SciencesPo
CHAIR DIGITAL, GOVERNANCE AND SOVEREIGNTY

Has the time come to end anonymity on social media?

Lorenzo Ancona, Gabriel Karl,
Arnau Martì & Wiktor Samek

Comparative Approach to Big Tech Regulation (Spring 2023)
Professor Florence G'sell

April 2023

Table of contents

Abstract

In contemporary times, anonymity may appear to be anachronistic. Present-day technical solutions have exposed us significantly to surveillance by both private and public actors. Additionally, our digital identity has become a commodity delivered and used by Big Tech companies. Concurrently, issues concerning disinformation and user verification can create an impression of anonymity as potentially perilous to our society and democracy. Social media platforms are a prime example of these phenomena, highlighting how crucial it is to protect our privacy and identity.

In our paper, we demonstrate that anonymity remains a valid tool for safeguarding our privacy on social networks. We recognize the inherent limitations of anonymity, but instead of using them as a reason to completely reject the concept, we endeavour to adapt them creatively to construct better regulatory models. Consequently, relying on the contextual and pseudonymous nature of modern digital anonymity, we propose an innovative solution that merges anonymity with the requirement for verification and an adequate level of privacy and control over users' data by themselves. Our recommendations draw on academic research and legal frameworks, with a primary emphasis on the European Commission, which is the target of our address.

At a general level, we urge European institutions to perceive anonymity as an opportunity to create a more privacy-focused environment on social media. To ensure compliance with the provisions of the Digital Market Act (DMA) and General Data Protection Regulation (GDPR), the EU should enhance the adoption of Privacy-Enhancing Technologies and establish autonomous data trusts. The EU must also ensure coherent interaction and interpretation between the DMA and GDPR. We encourage EU institutions to investigate digital identity solutions as a potential approach to addressing verification issues, while maintaining privacy and anonymity. We believe that public solutions such as the European Digital Identity can be applied in this realm, but not as a mandatory means of user authorization. Instead, we recommend developing a policy of interoperability with private stakeholders that offers EU citizens a range of options tailored to their specific needs. All of these measures will significantly strengthen the position of regular citizens vis-à-vis social media platforms, without putting too much valuable private information under the control of any other central authority, using anonymity in a modern, responsible way.

Introduction

Is anonymity a fundamental right on the internet? Should we be able to conceal our true identities on social media platforms while continuing to use them? How can we strike a balance between the right to anonymity and the need for accountability? Conversely, is anonymity crucial to preserving our privacy while navigating the digital world? Our brief was inspired by these thought-provoking questions about anonymity and its implications in the digital age. In pursuit of answers, we have attempted to dissect the intricate notion of anonymity on social media, weighing its benefits and risks and providing a comprehensive overview of various regulatory and policy approaches. Building upon this foundation, we have devised targeted policy recommendations to tackle the intriguing issue of anonymity.

In the first section, we seek to **define anonymity** and highlight its critical connection with privacy. By analyzing the inner functioning and dynamics of social media, we find that anonymity is a contextual and relational concept, thus making complete anonymity unattainable on social media. Further, drawing on Floridi's concept of "informational privacy", we acknowledge **the interdependence between anonymity and privacy**, with the former being a prerequisite for the latter.

In the second section, we outline a comprehensive analysis of anonymity, detailing both its **benefits** and **risks** to provide a well-rounded understanding. Benefits encompass freedom of expression, privacy protection, and self-disclosure, while risks include cyberbullying, disinformation, and illegal activities.

Our analysis is rounded off in the third section by examining **policy and legal approaches to anonymity.** We compare legal systems that protect anonymity, such as those in the United States, European Union, and the United Kingdom, with those adopting a more restrictive approach. Additionally, from a policy perspective, we highlight various policies devised by regulators to address anonymity and its implications.

Ultimately, drawing on our comprehensive analysis, we target the European Union and identify three critical policy challenges, tackled with **three policy recommendations**. We address the need for digital identity systems, the enforcement of regulations, and privacy protection enabled by anonymity.

1. The concept of anonymity: an overview

Anonymity is naturally intertwined with cyberspace. It was in many ways a big promise of the web at the moment of its creation. But it was also an act of capitulation. In his famous *Declaration of the Independence of Cyberspace,* J. P. Bartlow wrote: *Our identities have no bodies, so, unlike you, we cannot obtain order by physical coercion* (Barlow, 1996)*.* Many cyber-enthusiasts correctly observed the changes the internet provoked in regard to our identities. However, Barlow and others made a massive mistake by assuming that this identity will be out of reach of the traditional powers of the material world. Moreover, it quickly became clear that this new identity is in fact delivered by actors emerging from the changes coming with the Web 2.0 revolution, namely the social media platforms. Anonymity can be perceived as an answer for that[1].

In this section of the text, we shall address these matters. Firstly, we present our own definition of anonymity. Then, we show its connection with the notions of privacy and identity. We will clearly show both changes provoked by the rise of social media platforms that are crucial for our analysis and recommendations presented in the next parts of the paper.

1.1 How anonymous can we be? A definition of anonymity

Delivering a clear definition of anonymity is paradoxically not very challenging. However, what is truly important is to understand that it is much different from the popular understanding of this term. We tend to perceive anonymity as a state excluding the possibility of identification. In reality, anonymity is always contextual or relational (Wallace, 1999, pp. 23–24). Therefore, it is never complete, even in purely analog societies. An author writing a book under a pseudonym or anonymously is not revealing

[1] It is emblematic that it became the symbol of the Anonymous collective founded in 2003 to oppose the limitation of internet "primal freedom" (Cadwalladr, 2012).

their name, gender or nationality to the public. However, they are sharing ideas or skills, both being parts of their identity.[2] Furthermore, an author can build their artistic capital based on anonymous or pseudonymous publications (Scott and Orlikowski, 2014, p. 876). That is a deep **ontological limitation** of anonymity.

Furthermore, there is an issue of practical manners. Is there any truly effective way of achieving anonymity even in this limited form? Going back to the "anonymous author" example, we can use the known fragments of identity to decode its other elements. Moreover, the more books someone writes the easier it is to reveal the whole picture. That is highly important given that in social media reality we have to dispose of hundreds of posts and other activities that in some cases can be as important for revealing one's activity. With addition of the sophisticated methods of data acquisition and analysis at the disposal of social media companies, it is justified to state that full anonymity is practically impossible in the reality of social media platforms (Scott and Orlikowski, 2014, p. 877).

