DEMOS

WHAT'S IN A NAME?

A FORWARD VIEW OF ANONYMITY ONLINE

JOSH SMITH
ELLIOT JONES
ELLEN JUDSON

APRIL 2020

This project was supported by GCHQ

Published by Demos April 2020.

76 Vincent Square, London, SW1P 2PD
T: 020 3878 3955
hello@demos.co.uk
www.demos.co.uk
Charity number 1042046

ACKNOWLEDGEMENTS

First and foremost, this work would not have been possible without the support of GCHQ, whose expertise we were privileged to draw on in writing this report.

This report owes a great debt to those who have generously taken time to share their knowledge, and help shape the authors understanding of the philosophical, technical and social aspects of anonymity. In particular, thanks are due to Alfred Moore, Hany Farid and John Naughton, whose thinking, technical expertise and patient conversation were invaluable to the formation of this report.

At Demos, this work would not have been possible without the invaluable conversations, arguments and brainstroming sessions held within and without CASM, with particular thanks to Alex Krasodomski for his formative input and clarity of thought, and the ever guiding hand of Carl Miller. Thanks to Maeve Thompson and Josh Tapper, who helped shape the report into the document you hold before you now, to Izzy Little for her design genius, to Stanley Phillipson Brown for his thoughtful input and tireless proofreading, and to the entire Demos team for their support and bonhomie.

As ever, all mistakes and ommission remain the authors' own.

Josh Smith
Elliot Jones
Ellen Judson
April 2020

EXECUTIVE SUMMARY

"There is a dilemma at the heart of anonymity. It is valuable because it enables expression free from repercussions, but anonymity is also destructive for precisely the same reason."

Policymakers and other public figures are increasingly vocal on the importance of balancing the benefits and drawbacks of online anonymity. In our efforts to build a better Internet, we require clear and consensual understanding of the language, concepts and infrastructures of anonymity. Drawing on legal, philosophical and historical evidence and interviews, this paper clearly articulates how online anonymity should be understood. It presents a model through which future settlements on online anonymity can be tested, presented in a way that we hope is useful to both technologists and policymakers.

Anonymity is a concept with an inherent tension at its heart. It is valuable because it enables expression free from repercussions; it is destructive for precisely the same reason. Discussions of anonymity online have often ignored this complexity, lacking clarity, evidence or agreement. This has slowed progress towards a better settlement. Historically, liberal democracies have aimed to strike a balance between the value and threats of anonymity. This balance has been destabilised by the digital commons. This paper shows how it might be re-established.

Three questions underpin the concept of anonymity:

- Can our actions be connected to us?
- How are our actions and identities connected?
- Who is able to make those connections?

We believe anonymity should be understood as a relational concept. One can only be anonymous to some other individual or organisation. Anonymity in the future should be discussed in the context of *who or what is a user anonymous from?*

As such, we propose a three-fold test for how anonymity should function online in liberal democracies. Future solutions must:

1. Protect internet users' ability to choose anonymity online, and emphasise its importance in preserving freedom of expression.
2. Allow accountable institutions tasked with preserving security under a democratic mandate to exercise their powers effectively.
3. Ensure users are able to provide meaningful consent to any deanonymisation by third-parties.

Current approaches fail all three tests. Public debate tends to reject anonymity online, presenting it as little more than a mask for crime, 'trolling' and abuse, rather than a fundamental and important freedom. Current infrastructure hinders security services from carrying out their democratically mandated roles in protecting society. And internet users are woefully unable to give consent to the data collection and profiling practices that underpin the majority of online services.

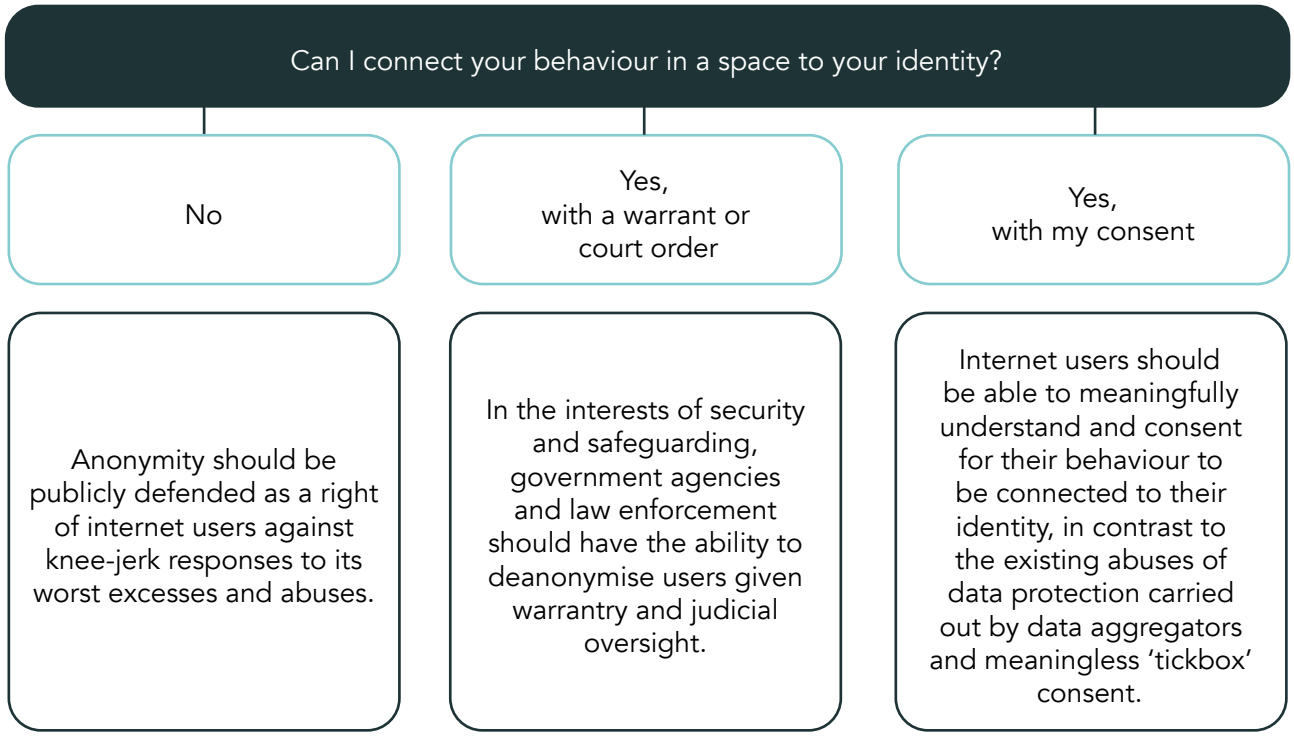
In line with these principles, we propose one solution to the problem of balancing online anonymity and identity: creating an alternative independent identity authentication body, at an arm's length from both the private sector and the central state. Possible approaches include a BBC-style royal charter, with some mixture of state and user-based funding. We also propose short-term fixes that could be made by stakeholders in this space.

In this report, we examine two identity systems - those of the Government Digital Service's 'Verify' program, and Facebook. Any attempt at identity provision needs to learn lessons from these systems.

In particular, it needs to recognise the significant challenges these examples highlight, in terms of preventing exploitation, serving users' needs, and securing sensitive data, among others.

SOLUTIONS TO THE ANONYMITY PARADOX

We believe that successfully balancing the benefits and challenges of anonymity online will require a system to allow for three possible answers to the question below.



INTRODUCTION

Anonymity is that rare word which seems to contain its own definition: it is the state of being nameless. This outward simplicity conceals complex questions of scope, surveillance, and the ways in which we construct and perform our identities.

Whether and how our actions are connected to us, and who is able to make those connections, is also of fundamental importance to the ways in which we inhabit physical and online space.

The hidden complexity and importance of the concept make it difficult to design for anonymity on platforms, and complicates the answer to a vital question: how should anonymity work online?

This report, conducted by the Centre for the Analysis of Social Media at Demos, investigates the regulatory and design challenges involved in anonymous action and sets out a series of technical and policy recommendations for how these challenges might be approached.

Drawing on existing literature and a series of interviews conducted with philosophers, legislators and those combatting harm online, the report provides some background on the historical, legal and political role played by anonymity, and examines some of the arguments currently being made for and against anonymity's importance online.

We then present a new definition of anonymity, along with a conceptual framework through which we hope some of the complexities raised can be more fully explored. Finally, we address the state of anonymity as it stands online today, examining as case studies the approach to identity taken by Facebook, and that pursued by the Government Digital Service's 'Verify' program.

Drawing on this research, we have developed a number of recommendations designed to help regulators, platform designers and those using services online think critically about the role which anonymity plays, and might play, on the Internet.

SECTION 1
THE RISKS AND REWARDS OF ANONYMITY

"The challenge for those regulating for anonymity or designing the ways in which users are described on platforms, is whether a solution can be found which maximises the benefits in each case while minimising the costs."

A precise diagnosis of the tension underpinning anonymity is provided by Alfred Moore, who describes two normative positions: "One is that anonymity is valuable because it enables expression free from fear of repercussions. The other is that anonymity is destructive because it enables expression free from repercussions. The same feature that enables a teenager from a religious community to talk freely about his sexuality without fear of exposure also enables cruel and abusive responses which may inhibit such expressions."[1]

The ability to anonymously post pictures, download music, or purchase goods enables free expression, access to art without censorship, and consumer privacy, but also allows for bullying, piracy, and the trade in controlled substances. The challenge for those regulating for anonymity or designing the ways in which users are described on platforms, is whether a solution can be found which maximises the benefits in each case while minimising the costs.

To bring some shape to what threatens to be an abstract discussion, we outline below some examples of the harms and benefits associated with anonymous action online. While this cannot be a comprehensive overview, we hope that addressing some specific cases will help cast light on the issue.

THE REWARDS

Anonymity can be essential in enabling people to exercise their rights to freedom of expression and freedom of opinion. It allows them to exchange information, develop points of view, engage in correspondence, express opinions; especially where they would otherwise face controls on what information they can access, or persecution for discussing or holding certain views.[2]

There are many groups who could be put at risk of significant harm if forced to disclose their identity to participate in online communications:

- Journalists and their sources, particularly corporate or state whistleblowers.
- Activists and civil society.
- Members of marginalised groups at risk of persecution or abuse due to their ethnicity, gender, religion or sexual orientation.
- Citizens trying to access, share or discuss information that their government does not wish them to see.[3]

1 Alfred Moore, 'Anonymity, Pseudonymity, and Deliberation: Why Not Everything Should Be Connected', Journal of Political Philosophy, 26.2 (2018), 169–92 <https://doi.org/10.1111/jopp.12149>.
2 David Kaye, Report on Encryption, Anonymity, and the Human Rights Framework (OHCHR, 2015) <https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx> [accessed 27 February 2020].
3 Human Rights Watch, 'UN: Online Anonymity, Encryption Protect Rights', Human Rights Watch, 2015 <https://www.hrw.org/news/2015/06/17/un-online-anonymity-encryption-protect-rights> [accessed 27 Feb 2020].

Even in conditions where people are at a lower risk of identity-based persecution, there can still be significant risks associated with being made to disclose their real identity online. Campaigns such as #MyNameIs, protesting real-name policies on platforms such as Facebook, highlight that people who have or are experiencing harassment, abuse, sexual violence, domestic violence or stalking need to be able to access online spaces anonymously in order to protect themselves from their abuser.[4] [5] [6] An international survey by Amnesty International found that '26% of women who experienced abuse or harassment... said personal or identifying details of them had been shared online'.[7]

As such, although anonymity may in some cases 'protect' criminals,[8] it also protects people (including law enforcement) from criminals and protects people whose 'crime' has been the exercise of their rights.[9]

THE RISKS

The ability to act anonymously can be a factor in enabling harmful behaviour. Below we examine the role anonymity plays in two cases, both the subject of current legislative attention in the UK:

1. Engaging in abuse, harassment and threats directed at specific groups or individuals.
2. Sharing and consuming content related to child sexual exploitation and abuse (CSEA).

