FILOZOFIA I NAUKA
Studia filozoficzne i interdyscyplinarne
Tom 10, zeszyt specjalny, 2022

Christoph M. Abels, Daniel Hardegger

PRIVACY AND TRANSPARENCY IN THE 4th SPACE: IMPLICATIONS FOR CONSPIRACY THEORIES

doi: 10.37240/FiN.2022.10.zs.8

ABSTRACT

This article investigates the role of privacy and transparency in the 4th Space and outlines their implications for the development and dissemination of conspiracy theories. We argue that privacy can be exploited by individuals and organizations to spread conspiracy theories online, while organizational transparency, intended to increase accountability and ultimately trust, can have the adverse effect and nurture conspiracy beliefs. Through the lens of the 4th Space concept, we offer suggestions on how to approach those challenges which emerge as a result of the complex entanglements of both actual and virtual world across time.

Keywords: Transparency, privacy, disinformation, conspiracy theory, 4th space.

1. INTRODUCTION

With great power comes great responsibility. Although that saying holds true for many circumstances, it oversimplifies several aspects that defines the relationship between power and responsibility. Consider this question: if someone has the power to do everything he or she wants, what constrains that person in exploiting this power for solely selfish purposes? The implicit premise of the power-responsibility-relationship points to personality as a constraining factor, which works for some traits (e.g., honesty-humility), but not for others, e.g., the dark triad, consisting of Machiavellianism, Psychopathy, and Narcissism, that tends to make power exploitation more likely (Lee et al., 2013).

Aside from this, fear of social punishment might serve as a strong inhibiting factor. If powerful individuals consider other people's judgements important and fears reputational damage (or worse), they might restrain themselves from behavior that elicits contempt and subsequently social exclusion. However, if no one ever knows about certain acts or these cannot be

attributed to a specific individual, social punishment is of no concern. Beyond that, being able to conceal one's actions can even constitute a source of power, as the individual is no longer bound to normative expectations and civility, if the fear of punishment was the only thing that restrained the individual.

In the virtual world as well as the 4th Space, this power comes from the absence of attribution. When no one is able to link your online behavior to your offline identity, you are free to do whatever you want online without the fear of being punished, either legally or socially, for your misbehavior. In the actual world,[1] being able to avoid public scrutiny is seen as enabling corruption in government and corporate misconduct. However, there are reasons to obscure an individual's identity, e.g., to avoid governmental harassment in autocratic regimes. Privacy, obscuring an individual's identity, can therefore be understood as a protective layer against powerful actors allowing freedom from undue interference (Floridi, 2016). In contrast, organizations like governments and corporations are inherently more powerful than a single person. Although there are reasons for secrecy in these organizations, e.g., to allow policymakers to discuss policy solutions in private before going public, safeguarding the effectiveness of criminal investigations, or protecting trade secrets (Bok, 1989), overall organizations deserve a higher degree of scrutiny.

For governments, transparency seems inherently justified, as they are both politically accountable to their citizens as well as financially dependent on them. Helen Darbishire (2010), for example, points out that every piece of information held by public bodies should be freely accessible to all citizens, as it was created using taxpayer funds. In this context, subjecting governments to transparency-based oversight therefore seems warranted. That, however, is not sufficient. Archon Fung and David Weil (2010) argue that private sector corporations potentially also pose great risk to individuals—ranging from product safety to housing prices, mortgage rates, and "even the very soundness of the economy" (p. 109). Transparency should therefore be understood as a method to protect citizens, or help citizens to protect themselves, from these organizations.

However, in the context of conspiracy theories, both privacy and transparency can have adverse effects. As mentioned above, privacy may make people behave in a way they would normally refrain from if their behavior was on public display. Outrageous conspiracy theories might only be disseminated if the individual can be certain that it will not impact his or her offline identity, especially when the theory involves drastic accusations and includes behavior which may be strongly condemned by society. Privacy also

[1] Subsequently, we use the term "actual world" to refer to the physical space, in contrast to the virtual world that can only accessed through a device. See Wideström (2020) for a conceptual discussion.

allows foreign governments to spread propaganda or promote conspiracy theories that help their own agenda (Bok, 1989). While governments have employed these tactics at least since the early 20th century (Aaronovitch, 2010; Rid, 2020), the internet provides them with unparalleled access to citizens of other countries, and subsequently opportunities for influence operations.