The platform character of social media is crucial to understand the limitations of anonymity they allow. That is because the platform is not really "allowing" us to be anonymous, it is providing us with anonymity. Hence, anonymity is in a sense just another functionality of the platform. That is related to the concept of *unlinkability.* Anonymity can be analysed from the perspective of *sender* and *recipient* or the *relationship.* The first two tell us if we can link a particular message with a user who sent it or received it. The *relationship anonymity* is related to the possibility of observing the exchange of information between specific users (Pfitzmann *et al.*, 2007, p. 9). A social media platform can easily trace those connections as all of them are part of a process taking place nearly exclusively on the platform infrastructure. With no internal or external constraints, the platform can monitor it from the moment of uploading data via its application, through the processing taking place on its servers, to the moment it is finally received also via its software on the recipient side.

[2] As will be explained in the following part, for the purpose of our text we accept the modern, broad definition of identity.

At the same time, the **contextuality of anonymity** results in the high importance of the size of the population (Pfitzmann *et al.*, 2007). Social media platforms are in this context paradoxical. They gather a massive amount of users, but the relationships between them are somehow similar to the ones typical for the very small communities. L. Floridi illustrated that with an interesting comparison between the *local* and *global* village and their relation to the concept of privacy. In both cases, we have to deal with communities that are open. The exchange of information is public, and the distance between individuals is short, being limited by the material conditions or by technological tools. The differences are crucial though, as the *global village* is not protecting its members with the dense network of informal and formal self-regulation (Floridi, 2014, p. 112). Thus, we can conclude that social media platforms create an environment that exposes our privacy on an unprecedented scale both in relation to other users and the platform itself. Anonymity perceived in the contextual way, can somehow protect our privacy from other users, but not from the platform's or governments' interference. In the case of the latter, authoritarian regimes are already very effective in curbing the possibilities of achieving even limited anonymity online (Bode and Makarychev, 2013). At the same time democratic countries are becoming more and more efficient in tracking cybercrimes or even intercepting the encrypted communications between criminals (EUROJUST, 2023), not to mention regular internet's users that are possible to track by less sophisticated methods such as using their IP number.

Moreover, the meta analysis of data is currently on a level that makes it hard to tell about anonymity even on truly decentralised platforms (De Filippi, 2016). Blockchain-based infrastructure is a perfect example. Thanks to advanced cryptography, users of the blockchain social platforms are able to hide their personality behind aliases. Nevertheless, the key functionality of the blockchain networks is also transparency, as all interactions are stored in the open ledger. Therefore, its analysis can in a relatively effective way discover particular elements of one's identity and finally allow their proper identification. In our analysis and recommendation we focus on big, centralised social media platforms, however it is important to notice that even their decentralised competitors are not introducing the new, perfect version of anonymity.

Based on the above, we can deliver a definition of anonymity that will be used in our paper:

1. We accept the classical definition of anonymity as ***a state of being not identifiable within a set of subjects*** (Pfitzmann *et al.*, 2007, p. 6).
2. At the same time, we acknowledge the **contextual and relational character of anonymity** that makes the possibility of anonymity within all sets of subjects and in relation to all sides of the communication process impossible.
3. We believe that the possibilities of **anonymity on the social media is massively limited**, due to
    a. the possibilities offered by the meta analysis of data,
    b. high dependence on the social media platforms in regard to our digital identity and privacy,
    c. growing capabilities of the state to monitor all activities happening online.
4. Due to that, both centralised and decentralised platforms offer pseudonymity rather than anonymity, allowing users to use pseudonyms instead of their real names (ibidem, p.14) but not to remain truly not identifiable. Nevertheless, for the sake of clarity, in the further parts of the text we use the term “anonymity” rather than “pseudonymity” having in mind all aforementioned remarks.

Both in the presented definition as in the above part of the text, we mentioned notions of privacy and identity. As they are the phenomena protected by anonymity, in the next parts we will examine how they evolved in the social media environment and how it changed our perception of anonymity.

1.2 Who truly owns our identity?

Digital identity can be understood in two ways: as a **technical solution** allowing for the identification of a person in cyberspace or as a **specific set of data** translating one’s social identity to the web (Feher, 2021, p. 193).

In regard to the latter, our definition of anonymity is based on a broad understanding of identity, in line with modern psychology, defining it as *an integrative configuration of self-in-the-adult-world* (McAdams, 2001, p. 102). Therefore, in the social media context, identity means not simply one's name. To the contrary, our digital identity evolves in the direction of having less connection with it. That is why authors such as L. Floridi state that our decision regarding our identity in cyberspace is no longer truly related to the choice between anonymity and openness. That became impossible in the world of near constant surveillance conducted in more or less open forms by governments and private companies. What is left is the ability to decide on the shape of the imaginary identity we want to create on the social platform (Floridi, 2014, p. 64). However, our agency in this matter is also limited by the relational character of identity. Social platforms created a notion of *digital gaze* (Floridi, 2014, p. 73). It means that the platform’s users are perceiving themselves nearly exclusively through the perception of other users. Hence, a particular person is reduced to the output of the process of establishing identity, which is greatly taking place outside of its reach. In this context the control platforms have over the algorithms and their content promotion policies, equips them with a control over the creation of our identity, especially in the case of the youngest users. That has major consequences for anonymity, as hiding some part of our identity online makes no sense, as long as it is developed in the process not controlled by the user.

The issue of digital identity from a technological perspective is analysed mostly in the context of the possible provider of this solution and its public or private character. Government-provided solutions are currently used in regard to the public administration with actors such as the EU Commission planning to expand their use on other sectors (European Commission, 2021) and decentralised blockchain-based solutions are experimentally implemented to guarantee people with more control over their identity (Mühle *et al.*, 2018). Nevertheless, in the social media reality, digital identity is still provided mostly by the platform. Hence, being anonymous on the web is getting more problematic due to the development of more efficient ways of identification in cyberspace by the government as well as the dependency on the private solutions, oftenly enhanced by the connection of different services to one digital identity.

1.3 How to achieve privacy in public?

Anonymity is so intertwined with privacy that for many those two can be synonymous. Nevertheless, in the content of social media we need to firstly, focus on data, secondly, to acknowledge significant differences in the perception of privacy in different legal cultures[3]. To simplify, we can say that continental Europe developed the concept of privacy as a means of defending one's dignity, while American culture is more oriented towards the notion of liberty (Whitman, 2004). Europeans are therefore more concerned with the issues of *right to informational self-determination* (ibidem, p. 1161) and the protection of one's dignity in contact with private actors, and Americans tend to cultivate an older approach, trying to limit the state's interference with an individual's life (ibidem). Above, we demonstrated that both state and private companies can limit the anonymity on social media. It is natural that different legal cultures will perceive and regulate those issues differently.

When it comes to understanding **informational privacy**, in our work we adapted the framework created by L. Floridi. He stated that *informational privacy is a function of the ontological friction in the infosphere* (Floridi, 2005, p. 187), where *ontological friction* represents forces opposing the information flow (ibidem, p. 186). The value of this approach from the policy making perspective is clear. Firstly, Floridi noticed the ontological change coming with the social media platforms and internet in general. New technological means are not changing the infosphere, they are creating a completely new model on the ontological level. Secondly, that means that we cannot make general judgments about privacy in cyberspace, we must analyse particular elements of the new infosphere. Thirdly, even previous technological changes were not synonymous with unconditional limitation of our privacy. The same is true about the internet, which at the same time created a more or less open repository of our private information, and presented us with the unprecedented possibilities in regard to anonymity or encryption of information.