The problem of abuse and harassment is widespread online and can have lasting negative repercussions for its victims. A survey commissioned in 2017 by Amnesty International found that 23% of women across eight countries had experienced online harassment at least once, with 41% of those who had experienced it stating that online abuse made them feel that their physical safety was threatened, and 55% saying they had been affected by stress, anxiety or panic attacks afterwards.[10] In these cases, anonymity can prevent victims, law enforcers and a broader social peer group from demanding that abusers face repercussions for their behaviour. As reported by the Law Society, the fact that abuse comes from an anonymous source can also affect the way in which the abuse is experienced by its victims.[11] Abuse and harassment also affect how its victims participate in online spaces.[12]

The sending or sharing of abusive messaging can be damaging to victims without meeting the high threshold for illegality, or, indeed, the lower threshold of each platform's terms of service for what constitutes unacceptable content. As such, it is as much an issue for those who moderate spaces online, and participants in an online discussion, as it is for law enforcement. However, anonymity also plays a role in behaviour which is clearly illegal, such as the creation and sharing of material related to child sexual exploitation and abuse (CSEA). This has been a focal point for British policymaking around online harms and features prominently in the government's Online Harms White Paper.[13]

As in cases of abuse, the perception of anonymity can allow people to distribute CSEA imagery without feeling they will be identified. It may also play a psychological role in enabling people to behave in ways which they would otherwise not contemplate. Suler suggests that the ability to act anonymously online produces a dissociative effect, allowing people to distance themselves from their behaviour, and therefore from responsibility for that behaviour.[14]

The ability to act anonymously is clearly not the only factor which influences someone's likelihood to abuse and exploit children. Indeed, neither is it a necessary condition. On Facebook, an explicitly 'real-name' environment which requires a verified email address or phone number, the company reported

4 #MyNameIs, My Name Is Campaign, 2020, <http://www.mynameiscampaign.org/> [accessed 27 Feb 2020].
5 NNEDV Safety Net Project, 'Why Privacy and Confidentiality Matters for Victims of Domestic & Sexual Violence', Tech Safety, 2016 <https://www.techsafety.org/privacymatters> [accessed 27 Feb 2020].
6 Hanane Boujemi, 'The right to online anonymity', Hivos, 2017 <https://www.hivos.org/opinion/the-right-to-online-anonymity/> [accessed 27 Feb 2020].
7 Amnesty, 'Amnesty Reveals Alarming Impact of Online Abuse against Women', 2017 <https://www.amnesty.org/en/latest/news/2017/11/amnesty-reveals-alarming-impact-of-online-abuse-against-women/> [accessed 27 February 2020].
8 Although the report from the Special Rapporteur notes that "State authorities have not generally identified situations - even in general terms, given the potential need for confidentiality - where a restriction has been necessary to achieve a legitimate goal" - David Kaye, Report on Encryption, Anonymity, and the Human Rights Framework. p.12.
9 David Kaye, Report on Encryption, Anonymity, and the Human Rights Framework.
10 Amnesty. This example, and others, are raised in DCMS' Online Harms white paper.
11 Law Commission, Abusive and Offensive Online Communications <https://www.lawcom.gov.uk/abusive-and-offensive-online-communications/> [accessed 27 February 2020]. Article 3.68
12 Amnesty.; Glitch, 'The Impact of Online Abuse', 2017 <https://fixtheglitch.org/impactofonlineabuse/> [accessed 27 February 2020].
13 Department for Digital, Culture, Media and Sport and Home Office, 'Online Harms White Paper', GOV.UK, 2019 <https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper> [accessed 27 February 2020].
14 John Suler, 'The Online Disinhibition Effect', CyberPsychology & Behavior, 7.3 (2004), 321–26 <https://doi.org/10.1089/1094931041291295>.

removing 11.6 million pieces of content related to child nudity and sexual exploitation in late 2019.[15] While some of this material could have been shared by fake accounts, interviews conducted for this report with those involved in combating CSEA online suggested that perpetrators often act using accounts bearing their full names, believing they are unlikely to be prosecuted for this behaviour or indeed caught at all.

Two other factors which contribute to the online sharing of illegal and abusive material are likely to be at least as important as the masking and psychological effects of anonymity. The first is a continued lack of technical capability to detect known abuse material at scale. While technologies such as PhotoDNA, launched in 2009, have been extraordinarily effective in detecting images of abuse, platforms have historically been slow to employ these technologies, and more development is needed to meet the challenge posed by increasing quantities of video content.[16]

The second is that law enforcement often lacks the resources needed to bring offenders to justice, even where these are directly reported. The Internet Watch Foundation has for the last two years verified record volumes of reported CSEA content, identifying ~137,000 pieces of CSEA material in 2018.[17] In 2019, the National Police Chiefs' Council lead for child protection claimed that the number of reported images and videos was overwhelming the police's ability to deal with serious offenders.[18]

CSEA material, then, remains difficult to detect and difficult to prosecute. These factors help create the damaging appearance that perpetrators can act without repercussion. While they remain at play, even the ability to completely remove anonymity from all online activity would not alone be sufficient to prevent online abuse.

15 'Facebook Removes 11.6 Million Child Abuse Posts', BBC News, 13 November 2019, section Technology <https://www.bbc.com/news/technology-50404812> [accessed 27 February 2020].

16 Hany Farid, 'Reining in Online Abuses', 2018 <https://doi.org/info:doi/10.21300/19.3.2018.593>.

17 Internet Watch Foundation, 'Annual Reports', IWF <https://www.iwf.org.uk/what-we-do/who-we-are/annual-reports> [accessed 27 February 2020].

18 Lizzie Dearden, 'Police "Overwhelmed" by Child Sex Abuse Image Cases Call for New Approach as Thousands of Paedophiles Seek Help | The Independent', The Independent <https://www.independent.co.uk/news/uk/crime/child-sex-abuse-paedophile-police-images-a8902036.html> [accessed 27 February 2020].

SECTION 2
ANONYMITY IN CONTEXT

"...the rise of the Internet has given us more opportunities for anonymous or pseudoanonymous interaction."

The section below provides some historical and legal context for anonymity, as well as exploring its importance as a core tenet of liberal democracy.

ANONYMITY IN HISTORY

Publishing under an assumed name or under no name at all is almost as old as the written word, across every kind of writing. Sometimes, the cloak of anonymity or the use of a pseudonym was necessitated by the underlying identity of the author; for example, a woman writer for whom writing and publishing would have been seen as improper.[19] In other circumstances, the intention of anonymity was for the arguments presented in a piece to succeed or fail on their own terms, rather than due to the prestige (or infamy) of their authors.[20]

Outside of acts of publication, anonymity in public space has historically been a relatively uncommon phenomenon. Until the modern era, the bulk of interpersonal interaction took place face-to-face, and true anonymity under these conditions is difficult. As Moore notes, even in the case of a brief conversation between strangers on the street, a wide range of personal characteristics and contextual clues about the other person are available to each which could enable some form of identification and, if the interlocutors were to encounter each other again, each may be able to identify the other as at least the same stranger.[21] It was not until the advent of the telephone in the early 20th century that real-time anonymous communication started to become plausible.

ANONYMITY IN THE LAW

There is a strong precedent for public anonymity (or at least partial anonymity) in British law. For example, judges are permitted to place reporting restrictions on cases, such that the identity of key actors is not known outside the courtroom, and thus is at least pseudoanonymous to the wider public. This protection extends beyond the antagonists in a case. In instances such as blackmail, the judge may not require the witness to give even their name in public The Crown Prosecution Service allows for crime to be reported anonymously, as through the 'Crimestoppers' charity.[22]

For greater protection and preemptive anonymity, applications for witness anonymity can be made pre-trial under sections 74 to 85 of the Coroners and Justice Act 2009.[23] These are only available to young adults, those part of an accused group primarily comprised of young adults, those accused of certain severe offences such as murder with a firearm, or those who it is reasonably expected would face harm or intimidation if they were identified. In very serious and extreme circumstances, witnesses who go into protection schemes may acquire whole new identities.[24]

These rights to anonymity in the UK context only extend to the process of the law itself, rather than protections granted by the law in other circumstances where one might want to remain anonymous. This likely reflects the fact that, as we noted above, the scope for scenarios where the

19 Gillian Paku, 'Anonymity in the Eighteenth Century', 2015
20 Moore.
21 Moore.
22 The Crown Prosecution Service, 'Reporting a Crime' <https://www.cps.gov.uk/reporting-crime> [accessed 27 February 2020].
23 Coroners and Justice Act 2009 <http://www.legislation.gov.uk/ukpga/2009/25/contents> [accessed 27 February 2020]
24 The Crown Prosecution Service, 'Witness Protection and Anonymity' <https://www.cps.gov.uk/legal-guidance/witness-protection-and-anonymity> [accessed 27 February 2020].

question of anonymity and its preservation might arise has only been expanded relatively recently.

Historically then, the circumstances in which the question of identity was both most sensitive and most likely to be contentious was in the courtroom. Anonymity, in this case, is often required to ensure a fair trial, for example by allowing witnesses to speak freely and give honest accounts without fear of consequences from potentially dangerous perpetrators. Further, anonymity during trials for young adults or serious offences protects the accused from having their reputations marred and lives derailed by those accusations if they turn out to be false or unprovable in the court of law.

The idea that anonymity should primarily be considered in the domain of the legal process has only recently begun to shift. Past governments, which were dominated by aristocratic and economic elites until the waves of suffrage in the 19th and 20th century, had little incentive to defend anonymous expressions where one might want to share information publicly but anonymously, such as whistleblowing or making critiques of the ruling class. Today, there are notable exceptions in the law, which enshrines, for example, the right to cast secret or anonymous ballots in elections. These can be linked to a shift towards democratisation and a recognition of the importance of circumstantial anonymity in a liberal democracy. We explore this further below.

ANONYMITY AS A CORE TENET OF LIBERAL DEMOCRACY

Anonymity in certain circumstances is seen as a core part of the function of liberal democracies.[25] In 19th century Britain, the election of parliamentary representatives was still accomplished by a show of hands. This meant that landlords and bosses knew how their tenant or employee had voted and so could coerce their decision. The demand for a secret ballot was a key demand of the Chartists and their campaign for suffrage for working-class men.[26]

It was not until the Ballot Act was passed in 1872 that votes became anonymous and the identity of a given voter became secret.[27] Today, this anonymity is seen as a crucial protection which ensures free and fair elections and undergirds the whole democratic process. By contrast, in the public sphere, we expect the votes of our representatives in the legislatures to be openly and transparently linked to those who cast them. We want them to be accountable for what they decide on our behalf.[28]

This demonstrates both the importance of anonymity in democratic life, as well as the dilemma it poses.[29] We want individuals to be able to freely express their preferences, to engage in discourse in an honest and constructive way without fear of persecution for their beliefs and to be able to blow the whistle on wrongdoing by public and private figures without fear of repercussion.

At the same time, accountability is key to a functioning liberal democracy. Individuals should be able to be held accountable and asked to defend their decisions and beliefs under scrutiny from others; those spreading hate, distrust and disrupting discourse should be able to be held accountable for their behaviour; those that slander and smear should be compelled to own that accusation.

As these examples show, there can be clear cut cases where absolute anonymity or absolute identification are justifiable and desirable in a functioning democracy. But in many cases, especially as the rise of the Internet has given us more opportunities for anonymous or pseudoanonymous interaction, we need a clear way of conceptualising anonymity and deciding what level and kind are appropriate in a way that balances the security of the individual with the health of societal discourse.

25 'Declaration on Criteria for Free and Fair Elections', Inter-Parliamentary Union <https://www.ipu.org/our-impact/strong-parliaments/setting-standards/declaration-criteria-free-and-fair-elections> [accessed 27 February 2020]. & Guy S. Goodwin-Gill, Free and Fair Elections, New expanded ed (Geneva: Inter-Parliamentary Union, 2006).

26 'The Secret Ballot' <http://www.bl.uk/learning/histcitizen/21cc/struggle/chartists1/historicalsources/source8/secretballot.html> [accessed 27 February 2020].

27 '1872 Ballot Act', UK Parliament <https://www.parliament.uk/about/living-heritage/transformingsociety/electionsvoting/chartists/case-study/the-right-to-vote/the-chartists-and-birmingham/the-chartist-legacy/1872-ballot-act/> [accessed 27 February 2020].

28 Daryl Glaser, 'The Case Against Granting a Secret Ballot to Elected Representatives: Democratic-Theoretical Reflections on a South African Controversy', Politikon, 46.2 (2019), 157–74 <https://doi.org/10.1080/02589346.2019.1601440>.

29 Tim Jordan, 'Does Online Anonymity Undermine the Sense of Personal Responsibility?', Media, Culture & Society, 41.4 (2019), 572–77 <https://doi.org/10.1177/0163443719842073>.

SECTION 3
DEFINING ANONYMITY: A NEW CONCEPTUAL FRAMEWORK

"An individual is anonymous to an observer to the extent that that observer cannot trace that individual's behaviour to them, or to accounts which relate to them."

'Anonymous' is a composite term, from the Ancient Greek 'an-' (without) and 'onyma' (name). Defining anonymity, then, seems trivial; it is the state of remaining unnamed.

This definition, however, conceals some important questions, a couple of which are brought sharply into focus when considering our actions in online space. One concerns what constitutes an act of naming; what it means to identify an individual. There is also a question of scope; whether the concept of anonymity can be properly applied to a person, or must apply to that person's actions, and the traces they leave, instead.

