Tracking the debate on COVID-19 surveillance tools". *Nat Mach Intell* 2 (2020): 301-304. Retrieved from 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.

Tinati, Ramine, Susan Halford, Leslie Carr and Catherine Pope. "Big data: Methodological challenges and approaches for sociological analysis". *Sociology*, *48*, no 4 (2014a): 663-681.

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* (2014b): 177-181.

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.

Uscinski, Joseph E. *Conspiracy Theories and the People Who Believe Them.* Oxford University Press, Oxford, 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. DOI: 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):e20572. DOI: 10.2196/20572.

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

Weaver, Matthew. “Don't coerce public over contact-tracing app, say campaigners”. *The Guardian*, 26 April 2020.

Woo, Jie. “Policy capacity and Singapore’s response to the COVID-19 pandemic”. *Policy and Society* 39, no 3 (2020): 345-362. DOI: 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

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