[3] Due to the scope of this paper that of course means different Western legal cultures, i.e. continental Europe and USA.

Therefore, in regard to privacy we acknowledge its connection to anonymity. It is important to remember, that both in the case of governmental or private actors, social media cannot guarantee privacy without some level of anonymity, as by definition privacy means keeping some parts of our personal (identified) data outside of their reach.

1. 2. Benefits and risks of anonymity on social media

In the Information Age (see Floridi, 2010), anonymity encompasses a complex interplay between various domains, including privacy, accountability, and free speech in democratic and non-democratic regimes. Therefore, a comprehensive examination of benefits and risks of anonymity is conducive to a thorough understanding of its implications and the design of effective policy recommendations.

2.1 Benefits and opportunities

2.1.1 Freedom of expression

Anonymity can contribute significantly to the freedom of expression by fostering **open discussions on sensitive topics** and providing **a safe shelter for dissenting voices**, especially in politically oppressive environments.

Firstly, individuals are more likely to express their opinions and voice their thoughts on social media without fear of political or personal repercussions (Nissembaum, 1999). Notably, they may dare to take stances or participate in discussions they would not engage in otherwise. Consequently, anonymity leads to a **more diverse and open public discourse**, thus benefiting democratic societies. (Nissembaum, 2009)

Secondly, as digitalization fuels the growth of **whistleblower** and **activist** organisations and social media are vital in disseminating leaked information, anonymity is crucial to safeguarding these individuals from potential retaliation or harm (Olesen, 2019). A case in point is the Arab Spring: activists relied on anonymous social media accounts to organise protests and share information about government crackdowns while avoiding detection by state authorities (Howard et al., 2011).

2.1.2 Privacy Protection

In an era of growing concern about personal data collection (Zuboff, 2015) and reformulation of the concept of privacy itself (Floridi, 2014), anonymity may offer considerable privacy protection benefits for users. As noted in Floridi (2005), “informational privacy” is not merely the control over personal data but also the attempt to keep one’s identity and autonomy.

Anonymous social media accounts and online interactions can **shield users from unwanted scrutiny**, allowing them to limit the flow of their personal information. However, as clarified in section 1 [The Concept of anonymity], true anonymity and a complete shelter from identifiability by social media is not achievable. Nevertheless, adopting this notion of partial traceability, users can avoid leaving behind trails of personal data exploitable for **commercial or malicious purposes**, such as identity theft (Nissembaum, 2004).

Furthermore, anonymity draws a separation line between *profile data* and *behavioural data*, dividing users' sensitive information—such as name, address, and birth date—from their online activities. This allows individuals to regain control over data they may prefer not to share online and mitigates the risk of malicious tracking that could link their activities to their identities.

2.1.3 Self-disclosure and Mental Health

Although the application scope is narrow compared to the freedom of expression and the protection of privacy, anonymity on social media has proven important for people seeking support for sensitive and potentially stigmatizing issues, such as mental health problems, addictions or trauma.

As anonymity facilitates **self-disclosure and online disinhibition** (Suler, 2004), users can express their feelings, seek advice, and share their experiences without fear of being judged or facing negative social consequences (Lawlor and Kirakowski, 2014). Studies have shown this positively impacts psychological well-being (Frye and Dornisch, 2010).

2.2 Risks and challenges

Anonymity on social media, despite its numerous advantages, also presents several risks for users. This analysis focuses on three primary challenges, all of which stem from a key issue: **the lack of accountability.** As a critical concern resulting from anonymity, accountability will be thoroughly examined and discussed in the subsequent sections of this policy brief.

2.2.1 Cyberbullying and Harassment.

The widespread use of social media combined with anonymity has fostered interactions among users, including practices such as **online harassment** and **cyberbullying**. Anonymity is conducive to cyberbullying (Whittaker and Kowalski, 2015) as the absence of identifiable information allows users to engage in harmful behaviours with little to no consequences, as it becomes difficult to trace these actions back to the perpetrator (Aboujaoude et al., 2015). This lack of accountability can foster a toxic online environment, where users feel emboldened to engage in aggressive or abusive behaviours they might not otherwise exhibit in face-to-face interactions.

As a consequence, the higher degree and frequency of cyberbullying may cause severe psychological distress for victims, that suffer from anxiety, depression, low self-esteem, and even suicidal ideation (Patchin and Hinduja, 2010).

2.2.2 Disinformation

The proliferation of fake news and false propaganda is a significant challenge posed by anonymity on social media. Anonymity is a fertile ground enabling **bots**, **fake accounts** and **inauthentic conversations** over various topics, leading to an unreliable and untrustworthy online information ecosystem that may spill over into real-world consequences.

Social media bots, defined as “automated accounts capable of producing content and interacting with human users on social media platforms" (Ferrara et al., 2016), thrive in an environment that privileges online anonymity (Persily, 2019*)*. With most people accessing news through social media (Gottfried and Shearer, 2016), bots play a decisive role in steering the public debate by spreading fake news online on topics ranging from politics to health. Bots are programmed to amplify specific narratives or influence public opinion, thus manipulating social media and deceiving users during initial phases, prior to content reaching viral status, and they focus on engaging with influential users via replies and mentions. This susceptibility to manipulation is evident as individuals tend to retweet bots sharing low-credibility content nearly as frequently as they retweet other people (Shao et al., 2018). Persily (2019) describes this as **"unaccountable engagement"**, where it is unclear not only *who* is speaking but also *whether* the speech comes from a real person. Finally, the anonymity provided by social media platforms makes it difficult to trace the origins of bot creators or hold them responsible for spreading false information (Ferrara, 2020).

This online disinformation environment causes a wide array of **consequences in the physical world**, ranging from manipulation during election campaigns (Allcott and Gentzkow, 2017) to dissemination of false information related to public health issues (Shahi et al., 2021).

2.2.3 Illegal activities

Anonymity on social media platforms can serve as a shelter for individuals and groups to participate in a variety of illegal activities. For instance, anonymous users can share **illicit content**, such as child pornography or copyrighted materials, hiding behind online anonymity without the fear of being identified and, thus, prosecuted. (UNICEF, 2022). Moreover, anonymity offers an incentive to hackers and cybercriminals to carry out other criminal activities such as **identity theft, phishing, or launching cyberattacks**, with reduced risk of being traced (Sullins, 2006).