ANONYMITY AND THE GDPR

The EU's General Data Protection Regulation (GDPR), perhaps the most important piece of modern legislation concerning people's privacy with respect to their actions, mentions anonymity only once. It sets out this definition, almost in passing:

"The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person."[30]

This legal view suggests a definition for anonymous information; it must not identify, or allow the identification of, a natural person. The meaning of 'natural person' here essentially equates to 'single human being', or a 'data subject' in the GDPR's terminology. Since these phrases can seem clunky, we will substitute the term 'individual' for them throughout. We will talk of an individual as a natural person, but we hope our definitions below will also apply to bots, companies and other actors who are present in online and offline space.

The GDPR also provides some insight into how an individual might be 'named'. Article 4 gives the following list:

"An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."[31]

In this way, the GDPR's definition of identifying data stretches beyond their name, address and National Insurance number. It encompasses the wide range of pseudonyms and aliases they might adopt online; from Twitter handles to usernames on an online game. Below, we refer to these various aliases as the 'accounts' operated by an individual.

The GDPR's consideration of online account names as identifying data might seem to diverge from

30 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)', 2016 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504> [accessed 27 February 2020].
31 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)'.

an intuitive definition of anonymity. For example, suppose a comment has been left under a news article, using the account name 'Nobody101', the only identifier known to us. In this case, it would seem reasonable to say that these posts were left anonymously, although their username would be considered an identifier under the GDPR. Below, we will argue that the extent to which this form of naming constitutes a breach on anonymity will depend on a number of factors, including how that account is habitually used by its owner, and how it can be linked to the rest of that individual's activity.

AN EXISTING DEFINITION

A precise definition of anonymity to which this paper is indebted is proposed by Pfitzmann and Köhntopp.[32] Their 2001 paper gives the example of a message sent between a subject and a recipient, and imagines an attacker who is trying to identify either party. To talk of anonymity, the authors introduce the concept of an 'anonymity set', defined as the collection of subjects who could have sent or received the message.

Anonymity is then defined as the state of being unidentifiable within this group of subjects. The more possible senders there are in an anonymity set, the more anonymous the actual sender can be; if the anonymity set contains only one person, the sender has been identified.

This definition provides a useful and precise way of thinking about anonymity, but focuses on the identity of a single account, rather than the various spaces which might be inhabited by an individual online. Furthermore, as stated by the Law Commission in 2018, the setting of messages sent between single individuals, and the antagonistic framing of subjects vs attackers, does not straightforwardly translate to the forms of communication in open social and discursive spaces, and where a user may want to remain anonymous from a party with whom they might have a legal relationship, for example in the form of a signed Terms of Service agreement.[33] We have attempted to frame the definition of anonymity developed below in a sense which takes these considerations into account and is a step less technical, but without contradicting Pfitzmann and Köhntopp's definition, or their suggested terminology.[34]

ANONYMITY AND PRIVACY

The concepts of anonymity and privacy are closely related. Privacy is a broad concept, which we do not intend to fully define here. In order to focus on anonymity, however, it is useful to draw a distinction between the two.

For the purposes of this report, we will take the concept of privacy to concern cases where an individual wants to ensure their actions or dispositions are not observed or known by a third party without the individual's consent. As a heuristic, where someone is 'private', the individual natural person is known but their actions unknown.

In cases of anonymity, the direction of emphasis is reversed. To say that an individual is acting or behaving anonymously is to say that the action is observed, but without that observer being able to identify that individual; as the GDPR puts it, the information is known but cannot be related to a natural person.

These concepts are clearly related. If a private individual wishes to perform public actions without having those actions ascribed to them, these actions need to remain anonymous. In this sense, anonymity can be a means for an individual to protect their privacy.

In short, privacy broadly relates to a known actor whose actions are unknown; anonymity relates to known actions with an unknown actor.

ANONYMITY AND SCOPE

In speech, we often assign anonymity as a property of individuals. We say, for example, that an online commenter is anonymous, or that a journalist has received an anonymous tip. This use conceals an important question of scope. When told that a user on an online platform is anonymous, the crucial question we need to ask is: anonymous to whom?

Take, for example, a news platform which requires users to register, but allows comments to be left without a username. In one sense, the authors of these comments remain anonymous, in the sense that other readers cannot link their comments to an author. If we widen the scope, however, this anonymity evaporates, as the news platform knows exactly which registered account left that message.

32 Andreas Pfitzmann and Marit Köhntopp, 'Anonymity, Unobservability, and Pseudeonymity — a Proposal for Terminology', in International Workshop on Designing Privacy Enhancing Technologies: Design Issues in Anonymity and Unobservability (Berkeley, California, USA: Springer-Verlag, 2001), pp. 1–9.

33 Law Commission

34 As Pfitzmann and Köhntopp themselves put it, our aim is to develop vocabulary which "might be added consistently to the terms" defined in their paper.

In some cases, the anonymity of an author will depend on the technical skills or data possessed by an observer. If our author sets up an account which does not require a verified email address, for example, they may remain anonymous to that account's provider, but could still be linked to their comment through some other identifier, such as the IP address of the computer they use to connect to the site. It could also depend on the content on the post. Users describing the name of the bands they used to be in as teenagers, or the specifics of their tattoos, may remain anonymous to all but those who knew them growing up. An individual action, then, can be anonymous to some observers but not to others.

This highlights an important point: anonymity is at its heart relational. Rather than being an intrinsic property of an actor in relation to an action, it describes a relationship between a subject and an observer, either specified or loosely defined.

With the above in place, we are now able to propose a definition of anonymity:

An individual is *anonymous* to an observer to the extent that that observer cannot trace that individual's behaviour to them, or to accounts which relate to them.

We explore this definition, and its implications, further below.

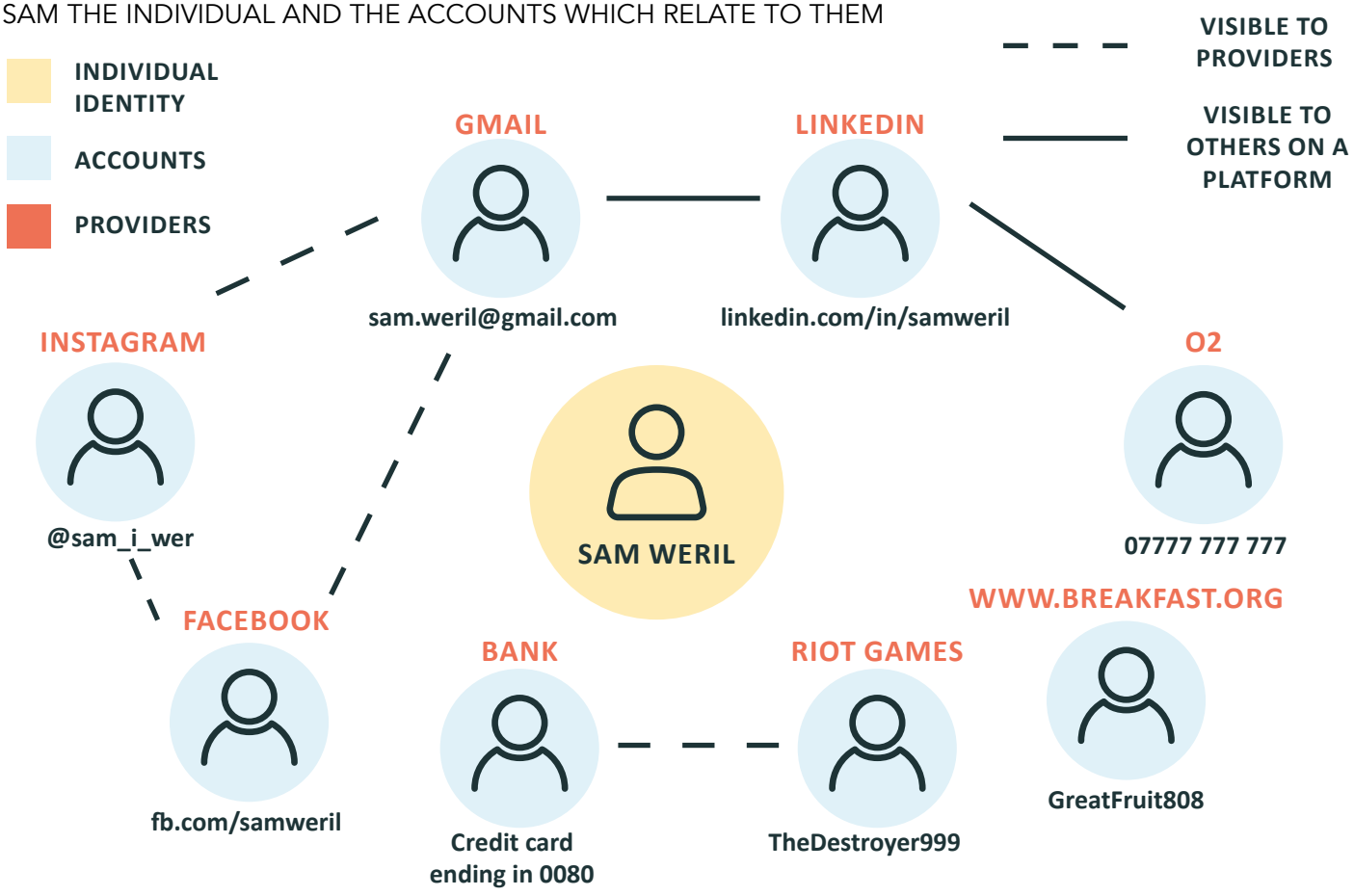
A HUMAN'S-EYE VIEW

In this section, we outline a framework for understanding anonymity. To do this, we examine the identity of Sam Weril, an invented person with a modest online presence. On top of the trappings of offline identity, e.g. a phone number, a credit card and so on, Sam has online accounts with Facebook, Gmail, LinkedIn and Instagram. They also contribute to www.breakfast.org, a niche online forum, play games under the pseudonym 'TheDestroyer999', and occasionally reply to threads posted on 4chan.org.[35]

Figure 1 maps out this online presence. Sam as an 'individual', a natural person who takes up physical space, sits in the centre. Around the edge of the graph sit the personae and addresses related to this

FIGURE 01.

SAM THE INDIVIDUAL AND THE ACCOUNTS WHICH RELATE TO THEM



35 Efforts have been made here to choose a name which does not belong to a living person. Similarly (and sadly) breakfast.org does not exist at the time of writing.

individual, which belong to or refer to them in some important way. We call these Sam's 'accounts'.

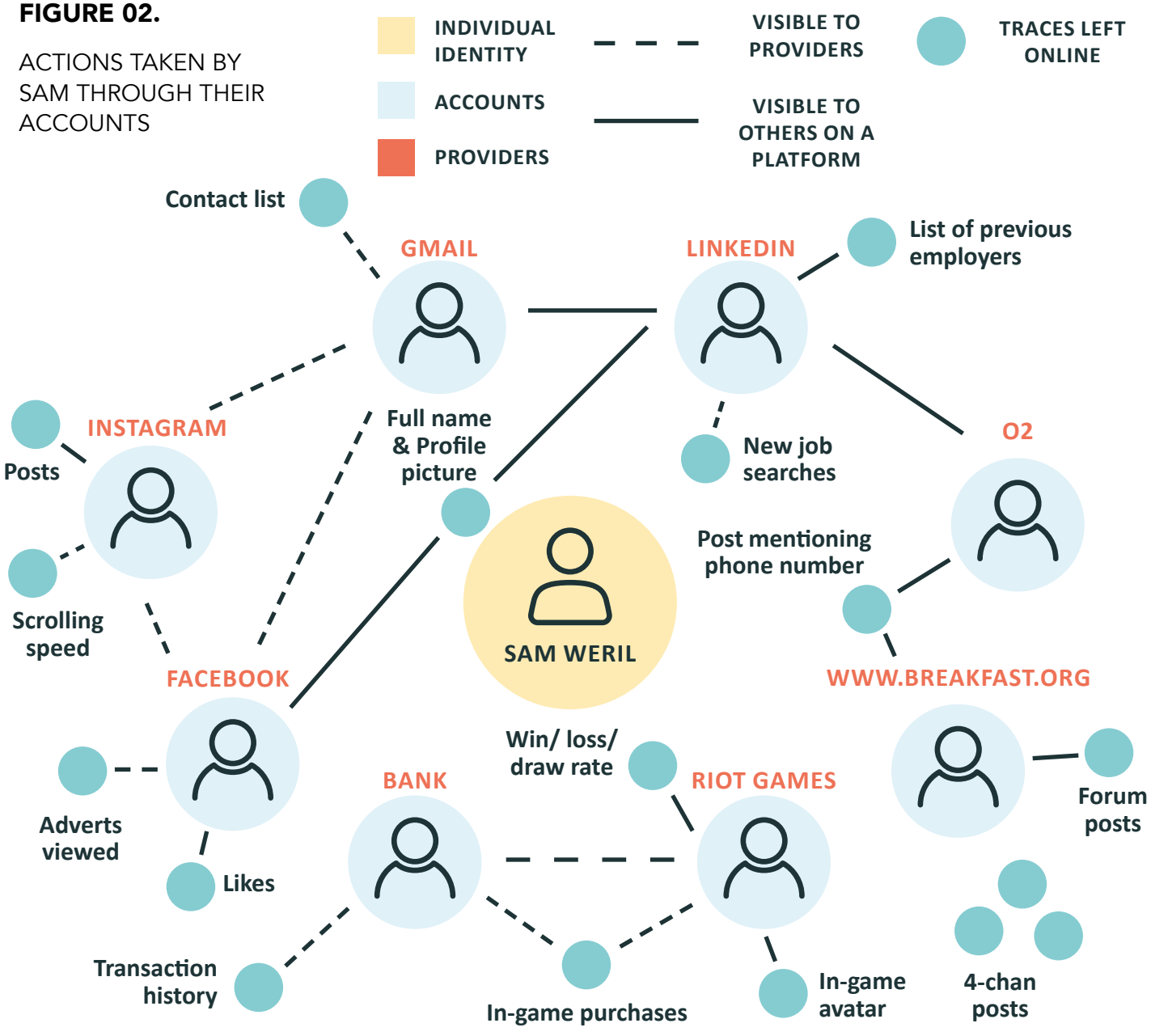
Some accounts are overtly connected to each other; Sam's LinkedIn profile, for example, publicly displays their phone number and email address. These links are visible to anyone else on the platform and are displayed as solid lines above. Other connections are typically invisible to the public but are known to the companies and organisations who provide the services which Sam is using. For example, Sam created their Instagram account by signing in through Facebook, and pays their gaming subscription with their credit card. These links are (ostensibly) visible only to the parties involved in those transactions, and are included as dotted lines.