For transparency, the situation is a bit more complicated. Transparency itself does not necessarily feed into the development and dissemination of conspiracy theories—how its results are used does. For governments, transparency is established through the publication of information, either proactively or via Freedom of Information (FOI) requests. Disclosure laws and regulations demand corporations to provide financial and operational information.[2] Frequently, however, whistleblowers and investigative journalists are exposing government and corporate misconduct and, eventually, induce change.[3] Given that some individuals already think that most political and corporate leaders are corrupt, working against the public interest and only concerned with their own political success, these incidents–often accompanied by large-scale media reporting and public debate, including references to past scandals–substantially feed into and bolster their mistrust. Empirical evidence indicates that people with a conspiracy predisposition, i.e., those being more likely to believe in conspiracy theories, name both "corporations and the rich" as well as, among others, governments as those "likely to work in secret against the rest of us" (Uscinski, Parent, 2014, p. 82). Additionally, as Joseph Uscinski and Joseph Parent found, people with a strong conspiracy predisposition also tend to have little trust in the government. Consequently, government and corporate misconduct fits into these people's overall image of the world: those in power will exploit us, and there is a strong body of evidence to support such claims.

The actual and virtual world reinforce each other in this respect–those who are already convinced that there are large ongoing conspiracies can go online to discuss their beliefs and further spread conspiracy theories, knowing that they do not have to fear any repercussions offline, as that their offline identity is protected through the veil of privacy. Those, however, critical about powerful organizations, might be tempted to initially engage in discussions about potential conspiracies, driven by the reporting about misconduct they encounter offline.

This complex web of interactions between actual and virtual world can be investigated through the lens of the 4th Space, which provides an analytical approach that incorporates an individual's simultaneous presence within

---

[2] The Sarbanes-Oxley Act, for example, which was enacted in 2002 after a series of major corporate and accounting scandals in the early 2000s (e.g., Enron and WorldCom), as a measure to increase the transparency of public corporations in the United States. For a summary, see Ivy Zhang (2007).

[3] For an overview of various corruption scandals, see Transparency International (2019).

a community in the actual world (e.g., a bar) and one that exists in the virtual world (e.g., Facebook), whilst also acknowledging the role of time in the interaction between these worlds (Hardegger, 2022). For example, while environments in the actual world are more likely to engage in a fact-based discussion, given the fear of social punishment for spreading falsehoods, there is little that prevents individuals from disseminating even the most outlandish claims imaginable online (Abels, 2022). In 4th Space communities, the costs of changing identities can be rather small, as individuals, e.g., can set up multiple accounts and drop those that are no longer able to gain the trust of fellow discussants.

The 4th Space understands today's information environment as a strong entanglement between an offline and online setting (actual and virtual world), along the lines of what was outlined by Zeynep Tufekci (2017), namely that "an internet society differs in significant ways from a pre-internet society, and this affects all members of that society, whether a person uses the internet or not" (p. 117). In this sense, the 4th Space provides an environment which addresses the concealment of information and its implications for the advancement of conspiracy theories in both environments.

Subsequently, we discuss the role of privacy and transparency in the 4th Space and investigate how both can nurture conspiracy theories. Starting with a brief introduction of the 4th Space, we describe the concept's elements and how it can be used to analyze interactions between the virtual and actual world. Afterwards, we contrast privacy and transparency and illustrate their role for the emergence of conspiracy theories. We conclude this paper by offering an outlook on further research questions.

2. THE 4th SPACE

The 4th Space is an inter- and transdisciplinary concept that provides an analytical approach for the analysis of the (emerging) hybrid society and communities.[4] It entails a methodological basis that allows to analyze and discuss how individuals and communities transcend between the actual and virtual world as well as how they interact with and among each other.