Digital communication technology and anonymity also significantly influence **radicalization** and **recruitment** (Meleagrou-Hitchens et al., 2017). This environment enables extremist groups to disseminate propaganda and recruits potential adepts, thus fostering radicalisation in some contexts. Particularly, unsuspected individuals that would not engage in such activities offline take advantage of the anonymous environment provided by the internet (McFarlane, 2010). Indeed, as Koehler (2014) found, anonymity is a key factor driving individuals towards extremist views and groups.

2. 3. Policy and legal approaches

We continue our analysis of the concept of anonymity by considering diverse regulatory systems and policy approaches. In the first part of this section, we look at how regulators have enforced rules concerning anonymity, examining liberal systems and authoritarian regimes. Then, in the second part, we outline some policies devised to grapple with anonymity and its implications.

3.1. Existing regulations on anonymity

In this section, we will observe how existing regulations apply online anonymity in different countries. Although each country has a different jurisprudence, we have identified two distinct positions: countries acknowledging anonymity as a legal right and those applying a restrictive approach.

Thus, we will explore the nuances of online anonymity as a legal right in various regions, including North America, the United Kingdom, and the European Union, as well as the contrasting restrictive approach to online anonymity in countries with limited media freedom, such as Russia and China.

3.1.1 Online anonymity as a right

For many of the western countries, anonymity of identity and communication is a legal right safeguarded by the article on freedom of expression in the UN Charter of Human Rights of 1948. However, ensuring anonymity is complex, as limitations on freedom of expression and anonymity may be justified in certain circumstances for reasons such as national security, prevention of defamation, harassment, or incitement to hatred. In countries with liberalized media systems, the challenges surrounding online anonymity often revolve around balancing speech rights against other individual rights within the framework of this conditional or pseudo-anonymity (Moyakine, 2016).

A. US and North America

In the US, traditionally, the Supreme Court has protected anonymous speech under the First Amendment, but as with other constitutional rights, it has balanced protection against competing interests, notably in the areas of political activity and campaign finance for example. On the internet, the Supreme Court has recognized anonymity rights in speech, but not as an absolute right, and state courts have generally taken a similar view.

In “The United States of Anonymous: How the First Amendment Shaped Online," author Jeff Kosseff explores two cases, *Dentrite International, Inc. v. Doe* No. 3, 775 A.2d 756 (N.J. App. Div. 2001) and *Cahill v. Doe*, 879 A.2d 943 (Del. Super. Ct., June 14, 2005), in which courts recognized relatively strong First Amendment presumptions on behalf of purveyors of anonymous speech, especially for those that are statements of opinions rather than obvious falsehoods, while recognizing that government sometimes has the right to identify such speakers when they have used their platforms to harass, engage in slander or sexual predation, make true threats, or allow foreign governments to influence U.S. elections. (Martin and Fargo, 2015)

In Canadian law, although such a right is sometimes recognized as tied to the right to privacy. With regard to online anonymity, Canadian courts have developed a balancing test requiring the party seeking to compel the identification of anonymous users to first show that it has a *bona fide* claim and that there is no alternative source of the needed information. If the party can make such a showing, a court must weigh factors favouring or disfavoring disclosure. Canadian courts developed this test in a case involving an attempt to unmask ISP customers who were allegedly violating the plaintiff’s copyright interests.(Martin and Fargo, 2015)

B. UK

Similarly, in 1973 the House of Lords established a test for the conditions under which a litigant could force a third party in a lawsuit to identify potential defendants. The party seeking the information must show that: (1) the unknown party arguably committed a wrong against the plaintiff; (2) identification of the unknown party is necessary; and (3) the third party is able to identify the alleged wrongdoer. Courts are expected to balance the third party's interests in maintaining confidentiality versus the interests of justice. This test has also been used in other UK lawsuits involving Internet bulletin boards and other online publications (Martin and Fargo, 2015).

C. European Union

European law tends to be more protective of privacy than American law, yet the extent of that protection can vary somewhat from country to country. Anonymity is sometimes viewed as a privacy-related right, particularly with regard to personal data. In 2003, the Committee of Ministers of the Council of Europe addressed the principle of anonymity in its declaration on freedom of communication on the Internet. The declaration provides that in order to ensure protection against online surveillance and to enhance the free expression of information and ideas, member states should respect the will of users of the Internet not to disclose their identity. In 2013, the European Parliament voted to adopt new regulations that would require companies to anonymize personal data collected from users after German Chancellor Angela Merkel persuaded EU commissioners to back regulations requiring Internet companies to report to whom they gave users' personal information. In 2014, the European Court of Justice ruled that Google and other ISPs and content providers must, in certain circumstances, accept demands that older links to even truthful information about persons be disabled so they do not appear in search results related to those persons (Moyakine, 2016).

More recently, since May 2018, the **General Data Protection Regulation (GDPR)**, a EU regulation on data protection and privacy for all individuals within the European Union (EU), aims to give people more control over their personal data and to unify data protection rules within the EU. It imposes strict requirements on how personal data is collected, processed, and stored, and it also gives individuals the right to access their data, have it corrected, and have it erased in certain circumstances. It applies to all organisations that handle personal data, regardless of whether they are based inside or outside the EU.

In terms of online anonymity, GDPR encourages the use of **pseudonymisation** and **encryption** to reduce risks for data subjects while helping data controllers and data processors to meet their obligations.[4] The EU law obliges data controllers to implement all appropriate technical and organisational measures, such as pseudonymisation, in

[4] We define 'data controllers' as natural or legal persons, competent authorities or other bodies that determine the purposes and means of the processing of personal data. Data Processors are natural or legal persons, competent authorities or other bodies that process personal data on behalf of controllers

order to comply with data protection principles and integrate necessary safeguards into the processing of personal data. The Regulation specifically mentions pseudonymisation and encryption as instruments to be deployed by controllers and processors in personal information processing. Recent European legislations as the Digital Markets Act, which aims to create a fair and competitive digital market in the EU by regulating gatekeepers, and the Digital Services Act, that obliges the major online platforms to fight hate, fake news and crime on the internet, offer the possibility to implement safeguards for the benefit of data subjects. These also include pseudonymisation and anonymization of personal data. With those legislations, anonymisation of data may gain significantly in importance, but GDPR still remains the standard when it comes to processing personal data (Demircan, 2022).

It should be noted that, under GDPR if personal data is properly anonymized, it is no longer considered personal data so, the GDPR's provisions on the protection of personal data do not apply to anonymized data.

To conclude, the right to online anonymity is not explicitly mentioned in EU Law as a standalone right. Nevertheless, some cases on online anonymity at the European Court of Human Rights demonstrates that the Court considers anonymity to be key to protecting freedom of expression online in the european union. On 7 December 2021, this court published its judgement in “Standard Verlagsgesellschaft MBH v Austria (No.3)” where she founds that the Austrian court had violated the applicant’s right to freedom of expression by requiring the applicant to disclose the identities of those who had posted allegedly defamatory comments on its website.