To complete this graph, Figure 2 adds some of the traces Sam leaves as they use these accounts to interact with online space. These include intentional actions, visible to various groups on a platform; emails sent to friends, pages 'liked' on Facebook and chat messages sent in-game. They also include a sample of the behavioural traces recorded by providers and other third parties as a result of an account's presence in a space: the time a website was accessed, adverts clicked or lingered on, search history. We display a small selection of these below.

Some of this behaviour creates connections to other parts of the graph. In this case, a long-forgotten forum post contains Sam's phone number, and Sam uses the same professional headshot, alongside their full name, on Facebook and LinkedIn. These

FIGURE 02.

ACTIONS TAKEN BY SAM THROUGH THEIR ACCOUNTS



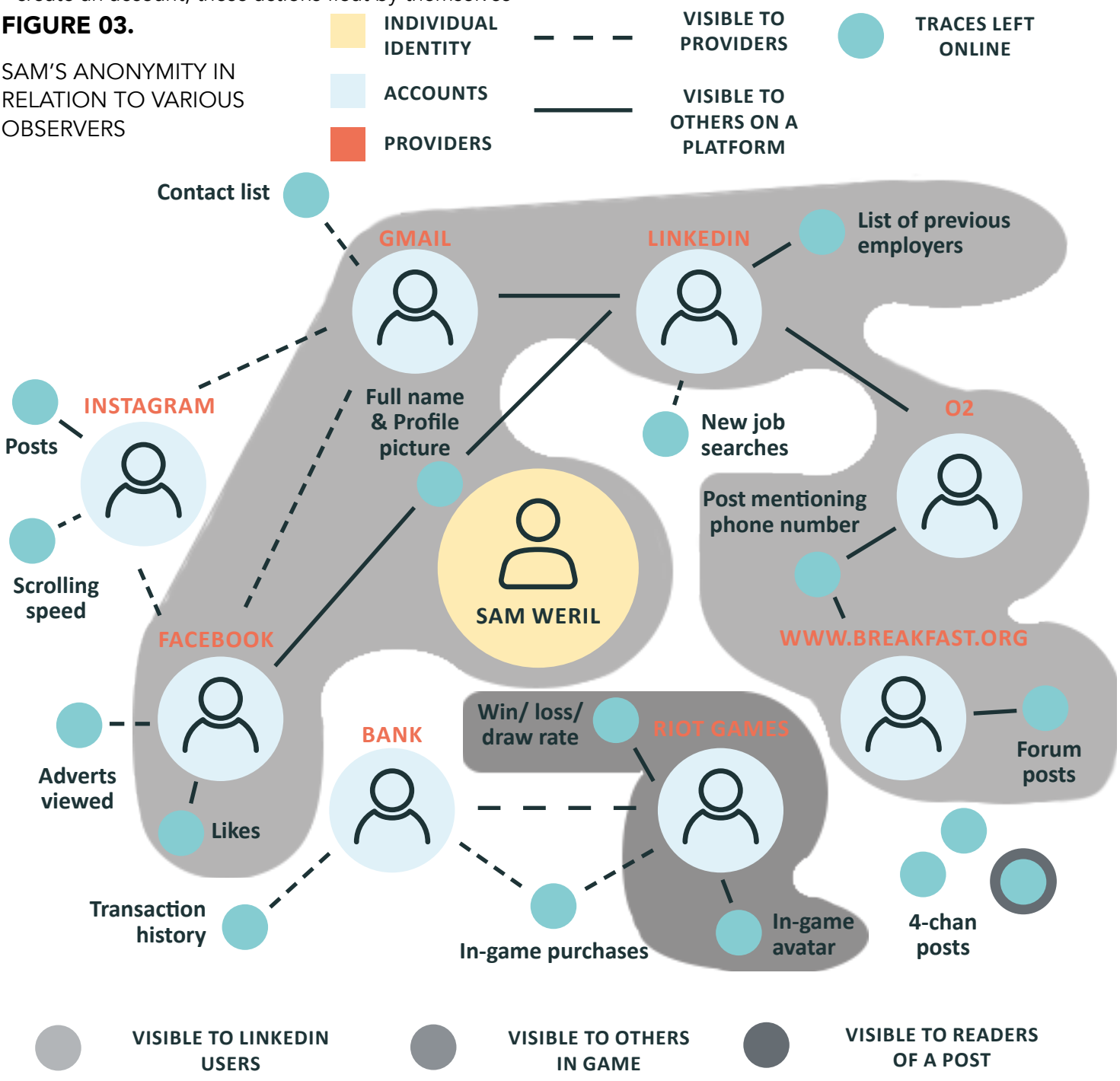
connections will be of different strengths, based on how many possible people could fit that description; the size of the anonymity set, in Köhntopp's terminology. In the case of a name, this set will be everyone online who uses the same name in their accounts; this could be a fairly weak connection.[36] For a phone number, the set will usually contain a single individual, and be a strong connection.

On platforms which do not require participants to create an account, these actions float by themselves in the void. As Sam has no 4Chan account, their posts on that platform are not shown connected to anything else on the graph. They are not even connected to each other.[37]

In order to talk about the anonymity of an individual's actions, we now introduce an observer, to whom some part of the graph in Figure 2 may be visible. Figure 3, below, maps out Sam's anonymity with respect to three possible observers.

FIGURE 03.

SAM'S ANONYMITY IN RELATION TO VARIOUS OBSERVERS



36 Though not for 'Sam Weril', which as far as we can tell has never been used online by anyone.

37 It is of course possible that 4Chan, or another third party, is able to connect these posts through use of e.g. the IP address through which they were sent; we will explore use of these identifiers below. Since these connections are invisible to the majority of other users in this space, however, we have for illustrative purposes left them out of these figures.

In light grey above, a connection of Sam's on LinkedIn who is considering them for a position is viewing Sam's professional page. Clearly, the public activity visible on Sam's profile, for example, their employment history, is visible to this observer. Through links in Sam's profile, she can also connect actions belonging to Sam's LinkedIn account to their phone number and email address, though the activities taken by these accounts remain unknown. A quick web search for each of these pieces of information turns up the public part of Sam's Facebook page, along with a years-old post made on breakfast.org about the merits of fruit in pancakes.[38] This connects the potential employer to their profile on the forum and their full posting history there. Finally, as Sam's LinkedIn profile contains a real name and photo, there is a sense in which this observer can also connect Sam's actions on the platform to them as an individual.

Other parts of their online graph, however, remain anonymous to this observer; if she were to come across an Instagram post left by @sam_i_werl, she will not necessarily be able to connect this activity to the 'Sam Weril' she knows from LinkedIn. Despite this, Sam's employment history, as well as the visible actions they have taken on connected platforms, intuitively have a very low level of anonymity to this observer.

Observers on other platforms will be able to see different parts of this graph. Those playing alongside Sam's gaming account can see a range of behaviours attached to that account, including the avatars or outfit Sam chooses for their characters in-game, as well as their win/draw/loss rates; but without being able to connect this activity to other aspects of Sam's identity. Those reading their comments on 4Chan will only see the name 'Anonymous' attached to a post without a linked account. Sam's behaviour in-game and on 4Chan, respectively, are intuitively more anonymous to their peers than their actions on LinkedIn.

At this point, we can restate our definition of anonymity with regards to Sam:

Sam Weril is anonymous to an observer to the extent that that observer cannot connect Sam's behaviour to them as an individual, or to their accounts.

IMPLICATIONS OF THE HUMAN'S EYE VIEW

This definition brings to light a few important features of anonymity:

The extent to which anonymity is breached with each new connection is affected by the role which accounts play in an individual's identity

Our homogenous 'account' icons above disguise the diversity of online platforms, each of which allows and encourages its users to behave in a different way. This is informed by the audience in each space, but also by the control afforded to users as to the amount of information their account displays alongside their actions; whether a profile picture is attached, for example, or pseudonym is permitted. Accounts whose actions can be sufficiently disconnected from the rest of an individual's online presence provide the opportunity for individuals to explore new facets of their identity.

Online space may particularly encourage the creation and performance of identity. As Merchant (2006) points out, when compared to face-to-face conversation, online communication takes place in a medium 'stripped of the paralinguistic features of gesture and eye contact.' As a result, he suggests, we work a lot harder to define and produce ourselves in these 'lean' online spaces.[39]

Our various audiences online, and the means of communication available to us on a given platform, affect the identities we choose to perform. Maintaining various accounts online lets people curate multiple identities, potentially straddling multiple platforms. In Sam's case, the persona they inhabit as 'GreatFruit808', a foul-mouthed citrus obsessive, is in an important sense separate from the sober and professional persona visible on LinkedIn.

This suggests that the act of anonymisation extends beyond the individual. A connection which can be made between two of Sam's online accounts might constitute an equivalent act of naming, even if those accounts are not overtly connected to an individual; the disclosure that 'GreatFruit808' is 'TheDestroyer999' may be as damaging to Sam as the disclosure that either account belongs to 'Sam Weril.' This seems particularly true if those accounts are used to perform distinct parts of Sam's identity.

The ability of an individual to keep actions anonymous between accounts is threatened by common points of access, and data collected by third parties.

In our example above, there are likely to be aspects of Sam's internet use which connect the vast majority of their actions. They might access all of their

38 We exert editorial privilege here to state that this post was packed with unusual expletives.

39 Guy Merchant, 'Identity, Social Networks and Online Communication':, E-Learning and Digital Media, 2016 <https://doi.org/10.2304/elea.2006.3.2.235>.

accounts through the same web browser, connect via a fixed IP address, or use a single device. Each of these would add another 'account' to our graph above, and an observer able to monitor it would be connected to the whole of Sam's activity.

A number of third parties have developed resilient methods to allow them to make, and profit from, precisely this type of connection. They employ techniques such as the use of third-party cookies which follow users across websites, and fingerprinting techniques which use unique combinations of features such as screen resolution, installed applications and fonts to restrict the size of a user's anonymity set to one known individual.[40] On our definition, meaningful anonymity from these observers becomes impossible while using an account monitored in this way.

The ability to make these kinds of connections has encouraged a new business model, termed 'surveillance capitalism' by Shoshana Zuboff. Under this model, private companies amass detailed collections of data on an individual and then use this data to predict future behaviour, capitalising both through selling these predictions on to third parties and, she argues, by influencing future behaviour.[41] Importantly, the data which proves most revealing, and thus most valuable to these actors, is not necessarily the data which we think of as behaviour which demands the protection of anonymity: our photos, blog posts and conversations. Rather, it is the myriad time stamps, taps, clicks and machine attributes recorded by companies every time we use a device; data which Zuboff terms 'behavioural surplus'.