3.1.2 Restrictive approaches to online anonymity

In countries with restricted media systems, online anonymity may be prohibited altogether or heavily restricted through laws and regulations requiring internet service providers and online platforms to collect and retain user data, including their identities and online activities. This data can be used by government agencies to monitor and control online content, and to identify and prosecute individuals who express dissenting views or engage in activities deemed threatening to the regime.

A. Russia

The Russian government has adopted several measures to control citizens' use of the Internet. The "Law on Information, Information Technologies and Protection of Information" (2006) required online service providers to collect and retain certain information about their users, including their full names, addresses, and other identifying information. In 2016 and 2019 the “Yarovaya Law” and the “Internet Isolation Law” reinforced the previous law and required online service providers to install equipment allowing the government to block access to certain websites and services, and to retain information about users' online activities, such as their browsing history and search queries, for at least six months. Additionally, it was reported that Russia's interior ministry was offering close to more than $100,000 for research on how to identify the anonymous users of Tor, which masks the sources and destinations of Internet browsing and prevents users from tracking(Martin and Fargo, 2015).

B. China

The Chinese constitution guarantees freedoms of speech, association, and publication subordinate to the ruling party but the Chinese government has taken great strides to prevent anonymous and participation in controversial topics through a complex system of filtering, blocking, and investigating websites ISPs and Internet users. In 2011, 2012 and 2016, China took several steps seeking to control anonymity on the Internet, including creating a new agency to coordinate Internet regulation, increasing pressure on intermediaries to "self-censor" content and users, and tightening controls on social media. In 2012, the Chinese government passed a policy requiring Internet users to register their real names with service providers to help service providers better protect customers' information. Lastly, to eliminate any ambiguity, the "Cybersecurity Law" and the "Internet Security Law," enacted in 2016 and 2017, mandate that online service providers store data collected in China on servers located within the country and grant full access to government authorities upon request. This demonstrates that the right to online anonymity in China is, in fact, not guaranteed (Martin and Fargo, 2015).

3.2. Policy approaches to identity verification

Faced with increasing levels of abuse, harassment, and the rise of global disinformation campaigns enabled by bot networks on social media, regulators have started to show greater interest in devising policies with the potential of reigning in these undesirable behaviours on social media. Anonymity is often pointed out as the culprit behind the prevalence of online harassment and abuse, because "anonymity abets anti-social behaviour" (Rainie et al., 2017, p. 7). This has led some policymakers to issue proposals aiming to ban or regulate the possibility for users of social media platforms to preserve their anonymity. Both the UK and Australia have discussed the possibility of mandating identity verification requirements for opening social media accounts (Baillie, 2021; Standing Committee on Social Policy and Legal Affairs, 2021, p. 31), and a bill in the French Senate tried to create an independent government authority tasked with linking the identity of French social media users to their accounts, effectively banning anonymous social media accounts (*Proposition de Loi Instituant Une Autorité de Contrôle de l'identité Numérique*, 2021).

Although none of these propositions were implemented, as they were deemed to constitute a significant impediment to freedom of speech, they highlight continued interest on the side of policymakers to use identification measures as a tool to disincentivize online abuse. Indeed, there is a case to be made for the necessity to strike the right balance between the freedom afforded to social media users by anonymity and the implementation of policy measures enabling competent authorities to effectively prosecute illicit behaviour on these platforms. Depending on the approach, such policies can fall on different parts of the spectrum between anonymity and control over user activity.

3.2.1 'Real name' policy

The most radical approach to tackling this issue would be to mandate the use of users' real identity on social media platforms, effectively prohibiting the use of pseudonyms. This stance is already adopted by certain social media platforms, for instance by Facebook with its **'real name' policy.** However, this approach significantly infringes on the rights of social media users to operate under aliases or pseudonyms in their online activities, and Facebook has had to relax its own policy in the wake of starch criticism by civil liberties associations in the past (Hern, 2015). This view is shared by a number of regulating bodies, first of which the European Data Protection Board and the French Data Protection Agency, as they both argue that every user has the right to use pseudonyms and should be free to maintain multiple digital identities, the attributes of which do not necessarily overlap with each other and can showcase different aspects of a person's identity that they do not necessarily want to associate with either their government identity or other digital identities (CNIL, 2023, p. 10). The potential benefits flowing from such a disruptive decision might also not outweigh the harm inflicted on free expression online. In fact, it should be considered that forcing the use of 'real' names on social media platforms has not been associated with an absolute decrease in harassment. Platforms such as Facebook, which operate under a 'real name' policy for users, are not immune to online harassment, and while anonymity is certainly a disinhibiting force that can encourage abuse in some people, the real driver behind such behaviours appears to be a lack of perceived accountability, rather than the possibility of remaining anonymous (Matias, 2017).

3.2.2 Opposable pseudonymization

The implementation of regulatory and technical infrastructure allowing for the use of **'opposable pseudonyms'** has been hailed as a conciliatory approach allowing to preserve a high level of relative anonymity for users on social media platforms, while equipping the platforms and public authorities with new tools to better apprehend the spread of hate speech and disinformation campaigns online (Basdevant et al., 2022, p. 96).

Using cryptographic tools such as Zero Knowledge Proof (ZKP), users would be able to share certain attributes of their identity with social media platforms without giving the platforms direct access to the information used for the certification, either through a trusted third party (e.g. a bank) or a personal digital wallet such as the one currently being developed by the European Union (European Commission, 2023). The trusted certifying service would reply to a query from social media platforms with an attribute acknowledging that the individual behind the account creation 'is a person' or 'is old enough to gain access to the service', instead of communicating a name, an ID document number or a birth date (Birch, 2019). If elaborated in conjunction with governments, this service could be designed with a procedure for competent authorities to be able to override the opposable pseudonym and link it back to the identity of an individual, thus facilitating legal recourse against illicit behaviours on social media platforms (Bennett & Beverton-Palmer, 2021).

Additionally, the possibility of ascertaining the owner of an account as being a physical person would create a new level of control offered to users on social media platforms. They could for instance define their preferences on social media platforms to prevent contact with accounts that have not yet been verified, interacting only with users they are certain to be real individuals. This has the potential of limiting the impact that networks of bots could have on user interactions on prominent social media networks. Giving more control to the users of social media platforms in determining who they accept to interact with also has the potential to reduce user exposure to abuse and harassment: on the one hand by shielding them from users that have not gone through the process of verification and by allowing for the identification of those that have been verified and engage in illicit behaviours (Birch, 2019).

Although this approach would preserve the possibility for social media users to remain anonymous vis-à-vis other users and the platforms themselves if they so choose, governments would need to tread carefully in their approach to the implementation of such a solution. The possibility for public authorities to ‘break’ digital credentials could limit the widespread adoption of such a measure and possibly lead to opposition from minorities that deem it to compromise their ability to express themselves free from any outside control or repression. This fear could be mitigated by designing the ZKP system in a way that prevents the trusted third parties from knowing what social media platform is requesting the token for verification. This would eliminate the fear by citizens that the trusted third party would be in possession of a list linking the real identity of a person and the token used to verify that individual’s identity directly to the social media platform it was generated for, while maintaining the possibility for competent authorities to create that link if the need arises over the course of an investigation warranting this intervention.

3. 4. Policy and Legal Recommendations

Drawing on the extensive analysis conducted in previous sections, we focus on the policy recommendation section of our brief. Recognizing the European Union's role in shaping digital policies, we identify **three critical policy challenges** that need to be addressed. To tackle these challenges, we propose **a set of policy recommendations**, which aim to establish robust digital identity systems, ensure privacy protection through anonymity, and enhance the enforcement of existing regulations.

4.1 Anonymity must be perceived in the broader framework of privacy and identity regulation.

Policy challenge:

Until now, the right to online anonymity has merely enjoyed limited recognition on international law and regulation and cannot be concluded to constitute a legal right universally recognised by States. However, while international law and regulation have provided some limited recognition of this right, <u>it is essential to acknowledge that when governments and private actors monitor online activities and gather information, they violate the rights to privacy and data protection</u>. These violations decrease people's confidence in Internet services and undermine their security online, leading to negative consequences for the free circulation of ideas and information on the Internet and violating the freedom of expression. As such, it is crucial for users to have the right to private correspondence, and it is the State's responsibility to take all necessary measures to ensure that communications reach their recipients without inspection or interference from State organs or private actors.

Policy recommendations:

While the right to online anonymity, like the right of freedom of expression, cannot be absolute, <u>improving online privacy and data protection can contribute to a more democratic digital society that respects freedom of expression while avoiding security and cybersecurity risks for states that stem from lack of accountability.</u> It is therefore necessary for the European Commission to adopt effective data protection laws providing clear rules on who is allowed to have access to personal data of individuals, for which purposes this data can be used, how it can be stored and for how long.

In this context, existing regulations such as the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act of 2018 (CCPA) can serve as the transnational gold standard for data protection, applicable to all domestic and cross-border transfers of personally identifiable data.

4.2 Digital identity verification solutions should be examined as a potential lever for reducing online abuse in consultation with stakeholders.

4.

Policy challenge:

The idea of mandating an **identity verification** for users of social media platforms regularly resurfaces in debates surrounding the possibility for governments to implement solutions limiting the proliferation of online abuse, as we have seen in the previous section. However, the prospect of allowing social media companies direct access to the identity attributes of all users has consistently led policymakers to decide against such a radical solution. The advent of projects aiming to implement government digital identities have nonetheless made new approaches, such as the implementation of ZKP protocols, possible. These could combine the preservation of a high level of anonymity for social media users with increased means of action for authorities, thus making legal recourse against offenders easier for victims of online abuse.

This should not be understood to mean that all roadblocks have been resolved, as many of them remain. One of the challenges relevant to attempts at regulating the internet in general is that national legislation is only rarely meaningfully applicable beyond a country's borders, making it difficult to deal with online services operating worldwide. This remains true even for legislation aimed to be applied only to the citizens of one country, as the widespread use of tools such as VPNs allows users to easily circumvent obligations implemented for their country. Although the EU has a history of being able to project its legislation beyond its borders through the Brussels effect

(Gunst & De Ville, 2021, p. 439), it cannot be expected that this would be the case for regulation on this issue, as proposed solutions might not be sufficiently consensual or realistically implementable at the international level.

Designing identity verification protocols that do not put the burden of verification on social media platforms will necessitate ensuring interoperable systems between several different public and private stakeholders. Interoperability can have multiple definitions depending on the context. In the case of European regulation, we can differentiate between two main approaches, related to the private and public sectors and both applicable in the European regulatory framework. The first is related to the Digital Market Act (DMA), which introduces the concepts of vertical and horizontal interoperability. Vertical interoperability is limited to app stores and the essential functionalities of operating systems, while horizontal interoperability applies to the basic functionalities and gatekeepers providing messaging services (Bourreau, 2022). Regarding the public sector, one of the main projects is the Interoperable Europe Act, which intends to create a trans-European framework for digital public service infrastructure (European Data Protection Supervisor, 2023). Finally, the **European Digital Identity** is the most ambitious project, aiming to create a decentralised digital wallet allowing EU citizens to control their personal data, in line with the notion of self-sovereign identity (European Commission, 2023).

Policy recommendations:

In light of these challenges, we make the following recommendations to orient discussions surrounding the use of secure identity verification solutions that remain protective of users' personal data:

- **Engage in discussions at the international level on strategies to prevent online abuse.** Illicit behaviours on social media platforms are not an issue unique to the EU and cannot be overcome without concerted efforts. Therefore, the EU should seek to build international consensus surrounding best practices that can increase protections for users on social media platforms by increasing accountability and the potential for legal recourse, without compromising users' ability to operate anonymously.

- **Negotiate a framework surrounding identity verification solutions in consultation with social media platforms.** The framework surrounding identity verification solutions should be elaborated by the European Commission in consultation with social media platforms. However, the protection of users' personal data needs to remain at the centre of these efforts, creating a system that allows neither the social media platform nor the trusted third party to create direct links between a real identity and an online pseudonym. Zero Knowledge Proof protocols should therefore be central to debate.
- **Allow interoperability between the European Digital Identity project and identity verification procedures put in place.** The **EU digital wallet** will enable users/citizens to store their data in a decentralised manner, allowing them to remain in complete control over it. It should be designed to be compatible with ZKP protocols, allowing for its use for identity verification procedures once it is officially launched.
- **Foster exchange and innovation between diverse public and private actors.** Citizens should be able to choose between a variety of providers of digital identity and trusted third parties. Private and public entities should thus be encouraged to propose digital identity solutions in accordance with the needs of users and in compliance with relevant protections afforded to EU citizens by EU regulations.

4.3 Ensure the privacy protection enabled by anonymity

Policy challenge:

We do not aim to frame anonymity as the right to be untraceable, but rather to leverage its benefits, granting users enhanced data protection. In other words, we seek to conceptualise **anonymity as a guarantee of privacy** rather than a shield from accountability.

This understanding of anonymity raises some policy and legal concerns, tackled in our recommendations. Central to this discussion is the pivotal role of social media platforms, which not only facilitate anonymity but also act as gatekeepers, controlling access to user information by third parties and managing data processing. Consequently, the extent of our "right to anonymity" largely hinges on these platforms. It is therefore imperative for the European Union to enshrine anonymity as a privacy-preserving measure in platform regulation. This involves applying and enforcing personal data protection through anonymity by bridging the General Data Protection Regulation (GDPR) and the Digital Markets Act (DMA).