Many of the companies who rely on this model for their income are crucial to the functioning of the western internet today, and as an example, we explore the impact of their choices concerning identity in a detailed examination of Facebook's approach to anonymisation below.

The importance of these companies to the modern online ecosystem run the danger of making the view of anonymity expressed above, as well as in privacy regulation, seem rather naïve. Behavioural profiles, historically the domain of states and security services, are now being compiled and offered commercially. Without a change to this business model, exerting full control over our identities online, control which is meant to be enshrined in the legal protections of the GDPR, seems difficult, if not impossible, to achieve.

Anonymity depends on the technical skill and tenacity of the observer

The question of which behaviours can be connected to various parts of an individual's graph of accounts will depend on how intent the observer is on discovering these links, and the toolkit of skills and data they are able to employ to this end. Above, we have assumed that our potential employer is sufficiently motivated to search for instances of Sam's name and number appearing elsewhere online, allowing them to connect the colourful behaviour of 'GreatFruit808' to Sam Weril, and removing the anonymity of their posts on the forum. To a less motivated observer or one which has decided to respect Sam's privacy and not to search for their details, more of Sam's activity online will be anonymous.

Levels of perceived and actual anonymity with respect to an observer may differ

Figures 1 to 3 paint a 'god's eye' view of activity online. In fact, connections which exist between accounts may not be known to individuals. As Sam has forgotten about the forum post containing their phone number, they would be surprised to find that their LinkedIn followers were able to connect their professional profile and forum activity.

This gap between perceived and actual anonymity will be increased where observers use tracking methods which people are likely to be unaware of, or might not expect to be possible, e.g. device fingerprinting. These methods include the current and future use of technology to identify individuals from uploaded images, characteristic text patterns or the tone of their voice.

Such techniques are already in use. Companies such as ClearviewAI have developed facial recognition technology, provided to law enforcement in the US, which they claim is able to use a single photo of an individual to locate them in images across forums and social media platforms, and so identify their

40 'Device Fingerprinting: What It Is And How Does It Work? - Clearcode Blog', Clearcode | Custom AdTech and MarTech Development, 2016 <https://clearcode.cc/blog/device-fingerprinting/> [accessed 27 February 2020]. A broader look at the technologies used in advertising is included in Demos' 2018 paper with the Information Commissioner's Office: Jamie Bartlett, Josh Smith, and Rose Acton, 'The Future of Political Campaigning', Demos <https://demos.co.uk/project/the-future-of-political-campaigning/> [accessed 27 February 2020].

41 Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, First edition (New York: PublicAffairs, 2019). A useful summary of Zuboff's argument is available in John Naughton's review in the Observer: John Naughton, '"The Goal Is to Automate Us": Welcome to the Age of Surveillance Capitalism', The Guardian <https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook> [accessed 27 February 2020].

social media accounts.[42] Widespread use of such technology could allow for the deanonymisation at scale of content which could never previously have been linked in the absence of a skilled investigator: faces in the back of strangers' holiday snaps; dating profile photos posted under a fake name; leaked photos of victims in witness protection.

Conversely, an individual might think that certain observers know more about them than they do, perceiving more of their graph to be visible than is, in fact, the case. Either way, this gap between perceived and actual anonymity can be damaging. The false belief that one is anonymous to an observer can lead to inadvertent disclosure. The false belief that all action is universally visible promotes fatalism. Why try to control your identity when Google can already see everything?

The anonymity of behaviour, even anonymity provided by encryption, will change over time

One technology which has been integral to ensuring anonymity is encryption; the process of encoding a message or information in such a way that only authorised parties can access it. Encryption, and attendant technologies such as the Tor network, can be effective in preventing unauthorised parties from viewing the content of communications, but also in obscuring identifiers, such as IP addresses, which link an individual to an activity.[43] In the language of our graphs above, encrypting content can help ensure that even providers can't draw a line between an individual's identifiers, such as a web browser, and the dots of their behaviour.

The promise of encryption is that, even in the case that an attacker has recorded all of the data sent from your device, e.g. through your internet service provider, they will not be able to read your communications or know their destination. This security, however, essentially relies on the encryption used being sufficiently difficult to break by brute force; that is, through techniques roughly akin to trying every possible combination until the safe springs open. Advances in computing power are likely to speed up this process to the point that once strong encryption becomes ineffectual; indeed, emerging technologies such as quantum computing are expected to be particularly powerful in breaking certain forms of encryption.[44]

This is not to say that anonymity through encryption will be impossible in the future. Privacy technology is an arms race, and new methods for decoding data will continue to be combated with increasingly ingenious methods for protecting it. The problem is that these new advances will be useless in hiding from an observer who has already collected data sent using now-breakable forms of encryption. Individuals who depend on this technology to keep their activities anonymous may find that this data is only secure for so long.

42 Kashmir Hill, 'The Secretive Company That Might End Privacy as We Know It', The New York Times, 18 January 2020, section Technology <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html> [accessed 27 February 2020].
43 David Kaye, Encryption and Anonymity Follow-up Report, 13 July 2018 <http://digitallibrary.un.org/record/1638475> [accessed 27 February 2020].
44 Princeton University CITP, 'Implications of Quantum Computing for Encryption Policy', Carnegie Endowment for International Peace <https://carnegieendowment.org/2019/04/25/implications-of-quantum-computing-for-encryption-policy-pub-78985> [accessed 27 February 2020].

SECTION 4
ANONYMITY IN ACTION: CASE STUDIES

In the next section, we will examine current approaches to anonymity and identity verification, both in the private and public sector. To do so, we examine Facebook as the most widespread example of a Western private sector approach, and GOV.UK's Verify programme as a recent attempt to build a state-run identity verification scheme.

CASE STUDY 1: FACEBOOK

Social media platforms, forums, and similar sites allow individuals to explore their identities online. A few big tech companies also act as identity authenticators for a significant part of the Internet.

Facebook takes both these roles in the modern internet. As such, it provides a useful example of a commercial approach to online anonymity and identity.

Anonymity on the platform

From its origins as an index of Harvard students, Facebook has always required its users to use their official offline identities as their identity on the site. The company's vice president of public policy, Elliot Schrage, put the company's position succinctly in 2011:

> *"Facebook has always been based on a real-name culture. We fundamentally believe this leads to greater accountability and a safer and more trusted environment for people who use the service."*[45]

Today, Facebook's terms of service require that "the name on your profile should be the name that your friends call you in everyday life." This must also be a name that appears on some form of official identification; a birth certificate, passport, driving license or similar.[46] In 2015, Facebook did clarify the policy to allow those in special circumstances, such as victims of stalking or those who identify as LGBT, to use a different name after an approval process.[47] Still, the platform generally requires users to operate using their primary offline identity.

In practice, many users evade this policy. For example, it is not uncommon for those applying for jobs, especially straight out of university, to change their Facebook name to hide from employers.[48] Here, they become theoretically anonymous to potential employers, who may only have a name and a university to go on, whereas existing friends will still be able to easily identify their friend after a name change through photos or existing messaging conversations. Others, such as teachers or police officers, will change their names to separate their personal lives from their professional lives.[49]

Facebook's identity verification around the web

Facebook's linking of people's behaviour to their real names extends beyond their platform. The company offers a service called Facebook Login, whereby Facebook acts as a de facto identity authenticator, sharing data on behalf of Facebook users trying to access services run by other companies. Facebook

45 Somini Sengupta, 'Rushdie Runs Afoul of Web's Real-Name Police', The New York Times, 14 November 2011, section Technology <https://www.nytimes.com/2011/11/15/technology/hiding-or-using-your-name-online-and-who-decides.html> [accessed 27 February 2020].
46 Facebook, 'What Types of ID Does Facebook Accept? | Facebook Help Centre' <https://www.facebook.com/help/159096464162185> [accessed 27 February 2020].
47 Facebook, 'Community Support FYI: Improving the Names Process on Facebook', About Facebook, 2015 <https://about.fb.com/news/2015/12/community-support-fyi-improving-the-names-process-on-facebook/> [accessed 27 February 2020].
48 Stephanie Goldberg, 'Young Job-Seekers Hiding Their Facebook Pages - CNN.Com' <http://www.cnn.com/2010/TECH/03/29/facebook.job-seekers/index.html> [accessed 27 February 2020].
49 BBC, 'This Is Why Some People Change Their Facebook Names', BBC Newsbeat, 2015 <http://www.bbc.co.uk/newsbeat/article/35112297/this-is-why-some-people-change-their-facebook-names> [accessed 27 February 2020].

makes a point of their login service being able to offer authenticated details about an individual's 'Real Identity'.

In today's Facebook Login Service, users are explicitly told what data they are sharing with the third-party App, can opt-out of optional data sharing, and are able to revoke access to that data. However, very few services allow users to use Facebook login in a way that doesn't require users to share identifying information, such as their real names or profile pictures.

This need to share was not always taken for granted. In 2014, Facebook announced an alternative service called Anonymous Login, providing a method for logging into apps without sharing any personal information from Facebook. This service was intended to sit alongside the real-name Facebook login, with applications offering a choice between the two, allowing users to conveniently sign in without exposing detailed identifying data to non-Facebook Apps.[50]

Sixteen months after the initial announcement, in August 2015, Facebook confirmed that Anonymous Login was dead. The company cited a lack of interest from developers.[51] A possible reason for this, highlighted by some at the time, was that the anonymity only applied in one direction: Facebook still knew which apps their users were interacting with, but individual developers got no information about those accessing their app.

Facebook offering a trusted international identity verification service is not necessarily a bad thing. For example, Facebook login is used by many apps to help ensure users are real people and who they say they are.[52] This can protect users' safety by making it more difficult for scammers to pose as someone else or otherwise be catfished into meeting someone they weren't expecting to.[53]

Facebook providing this service also means that dating platforms can verify identity without revealing and requesting information about their users from national governments. This allows, for example, LGBT individuals in countries where they might otherwise face persecution from the national government, to use dating apps without the risk of being exposed to those governments.

However, there is an important question here of alignment of incentives. Users want convenient safety and privacy across a working system; developers are economically incentivised to want to know as much as they can about their users, allowing them to personalise and optimise services and so maximise their profits.

Sometimes these align, as above, where users want to be able to trust verified real-name identities. However, in situations where users want to remain anonymous, either from other users or from the services they are using, developers very rarely give them that option. While it is available on smaller services and in less savoury parts of the Internet, like 4Chan, this option is almost absent from the mainstream Internet.

Facebook as a data aggregator

The elephant in the room here is that, although you can be optimally anonymous to these other services, it is difficult to remain anonymous to Facebook.

You can limit knowledge about yourself to other users on Facebook by not sharing revealing content or uploading identifying information. You can limit knowledge about yourself to other services by denying them permissions when you use Facebook to access their services. But you cannot remain anonymous to Facebook itself, at least, not without significant effort.

Facebook, like other actors, tracks users' habits around the internet and across devices – phone, tablet, laptop – to know where they habitually go, shop, and what kind of websites they visit. It has partnerships with marketing companies and advertising providers which allow it to track activity on websites beyond Facebook itself, including some not accessed with Facebook's Login service.[54] This reach extends into people's pockets, too. While it's obvious that Facebook-owned apps collect data when you have them installed, other apps, even those not using Facebook Login, may still share the

50 Facebook, 'Introducing Anonymous Login and an Updated Facebook Login', About Facebook, 2014 <https://about.fb.com/news/2014/04/f8-introducing-anonymous-login-and-an-updated-facebook-login/> [accessed 27 February 2020].
51 Karissa Bell, 'Facebook Created a Tool to Hide Your Data from Apps But It Never Launched', Mashable <https://mashable.com/2018/03/19/what-happened-to-facebook-anonymous-login/> [accessed 27 February 2020].
52 'How Do I Create a Tinder Account?', Tinder <http://www.help.tinder.com/hc/en-us/articles/115003356706-How-do-I-create-a-Tinder-account-> [accessed 27 February 2020].
53 Although many dating services, including Tinder, Bumble and Hinge have moved towards providing their own verification services as image recognition technology has become more accessible and more of their core demographic doesn't necessarily use Facebook.
54 'All the Ways Facebook Tracks You—and How to Limit It | WIRED' <https://www.wired.com/story/ways-facebook-tracks-you-limit-it/> [accessed 27 February 2020].

data they collect on you with the company.[55]

Facebook is just the tip of the iceberg in this regard. Google operates a similar system, and there are many other data aggregators and brokers for whom data aggregation and processing is integral to their business model, including credit rating agencies like Experian.[56]

All this allows Facebook to connect discrete activities or identities across the Internet, activities which may previously have remained highly anonymous, and at a scale open to few else but perhaps Google and the intelligence agencies of some governments.