Hence, a policy challenge arises: *how can the European Commission ensure and strengthen the privacy granted by anonymity on social media through the GDPR and DMA?*

Policy recommendations:

Provisions related to **anonymisation of personal data,** such as the Article 6(11) of DMA, spark two main sub-challenges:

- *How to balance strong anonymisation while maintaining data valuable?*
- *How to cope with the challenge of data anonymization in compliance with the GDPR, thus avoiding any possible re-identification (CIPL, 2021)?*

As anonymity and its application require a high level of technical expertise, these recommendations combine legal and technical measures that we advise the EU to undertake. The Commission could:

- **Improve and encourage the adoption of Privacy-Enhancing Technologies.** These ICT tools minimise personal information collection, processing, and storage while empowering individuals with greater control over their data. PETs effectively remove or transform identifiable personal information, making re-identification nearly impossible (OECD, 2023).
- **Establish independent data trusts as a means to protect privacy while facilitating data access.** Data trusts would collect raw user data and anonymize it appropriately, reducing the risk of de-anonymisation. Furthermore, data trusts could function as **data sandboxes,** allowing third-party algorithms to analyse the data without providing direct access to the raw data. However, practical challenges related to infrastructure, cost, and privacy must be addressed, and

the feasibility of such a solution may depend on focusing on specific subsets of data (Centre on Regulation in Europe, 2022).

Further, to ensure the effectiveness of GDPR and the DMA in regulating and policing anonymity on social media, the Commission should:

- **Ensure a coherent interplay between DMA and GDPR.** It is crucial to provide a consistent interpretation and maintain a **harmonised regulatory approach between the DMA and GDPR.** Specifically, as the DMA's provisions on data accumulation, data cross-use prohibitions and data sharing related obligations are closely tied to GDPR (Demircan, 2022), the EU must guarantee that the DMA neither undermines nor deviates from the principles set forth in the GDPR.

References

Aboujaoude, E., Savage, M.W., Starcevic, V., Salame, W.O., 2015. Cyberbullying: Review of an Old Problem Gone Viral. Journal of Adolescent Health 57, 10–18.

Allcott, H., Gentzkow, M., 2017. Social Media and Fake News in the 2016 Election. Journal of Economic Perspectives 31, 211–236.

Baillie, S. (2021) *Social Media Platforms (Identity Verification) Bill - Parliamentary Bills - UK Parliament*. Available at: https://bills.parliament.uk/bills/3073

Barlow, J.P. (1996) A Declaration of the Independence of Cyberspace, Electronic Frontier Foundation. Available at: https://www.eff.org/pl/cyberspace-independence.

Basdevant, A., François, C. and Ronfard, R. (2022) *Mission exploratoire sur le métavers*, p. 116.

Bennett, A. and Beverton-Palmer, M. (2021) *Social Media Futures: How to Reconcile Anonymity, Abuse and Identity Online*, *Tony Blair Institute for Global Change*. Available at: https://www.institute.global/insights/tech-and-digitalisation/social-media-futures-anonymity-abuse-and-identity-online.

Birch, D.G.W. (2019) 'Unknown, known and verified | 15Mb'. Available at: https://blog.dgwbirch.com/?p=562

Bode, N. and Makarychev, A. (2013) 'The New Social Media in Russia: Political Blogging by the Government and the Opposition', Problems of Post-Communism, 60(2), pp. 53–62.

Bourreau, M. (2022) *DMA: Horizontal and Vertical Interoperability Obligations*. Centre on Regulation in Europe.

Cadec, A. (2021) *Proposition de loi instituant une Autorité de contrôle de l'identité numérique*.

Cadwalladr, C. (2012) 'Anonymous: behind the masks of the cyber insurgents', The Observer, 8 September. Available at: https://www.theguardian.com/technology/2012/sep/08/anonymous-behind-masks-cyber-insurgents

CIPL (2019). Bridging the DMA and the GDPR.

CNIL (2023) *L'identité numérique*. Dossier thématique. Paris: CNIL, p. 20.

De Filippi, P. (2016) 'The Interplay between Decentralization and Privacy: The Case of Blockchain Technologies'. Rochester, NY. Available at: https://papers.ssrn.com/abstract=2852689 (Accessed: 13 April 2023).

Demircan, M., 2022. The DMA and the GDPR: Making Sense of Data Accumulation, Cross-Use and Data Sharing Provisions.

Demircan, Muhammed. ‘The DMA and the GDPR: Making Sense of Data Accumulation, Cross-Use and Data Sharing Provisions’. *Vrije Universiteit Brussel*, December 2022

EUROJUST (2023) New strike against encrypted criminal communications with dismantling of Exclu tool | Eurojust | European Union Agency for Criminal Justice Cooperation. Available at: https://www.eurojust.europa.eu/news/new-strike-against-encrypted-criminal-communications-dismantling-exclu-tool (Accessed: 13 April 2023).

European Commission (2021) Commission Recommendation of of 3.6.2021.

European Commission (2023) *European Digital Identity*. Available at: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en (Accessed: 15 April 2023).

European Data Protection Supervisor (2023) *Opinion on the Proposal for an Interoperable Europe Act*.

Feher, K. (2021) ‘Digital identity and the online self: Footprint strategies – An exploratory and comparative research study’, Journal of Information Science, 47(2), pp. 192–205. Available at: https://doi.org/10.1177/0165551519879702.

Ferrara, E., 2020. What Types of COVID-19 Conspiracies are Populated by Twitter Bots? FM.

Ferrara, E., Varol, O., Davis, C., Menczer, F., Flammini, A., 2016. The Rise of Social Bots. Commun. ACM 59, 96–104.

Floridi, L. 2005.‘The Ontological Interpretation of Informational Privacy’, Ethics and Information Technology, 7(4), pp. 185–200. Available at: https://doi.org/10.1007/s10676-006-0001-7.

Floridi, L. 2014. The 4th revolution: how the infosphere is reshaping human reality. First edition. New York ; Oxford: Oxford University Press.

Floridi, L., 2005. The Ontological Interpretation of Informational Privacy. Ethics Inf Technol 7, 185–200.

Frye, N.E., Dornisch, M.M., 2010. When is trust not enough? The role of perceived privacy of communication tools in comfort with self-disclosure. Computers in Human Behavior, Advancing Educational Research on Computer-supported Collaborative Learning (CSCL) through the use of gStudy CSCL Tools 26, 1120–1127.

Gottfried, J., Shearer, E., 2016. News use across social media platforms. White paper, Pew Research Center.

Gunst, S., De Ville, F., 2021. The Brussels Effect: How the GDPR Conquered Silicon Valley. EERR 26, 437–458. https://doi.org/10.54648/EERR2021036

Nissenbaum, H., 1999. The Meaning of Anonymity in an Information Age, The Information Society, 15:2, 141-144

Hern, A. 2015. 'Facebook relaxes "real name" policy in face of protest', *The Guardian*, 2 November. Available at: https://www.theguardian.com/technology/2015/nov/02/facebook-real-name-policy-protest.

Howard, P.N., Duffy, A., Freelon, D., Hussain, M.M., Mari, W. & Maziad, M., 2011. Opening Closed Regimes: What Was the Role of Social Media During the Arab Spring?

Koehler, D. 2014. The Radical Online: Individual Radicalization Processes and the Role of the Internet. Journal for Deradicalization 116–134.

Kramer, J. 2022. Data Access Provisions in the DMA. *Centre on Regulation in Europe - Issue Paper November 2022*

Lawlor, A., Kirakowski, J., 2014. Online support groups for mental health: A space for challenging self-stigma or a means of social avoidance? Computers in Human Behavior 32, 152–161.

Martin, Jason A., and Anthony L. Fargo. 'Anonymity as a Legal Right: Where and Why It Matters'. *16 N.C. J.L. & Tech. 311*, 2015.

Matias, J.N. 2017. 'The Real Name Fallacy', *Coral by Vox Media*, 3 January. Available at: https://coralproject.net/blog/the-real-name-fallacy/

McAdams, D.P. 2001. 'The Psychology of Life Stories', Review of General Psychology, 5(2), pp. 100–122. Available at: https://doi.org/10.1037/1089-2680.5.2.100.

Meleagrou-Hitchens, A., Alexander, A., Kaderbhai, N., 2017. The impact of digital communications technology on radicalization and recruitment. International Affairs 93, 1233–1249.

Moyakine, Evgeni. 'Online Anonymity in the Modern Digital Age: Quest for a Legal Right'. *Journl of Information Rights Policy and Practice*, October 2016.

Mühle, A. et al. (2018) 'A survey on essential components of a self-sovereign identity', Computer Science Review, 30, pp. 80–86. Available at: https://doi.org/10.1016/j.cosrev.2018.10.002.

Nathaniel A. Persily, 2019. The Internet's Challenge to Democracy: Framing the Problem and Assessing Reforms (2019).

Nissenbaum, H., 2004. Privacy as Contextual Integrity. Washington Law Review 79.

Nissenbaum, H., 2009. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press.

OECD, 2023. Emerging Privacy Enhancing Technologies. Current Regulatory and Policy Approaches. *OECD Digital Economy Papers*

Patchin, J.W., Hinduja, S., 2010. Cyberbullying and Self-Esteem*. Journal of School Health 80, 614–621.

Pfitzmann, A. et al. 2007. 'Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology'.

Rainie, L. *et al.* 2017. *The Future of Free Speech, Trolls, Anonymity and Fake News Online*. Pew Research Center. Available at: https://www.pewresearch.org/internet/2017/03/29/the-future-of-free-speech-trolls-anonymity-and-fake-news-online/.

Salmony, M. (2018) 'Rethinking digital identity', *Journal of Payments Strategy and Systems*, 12, pp. 40–57.

Scott, S.V. and Orlikowski, W.J. (2014) 'v', MIS Quarterly, 38(3), pp. 873–894.

Shahi, G.K., Dirkson, A., Majchrzak, T.A., 2021. An exploratory study of COVID-19 misinformation on Twitter. Online Social Networks and Media 22, 100104.

Shao, C., Ciampaglia, G.L., Varol, O., Yang, K., Flammini, A., Menczer, F., 2018. The spread of low-credibility content by social bots. Nat Commun 9, 4787.

Shao, C., Ciampaglia, G.L., Varol, O., Yang, K.-C., Flammini, A., Menczer, F., 2018. The spread of low-credibility content by social bots. Nat Commun 9, 4787.

Standing Committee on Social Policy and Legal Affairs, 2021. *Inquiry into family, domestic and sexual violence*. Canberra: Parliament of the Commonwealth of Australia, p. 471.

Suler, J., 2004. The Online Disinhibition Effect. CyberPsychology & Behavior 7, 321–326.

Sullins, Lauren L. « "Phishing" for a solution: domestic and international approaches to decreasing online identity theft », Emory international law review. 2006, vol.20 no 1. p. 397-.

Wallace, K.A. 1999. 'Anonymity', Ethics and Information Technology, 1(1), pp. 21–31. Available at: https://doi.org/10.1023/A:1010066509278.

Whitman, J.Q. 2004. 'The Two Western Cultures of Privacy: Dignity versus Liberty', The Yale Law Journal, 113(6), pp. 1151–1221. Available at: https://doi.org/10.2307/4135723.

Whittaker, E., Kowalski, R.M., 2015. Cyberbullying Via Social Media. Journal of School Violence 14, 11–29.

Zuboff, S., 2015. Big Other: Surveillance Capitalism and the Prospects of an Information Civilization.

About the authors :

Lorenzo Ancona has a background in Political Science and Digital Communication and is currently doing an internship as Digital Policy Analyst. He is keenly interested in the transformative potential of digitalization as a vehicle to strengthen democracy and catalyze citizen participation. His research revolves around the intersection of technology and societal values, digital transformation for government and innovation for democracy.

Wiktor Samek is a second-year master's student in the Digital, New Technology, and Public Policy stream and an intern at the OECD Digital Government and Data Unit. With a background in political science and law, his primary areas of interest revolve around the impact of technology on the development of contemporary political identities, the involvement of the state in the digital economy, and the concept of digital identity

With a background in economics and sociology. **Arnau Marti** is currently pursuing a master's degree in public policy and innovation at Sciences Po's School of Public Affairs. Having worked as a research assistant and member of government programme teams in Latin America, his interests lie in macroeconomic policy innovation. His latest research focuses on energy transition and sustainable international trade and finance.

Gabriel Karl has a background in international relations, comparative politics, and European affairs. A graduate of the dual degree program between Sciences Po and Columbia University, he was able to engage with both American and European perspectives on a variety of topics central to international affairs. He is particularly interested in the digital transformation of governments and the impact of open data on public policy.

About the Digital, governance and sovereignty Chair:

Sciences Po's Digital, Governance and Sovereignty Chair's mission is to foster a unique forum bringing together technical companies, academia, policymakers, civil societies stakeholders, public policy incubators as well as digital regulation experts. Hosted by the School of Public Affairs, the Chair adopts a multidisciplinary and holistic approach to research and analyze the economic, legal, social and institutional transformations brought by digital innovation. The Digital, Governance and Sovereignty

SciencesPo
CHAIR DIGITAL, GOVERNANCE AND SOVEREIGNTY

Chair is chaired by **Florence G'sell**, Professor of Law at the Université de Lorraine, lecturer at the Sciences Po School of Public Affairs.

The Chair's activities are supported by:

sopra steria next

Caisse des Dépôts GROUPE