As noted above, this activity is driven by an underlying economic logic. Companies are incentivised to collect as much data as they can on each and every user of the internet by a powerful advertising business model. Aggregated data is used to group people into a wide array of categories, to predict and influence their future behaviour, and sell all this to advertisers. Increasing the accuracy of these predictions pushes companies towards deanonymising their users to the fullest extent possible.

As a result, very few people can be truly anonymous to companies like Facebook and Google. The control of citizens' identities and ability to remain anonymous should they want to do so thus ultimately rest in the hands of private natural monopolies. These have limited incentives from competition and public opinion to serve the interests of society with respect to anonymity, be that in the service of the security of individuals or the health of public discourse.

CASE STUDY 2: VERIFY AND THE DIGITAL IDENTITY UNIT

Facebook's involvement in identity represents a departure from history; verification of identity, through passports, driving licences and often ID cards, has traditionally been the preserve of the state.

There are a number of reasons why states may want to verify an individual's identity or attributes about their identity. It allows for government administration, e.g. when verifying whether someone is a citizen when they register to take part in elections.[57] It may also be used to exclude migrants from accessing public services and to exclude the poorest in society who may not have the time or financial resources to go through the bureaucracy necessary to obtain identification.

Governments may also want to verify identity to apply the rule of law; for example, to ensure that age-restricted products such as alcohol or fireworks are only sold to those over the legal age; verification which currently poses greater difficulties in e-commerce than face to face transactions.

Online identity policy around the world

States around the world are grappling with different approaches to online anonymity. David Kaye, UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, has described digital anonymity as "indispensable to the exercise of privacy and freedom of expression" and stated that "restrictions on digital anonymity must also satisfy the requirements of legality, necessity and proportionality, and legitimacy". He is essentially arguing for anonymity by default.[58]

There is, however, little international consensus on this issue within the UN, as evidenced by a variety of approaches to the position of anonymity in law. For example, in South Korea, law enforcement can request online customer identity data without a warrant. In Russia, communications services have been forced to disclose the identity of users under government investigation. In China, Apple was compelled by the government to remove VPN services from it's App Store.[59]

Similar policies are being discussed in Europe. In April 2019, the Austrian government proposed a "Diligence and Responsibility on the Web" law, although after a general election later that year, it is unclear whether the law will still go ahead.[60] The law would require platforms with more than 100,000 registered users and annual revenue exceeding €500,000 (£444,000) to know the full name and address of their users. Users could still use public

55 Although perhaps the extent of the data they collect, including your location, might not be obvious. Privacy International, 'Guess What? Facebook Still Tracks You on Android Apps (Even If You Don't Have a Facebook Account)', Privacy International <http://privacyinternational.org/blog/2758/guess-what-facebook-still-tracks-you-android-apps-even-if-you-dont-have-facebook-account> [accessed 27 February 2020].

56 Experian, 'Marketing-Data-Practices-and-Policies' <http://www.experian.com/privacy/marketing-data-practices-and-policies.html> [accessed 27 February 2020].

57 Setting aside the question of whether only citizens should be able to vote.

58 David Kaye, Encryption and Anonymity Follow-up Report.

59 David Kaye, Encryption and Anonymity Follow-up Report.

60 Morgan Meaker, 'Austria's General Election Could Spell the End of Anonymity Online', Wired UK, 28 September 2019 <https://www.wired.co.uk/article/austria-online-anonymity-elections> [accessed 27 February 2020].

pseudonyms but platforms would be able to connect those pseudonyms with people's actual identities and would be required to hand over that information during a police investigation.

In Estonia, a well-known digital state, every citizen has a state-issued digital identity, originally through chipped ID cards in 2001, then special SIM cards, and now through a smartphone app.[61]

GOV.UK Verify and state identity authentication in Britain

The UK government has been working on the question of digital identity for at least the last decade, with mixed results. The Government Digital Service (GDS) first began developing an identity assurance strategy and framework in 2011, which would become GOV.UK Verify in 2016.[62]

Verify was intended to be the default way for citizens to prove their identity when using digital services, such as claiming tax back and receiving benefit payments.[63] It does not verify identities directly but contracts out identity verification services to five private sector identity providers.

Government schemes like Verify start with some advantages over private providers:

- They have a large innate user-base in the form of citizens who need to use public services. This can guarantee the ability to reach economies of scale and allow the developers to plan for scale rather than being concerned about acquiring their first customers.
- Governments already hold significant amounts of data on their citizens, and have the infrastructure in place for existing identification systems like passports which can be repurposed for digital identity systems.
- Governments have an in-built reputational advantage, in so far as they have provided traditional identification services, and are unlikely to disappear into the night with reams of personal information.

Government schemes also face some limitations not shared by private attempts:

The reach of governmental identity verification is limited to those who fall under its jurisdiction, e.g. to citizens of the United Kingdom, whereas a private company is not necessarily tied to a single country and can offer services across borders, to the stateless or those who do not trust their state.

Government-provided services also have a relative immunity from Schumpeter's gale of creative destruction.[64] Once a public service is established and citizens are relying on it, particularly vulnerable groups like the disabled, then the service cannot be allowed to fail, even if it is flawed.[65] These raised stakes mean that attempts at identity assurance by states can become locked into particular solutions and ways of working.

Many of the advantages of government provision could also apply to a well-established internet company, with a large user base, vast reserves of data, and strong track record in delivering other services. However, perhaps the key differentiator between public and private provision in a democracy is that democratic governments are expected to work in the public interest, rather than being driven by the profit motive. This means being more accountable than private companies, including in providing identity authentication services.

Problems encountered by GOV.UK Verify

The experience of Verify provides some salient lessons from which any central identity authenticator might learn, as spelt out in a report by the Commons Public Accounts Committee.

The first problem faced by Verify has been that of usability and so a subsequent lack of uptake. For example, Verify users could be 'locked out' if pre-existing data held on them by the service does not match their Verify details. This led to only 19 government services adopting Verify, fewer than half the number expected, and only 3,900,000 Verify users, less than one-sixth of the originally forecast 25,000,000 users by 2020. This has been blamed on GDS failing to develop a product that departments wanted to use, having failed to bring important stakeholders into the design process. The Cabinet Office has also recognised that the right incentives did not exist for departments to adopt Verify, largely because it was expensive for departments to implement.

61 'E-Identity', E-Estonia <https://e-estonia.com/solutions/e-identity/> [accessed 27 February 2020].
62 Committee of Public Accounts, Accessing Public Services through the Government's Verify Digital System (House of Commons, 1 May 2019) <https://publications.parliament.uk/pa/cm201719/cmselect/cmpubacc/1748/174802.htm> [accessed 27 February 2020].
63 National Audit Office, Investigation into Verify, 2019.
64 Joseph A. Schumpeter, Capitalism, Socialism, and Democracy, 1st ed (New York: Harper Perennial Modern Thought, 2008).
65 Stian Westlake, Laura Bunt, and Michael Harris, 'Schumpeter Comes to Whitehall', Nesta, 2010 <https://www.nesta.org.uk/report/schumpeter-comes-to-whitehall/> [accessed 27 February 2020].

There are also concerns about whether the government's investment in the service has been adequately protected. The Public Accounts Committee suggested the Cabinet Office and GDS had not safeguarded taxpayers' interests in securing Verify's intellectual property, including the Verify brand, its public portal and the infrastructure 'hub' that links Verify's users, private providers and government services. Further, they suggest that the Cabinet Office and GDS seem to have given little thought to the value of this intellectual property, and how taxpayers' investment in it would be recouped should private providers secure substantial profits from Verify in the future.

The Verify programme has also been criticised for not securing the future sustainability of the service. In October 2018, the Cabinet Office announced that government funding would stop in March 2020. After this time, GDS intends that the private sector will take over responsibility for Verify, including for investment to ensure its future delivery. However, the Public Accounts Committee highlighted that there are major uncertainties about how Verify will operate beyond that date and, as of mid-February 2020, that is still the case.[66]

None of these are insurmountable barriers to state provision of identity authentication, but they demonstrate how easily it can go wrong and provide important lessons for future public sector identity systems.

In the course of developing Verify, the Government Digital Service created and used open standards.[67] The government is 'betting' on a private sector market emerging that can provide services more cheaply than anything it could build or buy for itself. However, these standards also offer a foundation that future not-for-profit or public service identity providers could build on.

Post-Verify online identity policy in the UK

Verify has represented the bulk of the UK's approach to online anonymity over the past few years. However, it sits alongside another governmental approach to digital identity policy; that of the Digital Identity Unit.

In June 2019, the government announced a new Digital Identity Unit, a collaboration between the Department for Digital, Culture, Media and Sport (DCMS) and the Cabinet Office, aimed at bringing the public and private sector together to ensure the adoption of interoperable standards, specifications and schemes.[68] DCMS launched a consultation on digital identity with a call for evidence in July 2019, and the Digital Identity Unit (DIU) is to be tasked with delivering on the outcome of the consultation.[69]

The framing of this consultation suggests a privacy-centric model of identity sharing, focused on being able to provide authenticated proof of specific attributes (e.g. that the citizen is over 18) rather than sharing the underlying sensitive data (e.g. their full birth date). The DIU is thus aiming for the ability to have strong proofs of particular attributes alongside pseudoanonymity in the same context, e.g. when accessing age-restricted products such as pornography.

The DIU is also committed to a digital identity system that avoids identity cards, though this may be for political rather than practical reasons. When the government last tried to introduce identity cards in the early 2000s, it faced widespread negative media coverage and a concerted NO2ID campaign against the cards, both of which may re-emerge if a similar scheme were introduced today.[70]

It also identifies trust as the key to a successful approach to digital identity. In particular, trust between the person or organisation aiming to prove something about themselves, and the person or organisation they are dealing with (the 'relying party'). In its mind, the essential criteria to achieve high levels of trust in digital identity provision include universal coverage (free to the public), standardisation, social inclusion, privacy, data protection, legality, security, proven liability models and consumer protection.

66 Bryan Glick, 'Want to Hear the Latest on Gov.Uk Verify? Sorry, GDS Still Has Nothing to Say - Computer Weekly Editor's Blog' <https://www.computerweekly.com/blog/Computer-Weekly-Editors-Blog/Want-to-hear-the-latest-on-Govuk-Verify-Sorry-GDS-still-has-nothing-to-say> [accessed 27 February 2020].

67 'Identity Proofing and Verification of an Individual', GOV.UK <https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual/identity-proofing-and-verification-of-an-individual> [accessed 27 February 2020].

68 'Minister Confirms Government Ambition on Digital Identity', GOV.UK <https://www.gov.uk/government/news/minister-confirms-government-ambition-on-digital-identity> [accessed 27 February 2020].

69 'Digital Identity', GOV.UK <https://www.gov.uk/government/consultations/digital-identity> [accessed 27 February 2020].

70 E. Pieri, 'ID Cards: A Snapshot of the Debate in the UK Press. Project Report.', 2009 <https://www.research.manchester.ac.uk/portal/en/publications/id-cards-a-snapshot-of-the-debate-in-the-uk-press-project-report(b00a2a09-025f-4962-b625-80e5991a3ed2).html> [accessed 27 February 2020]. 'Success Story: Dismantling UK's Biometric ID Database', Electronic Frontier Foundation, 2012 <https://www.eff.org/pages/success-story-dismantling-uk%E2%80%99s-biometric-id-database> [accessed 27 February 2020].

RECOMMENDATIONS

A series of recommendations for platforms, regulators and other stakeholders on how to positively design for anonymous action online.

IMMEDIATE ACTIONS

The British Government

Clarify the future of the Verify programme and plans for future sustainability beyond April 2020.

Regulators

The Information Commissioner's Office should clarify its stance on behavioural surplus and its relationship to personal data. Does, for example, mouse movements, keystrokes and writing style count as personal data if it is used to infer the identity of individuals?

Parliamentarians

Parliamentarians discussing anonymity must make it clear who the observer is. Rather than discussing anonymity in the abstract, politicians should make sure they raise and can answer the question: 'Anonymity from whom?'

Civil Society

When privacy focused organisations are championing online anonymity or when security focused organisations are decrying online anonymity, they should specify from whom they want individuals to be anonymous or identifiable to, in order to raise the quality of the debate. All organisations should examine whether their proposals on online anonymity meet the 'acid test' outlined below.

Users

While it is currently difficult for users to understand how their behaviour and identity can be connected, and who is able to make such connections, there are a few steps which can be taken to help get a handle on personal anonymity online. Firstly, users should be aware of how they can reduce online tracking, and have an idea of how much information about them is currently online - tools such as Tactical Tech's 'Digital Detox Kit' can help here.[71]

Secondly, users have a solid idea of their rights with regards to their personal data online. The most relevant legislation here remains the General Data Protection Regulation (or GDPR). While many guides to this are written with those who control and process data in mind, Which? has published a useful overview on how users can exercise their data rights, as well as clarifying some of the terms and concepts used in the GDPR.[72]

Finally, where people feel that their rights are being abused, or that they don't have control over their anonymity, they should act - for example by changing their privacy settings within platforms, or writing to platforms or their MP to protest.

Technology Companies

Actively inform users when their activity on your website or application is being linked to other online or offline activity and identities.

International Institutions

International institutions should ensure that human rights mechanisms such as the Universal Periodic Review are gathering information on and considering the ramifications for human rights (such as freedom

71 https://datadetoxkit.org/en/home

72 https://www.which.co.uk/consumer-rights/regulation/gdpr-data-protection-act. A more technical guide from the ICO can be found here: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/

of opinion and expression, and privacy) of member States' approaches to anonymity online. As technology further develops, they should continue to provide guidance to states on how to ensure their approach to anonymity complies with their obligations.

RECOMMENDATIONS ON FUNDAMENTAL RIGHTS AND THE FRAMING OF ANONYMITY

Any forthcoming British Bill of Rights should enshrine the right for individuals to remain anonymous online.

The Government should assert that control over anonymity is essential for the exercise of people's fundamental human rights, and any divergence from the ECHR or the Human Rights Act should include strong protection for anonymity on this basis.

Powers to remain anonymous should keep pace with powers to be deanonymised.

The government should commit to ensuring that, as the technical tools for connecting behaviour to individuals become more powerful, regulator power keeps pace to protect anonymity. In particular, individuals should have the right to effective deletion of new and existing categories of data which relate to them. For example, the Information Commissioner's Office should clarify whether the development of facial recognition and other advances in deanonymisation technology mean that you can reasonably request Facebook to remove (or obfuscate through blurring or replacement) images of your face in the background of other people's photos.

Parliamentarians, regulators and other public bodies discussing anonymity must make it clear who the observer is.

Rather than discussing anonymity in the abstract, officials and politicians should make sure they raise and can answer the question: 'Anonymity from whom?'

RECOMMENDATIONS ON ENFORCING AND PROTECTING THESE RIGHTS

The Privacy and Electronic Communications Regulations should be altered to mandate a default global opt-out to advertising cookies.

The Information Commissioner's Office should clarify its stance on behavioural surplus and its relationship to personal data.

For example, do mouse movements, keystrokes and writing style count as personal data if it is used to infer the identity of individuals?

Existing cookie laws should be expanded to compel platforms to clarify which connections between their behaviour on that platform and their other accounts.

To help people exert meaningful control over their data, people should be able to find out how it is being used to track and make decisions about them.

The development and adoption of applications which preserve the content side of anonymity should be encouraged.

One idea to prevent against unwanted unmasking online is to have phone cameras with a setting that automatically anonymises faces in the backgrounds of pictures, by simply blurring them. To be more secure, they could be overwritten with the generative-adversarial machine learning systems currently used to power deepfakes.

Alex Hern, UK technology editor for the Guardian, has posited an expansion of this idea.[73] He envisages a camera app which scrambles any identifiable features in a picture or video, replacing faces with those of people who do not exist, cars with those of a similar make and model, superfluous text with some form of Lorem Ipsum. With this, a new scene is created, one that conceals the identities of those in it but still maps onto the same meaning, captures the same idea, as the original.

A PUBLIC SERVICE IDENTITY AUTHENTICATOR

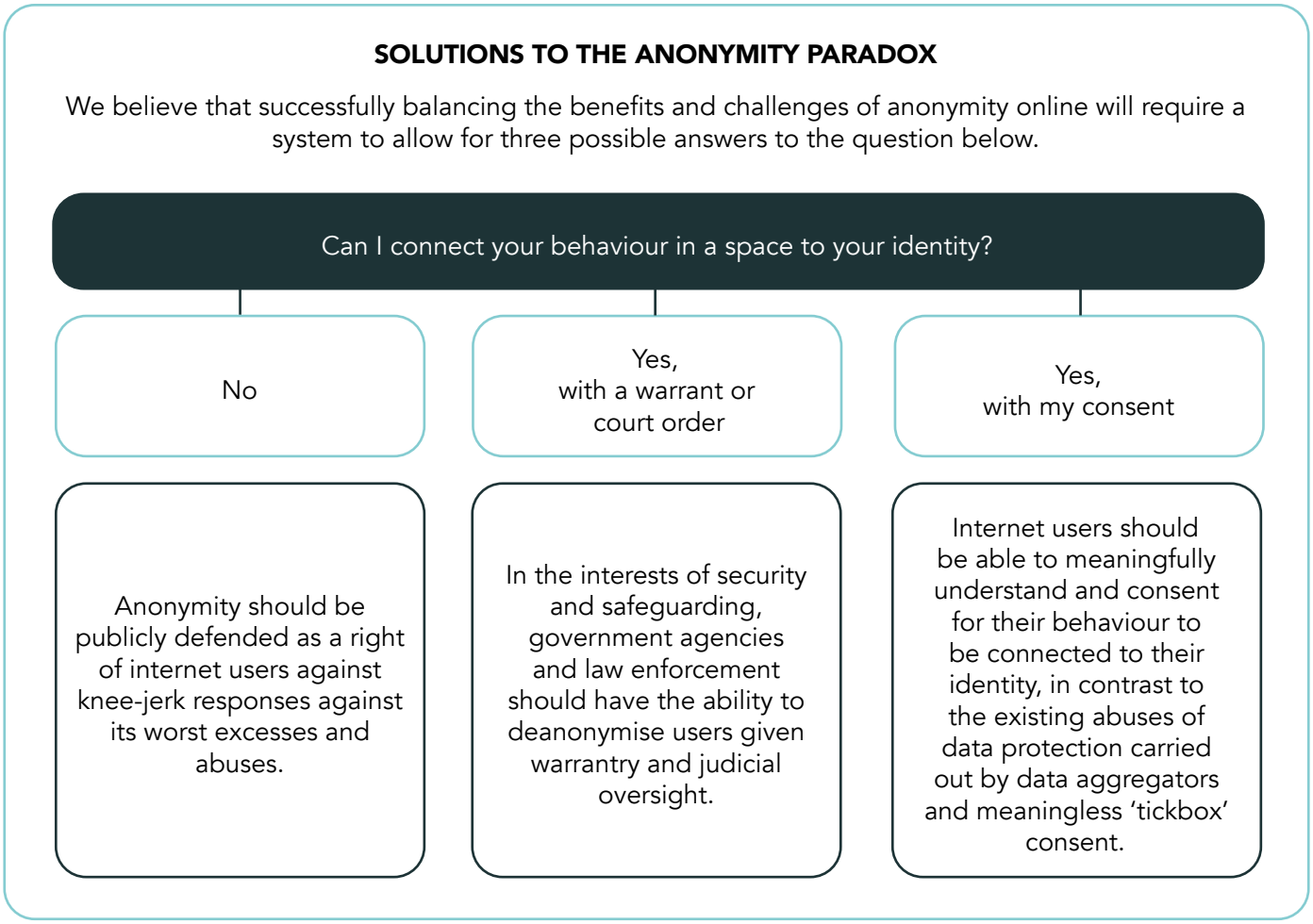
Based on this understanding of anonymity and its position in liberal democracies, we believe there are three tests that a future settlement on anonymity ought to pass.

We believe the default answer for most observers of internet users to the question 'Can I connect your behaviour in a space to your identity?' should remain 'no'. Controversy over the excesses and abuses perpetrated by some internet users under the shadow of anonymity or pseudoanonymity should not blind us to how important the ability to be anonymous is in a liberal democracy. We must ensure that where speech or behaviour is legal and protected, it is not restricted in a simplistic and myopic response to an online harm. Our hope for this paper is that policymakers will understand how Britain's defence of civil and human rights online is a powerful tool in diplomacy and influence; we should

73 Alex Hern, 'Vcs i Will Sell You This Idea for £5bn' <https://alexhern.substack.com/p/vcs-i-will-sell-you-this-idea-for> [accessed 10 March 2020].

FIGURE 04.

A TEST FOR SETTLEMENTS
ON ONLINE ANONYMITY



be setting a high liberal standard for online spaces going forward.

Nevertheless, there are exceptions that must be able to be enforced. In liberal democracies, we sacrifice a number of our 'freedoms to' in order to preserve our 'freedoms from'. As such, we expect our legal structures and security services to keep us safe from harm, for them to be able to operate effectively, and to exercise the powers entrusted in them as part of their mandate. Where protections to anonymity prevent this happening, the system sits poorly within a liberal democracy, and a future settlement must ensure that the safety and security apparatus is able to operate.

Finally, we believe a system must allow for meaningful consent as part of the deanonymisation process. Deanonymisation is, of course, a useful and natural function of social spaces - we are willing to share our identities with other people or institutions in exchange for goods and services or as part of a deepening social relationship. The status quo makes a mockery of this: users are unable to meaningfully offer consent to their data being used and their identities being tied together by thousands of companies and websites, leading to so-called 'tickbox consent' where, in order to access a site or service, users are forced to accept a dizzying array of unintelligible terms and conditions, including around the use of their data and their deanonymisation by a range of actors. Going forward, we expect users to be able to clearly and cleanly understand the extent to which a site or service is looking to deanonymize them.

THE VISION

So how do we pass this test? Is there a system of identity verification which gives society all three of these options? Which balances the dilemma of accountability versus openness?

We think there is. We propose the British Identity Corporation (BIDC), a public service identity

authenticator as an answer to the acid test. A version of the future which learns from the lessons of Facebook and Verify, and seeks to offer a new way forward.

First things first. This is an idea. This is a vision of what something better could look like. We are not claiming to have all the answers, or that this is the only solution. There are complications and complexities and plenty of failure modes. If it were easy to solve the question of online identity, someone would have done it by now.

But this proposal we think meets the tests set out above, and the core of it represents something that will be fundamental to building a better internet.

We imagine the BIDC as ultimately an independent and non-for-profit body, though one with significant state backing and guarantees. Something like the BBC might offer inspiration: a public service identity authenticator with a Royal Charter which guaranteed legal firewalling of its data from the rest of the public sector (unless explicit permission is given by users) and legal protections from interference.

It would also have an independent board. This board would be made up of a broad selection of stakeholders including but not limited to:

- Government representatives
- Representatives of internet platforms
- Representatives of the third-sector and large membership organisations
- Academics
- Members of the British Identity Corporation staff
- Directly-elected citizen representatives.

This platform would work by offerring an alternative to state or commercial online identity verification. Rather than entering their personal details into each online platform, users would instead authenticate once to the BIDC, which would in turn provide platforms with the minimal information they need to identify or validate that user. In the example of a platform requiring age verfication, BIDC would send a message stating that the user was over 18, rather than sharing their birth date and proof of age. For platforms which simply need to know that this user is the same person who logged in last week, BIDC could provide an ID number; potentially a different ID number for each platform.

This centralised system would also allow users to see which requests which have been made for each part of their personal data, by which actors, at which time.It would also enable them to deny future access to that data.

Through making this transparent and auditable, we hope that it would enable users to have meaningful control over their identity online. Law enforcement could apply for a warrant to compel this body to hand over identifying data in the case of investigation of illegal activity.

Possible Approaches

There seems to be broadly two approaches to a system like the one we propose, competition or monopoly. Essentially whether this new independent organisation should be an alternative system, albeit one likely legally empowered to allow it to compete, versus a universal replacement for existing arrangements:

- A state-granted monopoly on identity provision, i.e. all companies and public services must use service to verify identity attributes
- Adversarial interoperable competition with current identity providers

Funding Models

Any sustainable identity system will need to consider sources of funding, both short-term and long-term, at the outset. The funding models below are not mutually exclusive and it is likely that different models may be appropriate at different stages in the project's lifecycle, and depending on the scope and scale it comes to encompass:

- United Nations funding
- State funding
- Subscription model, which might include means-tested subsidies for low-income users
- Levy on companies utlising the service
- Endowment funded, with private, public or third-sector investment in the endowment.

Challenges

This proposal is by no means a panacea. It must learn from the mistakes of governmental attempts like Verify and the problems with surveillance capitalism. There are a number of challenges we believe this kind of system is likely to face, which broadly fall into issues of:

1. Access
2. Oversight

3. Implementation
4. Trust

Access

How do we ensure access?

No matter what funding model is chosen, there needs to be a consideration of access and equality.

Although platforms would not have to use a high level of verification that would require a comprehensive identity system, if they were a) able to without any extra resourcing needed on their part, due to their reliance on the identity system, and b) incentivised to by increased governmental scrutiny of e.g. age verification of users, we could see 'verification creep' whereby platforms put up higher and higher barriers to entry as they require more details verified.

If, therefore, people were required to have provided comprehensive proof of their identity to access an online service, this would disproportionately affect marginalised and vulnerable groups, and would risk severe inequalities in access to online services. Groups who might be particularly at risk of being unable to access and use official documentation could include: undocumented migrants; people who are homeless; people on low incomes; people in abusive relationships whose documents might be controlled by another person; and children who are reliant on their parents to obtain official documentation for them.

Any such ID provider would thus have to consider a range of methods of identity verification which did not rely on costly or government-issued identification (such as email, phone, or photo identification); and any online regulator would need to make it clear to companies that they expected verification barriers to tend towards the minimum rather than the maximum.

Moreover, we posit the ideal that all personal data shared by an individual with the independent body would be secure and not shared with the government. However, even if that were in fact the case, there would be very real and reasonable concern that it would not be, that could deter people from sharing their details, and hence affect equality of access.

Implementation

How do we build a resilient, people-centred system which protects individuals data while minimising the burden it places on users?

There will also no doubt be all manner of technical and design challenges. One is a simple question of useability; does the system match the needs of users and platforms, for example:

- Is it easy for users to verify their identity in an uncumbersome manner?
- Is it easy to access and control the data held about them?
- Is there an accessible API that platforms can use to intuitively plug the system into their website or application?

Much of this will be a task of conducting and implementing user experience and user design research at the outset of the project, but the impact of poor implementation can be underestimated.

Another implementation concern will be cyber-security. Users will be rightly concerned about the security of the sensitive data an identity provider will necessarily need to hold in order to perform its functions. Perhaps the biggest challenge here will be acquiring highly skilled technical staff, as cybersecurity skills are already in high demand in the private sector. Even with a clear sense of public purpose and social benefit, the identity provider may struggle to compete unless it can provide competitive salaries, which ties into the questions of costs and funding.

There is also the question of how the identity provider would handle user data. Would the provider use a single central database which would create a single point of failure? Or a decentralised system that might cause coordination issues and difficulties for legitimately linking data when necessary by law enforcement?

Then we have to decide where the provider gets their server space. The most obvious choice would be cloud platforms such as those offered by Amazon, Microsoft, Google and others. This would outsource some of the questions around ability to scale and protection from outside threats, as these companies are well-versed in large-scale data storage.

However, this runs the risk of putting personal data back into the hands of the private companies this system is intended to circumvent and who have strong incentives to use that data to further their own business mode.

Oversight

How do we keep this system accountable to the citizens it is meant to serve?

These issues are both tied closely together with the

problems of access and trust. No identity verification system can be successful without appropriate oversight that ensures the data is used only to facilitate identity verification, and not shared with governments or corporations outside of the bounds of a legal warrant.

In the UK, there has been widespread criticism of the 'hostile environment' policy which has seen data shared between schools, healthcare providers and the Home Office for immigration purposes, which naturally prevents some people from being able to access these essential services safely.[74] This sharing has since been curtailed. However, any successful third party identity verification body would need to include robust guarantees, endorsed by civil rights groups, that there would be no automatic data-sharing, or data shared except in specific circumstances.

In other country contexts, the risks could be much higher. For instance, consider countries where human rights and the rule of law are not protected and there are insufficient safeguards around personal data. In those countries, the government could compel such a body to hand over identifying data to facilitate government persecution of individuals or groups. This data could then potentially be shared internationally.

There would likely be a need for supranational oversight of how warrants were being exercised by governments to access this information, whether at the European Union and African Union level or at a United Nations level.

Trust

How do we build and retain trust in a new and sensitive system?

Even if issues around access, implementation and oversight are solved, if potential users do not trust the identity system, they may not believe that those prior solutions have actually been implemented or are effective. A system with low trust is likely to see low take-up by intended users and the possibility that users will try to work around the system rather than embracing it.

Individuals already sceptical of the intentions of private providers and/or the state holding their data may choose not to share information with the service if they believe their data will be shared with companies or government departments without their consent.

One possible idea is to leverage existing highly trusted organisations. In the UK, this could mean government institutions like the National Health Service. Another potential option would be getting buy-in from large membership organisations. For example, according to YouGov opinion data, the British public has a 72% net positive opinion of the National Trust, versus a 28% net positive opinion of Facebook.[75] [76]

However, if the system fails, for example through a data breach, and public trust in the identity provider rightly falls, it risks harming trust in those other organisations.

Conclusion

These challenges are substantial and we are sure there are more that we have not considered here. We are open to hearing those and alternative proposals which meet our tests. However, the current situation is untenable and we need to do things differently, if not this way, then some way.

We hope that this proposal, and the report as a whole, provokes a better debate about how we conceptualise online anonymity and confront the dilemma it poses.

74 Liberty, 'Challenge Hostile Environment Data Sharing', <https://www.libertyhumanrights.org.uk/challenge-hostile-environment-data-sharing> [accessed 10 March 2020].
75 YouGov, 'National Trust Popularity & Fame' <https://yougov.co.uk/topics/politics/explore/not-for-profit/National_Trust> [accessed 10 March 2020].
76 YouGov, 'Facebook Popularity & Fame' <https://yougov.co.uk/topics/technology/explore/social_network/Facebook> [accessed 10 March 2020].

Licence to publish

Demos – License to Publish
The work (as defined below) is provided under the terms of this licence ('licence'). The work is protected by copyright and/or other applicable law. Any use of the work other than as authorized under this licence is prohibited. By exercising any rights to the work provided here, you accept and agree to be bound by the terms of this licence. Demos grants you the rights contained here in consideration of your acceptance of such terms and conditions.

1 Definitions
a 'Collective Work' means a work, such as a periodical issue, anthology or encyclopedia, in which the Work in its entirety in unmodified form, along with a number of other contributions, constituting separate and independent works in themselves, are assembled into a collective whole. A work that constitutes a Collective Work will not be considered a Derivative Work (as defined below) for the purposes of this License.
b 'Derivative Work' means a work based upon the Work or upon the Work and other pre-existing works, such as a musical arrangement, dramatization, fictionalization, motion picture version, sound recording, art reproduction, abridgment, condensation, or any other form in which the Work may be recast, transformed, or adapted, except that a work that constitutes a Collective Work or a translation from English into another language will not be considered a Derivative Work for the purpose of this License.
c 'Licensor' means the individual or entity that offers the Work under the terms of this License.
d 'Original Author' means the individual or entity who created the Work.
e 'Work' means the copyrightable work of authorship offered under the terms of this License.
f 'You' means an individual or entity exercising rights under this License who has not previously violated the terms of this License with respect to the Work, or who has received express permission from Demos to exercise rights under this License despite a previous violation.

2 Fair Use Rights
Nothing in this licence is intended to reduce, limit, or restrict any rights arising from fair use, first sale or other limitations on the exclusive rights of the copyright owner under copyright law or other applicable laws.

3 License Grant
Subject to the terms and conditions of this License, Licensor hereby grants You a worldwide, royalty-free, non-exclusive, perpetual (for the duration of the applicable copyright) licence to exercise the rights in the Work as stated below:
a to reproduce the Work, to incorporate the Work into one or more Collective Works, and to reproduce the Work as incorporated in the Collective Works;
b to distribute copies or phono-records of, display publicly, perform publicly, and perform publicly by means of a digital audio transmission the Work including as incorporated in Collective Works; The above rights may be exercised in all media and formats whether now known or hereafter devised. The above rights include the right to make such modifications as are technically necessary to exercise the rights in other media and formats. All rights not expressly granted by Licensor are hereby reserved.

4 Restrictions
The licence granted in Section 3 above is expressly made subject to and limited by the following restrictions:
a You may distribute, publicly display, publicly perform, or publicly digitally perform the Work only under the terms of this License, and You must include a copy of, or the Uniform Resource Identifier for, this License with every copy or phono-record of the Work You distribute, publicly display, publicly perform, or publicly digitally perform. You may not offer or impose any terms on the Work that alter or restrict the terms of this License or the recipients' exercise of the rights granted hereunder. You may not sublicence the Work. You must keep intact all notices that refer to this License and to the disclaimer of warranties. You may not distribute, publicly display, publicly perform, or publicly digitally perform the Work with any technological measures that control access or use of the Work in a manner inconsistent with the terms of this License Agreement. The above applies to the Work as incorporated in a Collective Work, but this does not require the Collective Work apart from the Work itself to be made subject to the terms of this License. If You create a Collective Work, upon notice from any Licensor You must, to the extent practicable, remove from the Collective Work any reference to such Licensor or the Original Author, as requested.

b You may not exercise any of the rights granted to You in Section 3 above in any manner that is primarily intended for or directed toward commercial advantage or private monetary compensation. The exchange of the Work for other copyrighted works by means of digital file sharing or otherwise shall not be considered to be intended for or directed toward commercial advantage or private monetary compensation, provided there is no payment of any monetary compensation in connection with the exchange of copyrighted works.
c If you distribute, publicly display, publicly perform, or publicly digitally perform the Work or any Collective Works, you must keep intact all copyright notices for the Work and give the Original Author credit reasonable to the medium or means You are utilizing by conveying the name (or pseudonym if applicable) of the Original Author if supplied; the title of the Work if supplied. Such credit may be implemented in any reasonable manner; provided, however, that in the case of a Collective Work, at a minimum such credit will appear where any other comparable authorship credit appears and in a manner at least as prominent as such other comparable authorship credit.

5 Representations, Warranties and Disclaimer
a By offering the Work for public release under this License, Licensor represents and warrants that, to the best of Licensor's knowledge after reasonable inquiry:
i Licensor has secured all rights in the Work necessary to grant the licence rights hereunder
and to permit the lawful exercise of the rights granted hereunder without You having any obligation to pay any royalties, compulsory licence fees, residuals or any other payments;
ii The Work does not infringe the copyright, trademark, publicity rights, common law rights or any other right of any third party or constitute defamation, invasion of privacy or other tortious injury to any third party.
b Except as expressly stated in this licence or otherwise agreed in writing or required by applicable law, the work is licenced on an 'as is' basis, without warranties of any kind, either express or implied including, without limitation, any warranties regarding the contents or accuracy of the work.

6 Limitation on Liability
Except to the extent required by applicable law, and except for damages arising from liability to a third party resulting from breach of the warranties in section 5, in no event will licensor be liable to you on any legal theory for any special, incidental, consequential, punitive or exemplary damages arising out of this licence or the use of the work, even if licensor has been advised of the possibility of such damages.

7 Termination
a This License and the rights granted hereunder will terminate automatically upon any breach by You of the terms of this License. Individuals or entities who have received Collective Works from You under this License, however, will not have their licences terminated provided such individuals or entities remain in full compliance with those licences. Sections 1, 2, 5, 6, 7, and 8 will survive any termination of this License.
b Subject to the above terms and conditions, the licence granted here is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, Licensor reserves the right to release the Work under different licence terms or to stop distributing the Work at any time; provided, however that any such election will not serve to withdraw this License (or any other licence that has been, or is required to be, granted under the terms of this License), and this License will continue in full force and effect unless terminated as stated above.

8 Miscellaneous
a Each time You distribute or publicly digitally perform the Work or a Collective Work, Demos offers to the recipient a licence to the Work on the same terms and conditions as the licence granted to You under this License.
b If any provision of this License is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this License, and without further action by the parties to this agreement, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.
c No term or provision of this License shall be deemed waived and no breach consented to unless such waiver or consent shall be in writing and signed by the party to be charged with such waiver or consent.
d This License constitutes the entire agreement between the parties with respect to the Work licensed here. There are no understandings, agreements or representations with respect to the Work not specified here. Licensor shall not be bound by any additional provisions that may appear in any communication from You. This License may not be modified without the mutual written agreement of Demos and You.

DEMOS

Demos is a champion of people, ideas and democracy. We bring people together. We bridge divides. We listen and we understand. We are practical about the problems we face, but endlessly optimistic and ambitious about our capacity, together, to overcome them.

At a crossroads in Britain's history, we need ideas for renewal, reconnection and the restoration of hope. Challenges from populism to climate change remain unsolved, and a technological revolution dawns, but the centre of politics has been intellectually paralysed. Demos will change that. We can counter the impossible promises of the political extremes, and challenge despair – by bringing to life an aspirational narrative about the future of Britain that is rooted in the hopes and ambitions of people from across our country.

Demos is an independent, educational charity, registered in England and Wales. (Charity Registration no. 1042046)

Find out more at **www.demos.co.uk**

DEMOS

PUBLISHED BY DEMOS APRIL 2020.

76 VINCENT SQUARE, LONDON, SW1P 2PD
T: 020 3878 3955
HELLO@DEMOS.CO.UK
WWW.DEMOS.CO.UK