The 4th Space builds upon other concepts of community places, especially Ray Oldenburg (1989), Robert D. Putnam (2000), and Arnault Morisson (2019). Oldenburg, and subsequently Putnam, established the concept of the first, second, and third place. The first place represents an individual's home, the second its workplace. The third place, however, is the anchor of a community. It is "where you relax in public, where you encounter familiar

[4] For conceptual discussions of inter- and transdisciplinarity, see Bernard Choi and Anita Pak (2006) as well as Julie Klein (2008).

faces and make new acquaintances" (White, 2018). In his article *A typology of places in the knowledge economy: Towards the fourth place* Morrison further develops Oldenburg's concept by creating the fourth place. He argues that the knowledge economy is blurring the lines between the formerly separated places and, by doing so, establishes a fourth place that merges the other places in different configurations (Morisson, 2019).

The 4th Space concept, however, goes beyond Morisson's considerations by incorporating communities (and societies, which are constituted by the sum of communities) that emerge within and/or expand into the virtual world. These communities differ in various characteristics from (solely) actual world communities as they are not bound to a location within the actual world. Additionally, they are influenced by developments and interactions in actual and virtual world, and simultaneously influence these worlds through their individuals and/or organizations that are both present within the community. Conceptually, the 4th Space can be understood as a three-dimensional space. Each axis not only represents factors that influence and define the 4th Space but are also constitutional for the communities that emerge within this space. The three different factors are place, medium, and time.

The x or place-axis represents the most direct connection of the actual world into the virtual space and vice versa: Every individual who enters the virtual space is, in parallel, still anchored to a place in the actual world. The impressions and influences of the actual world are being taken into the virtual space and affect it through interactions of the individual with content and other individuals. Additionally, individuals' impressions of this virtual environment are also influencing the places these individuals are located in the actual world.

The medium, represented by the y-axis, is required to enter the virtual world. This includes both technical aspects, hardware and software. The medium creates heterogeneous experiences among individuals, due to software and hardware differences (e.g., accessing a community using a mobile phone in difference to a laptop or desktop computer) as well as small variations in their settings within their medium (e.g., screen brightness, adjustments of buttons, or the haptic experience that is perceived differently based on varying hand sizes of the medium's users).

The z-axis represents time. Each piece of content that is being created, amended, shared, or added, each interaction that is happening among individuals, as well as everyone that is present is doing so within a certain time (frame). Time includes the actual time as well an individual's perception of time, hence it includes the relativity of time as well. Furthermore, individuals differ in their perception on time, depending on their location as well as personal experience and expectation of time as factor.

3. PRIVACY & TRANSPARENCY

According to the Meriam-Webster Dictionary, something is transparent if it is "easily detected or seen through" or "characterized by visibility or accessibility of information especially concerning business practices."[5] Transparency therefore allows us to investigate the inner workings of a system or an organization. In personal affairs, this transparency is frequently avoided, as individuals want to hide certain aspects of their lives from the public (although the aspects an individual wants to hide depend on the individual itself). This privacy can be understood as "someone's right to keep their personal matters and relationships secret."[6] Frequently, transparency is discussed in the contexts of organizations, such as governments or corporations, while privacy addresses the individual level.

In the following section, we will point out how privacy and transparency are realized in the 4th Space. Starting with privacy, we illustrate how privacy differs in both virtual and actual world and how the concept of anonymity has changed online. Afterwards, we discuss the concept of transparency for corporations and governments, before relating both concepts to the 4th Space.

3.1. Privacy

It is an individuals' right to keep certain personal information concealed from the public and therefore prevent others from interfering in personal matters. Hence, it can also be seen as freedom from interferences and intrusion, as indicated by the Merriam-Webster definition.[7] Four kinds of freedoms can be distinguished in this respect: physical privacy, mental privacy, decisional privacy, and informational privacy (Floridi, 2016). These freedoms refer to the absence of interference or intrusion in a person's physical space, mental life, decision making, and information made accessible to the people. Luciano Floridi, however, points out that these freedoms are often intertwined, yet should be treated separately.

Lawrence Lessig (1999) takes a different approach to privacy. For him, privacy is that part of life that that is left over once everything that can be monitored (e.g., that others see or is noticed by them) or searched (all activities that create a searchable record) is subtracted. Being monitored is normal in everyday life—we are, for example, observed by other people on the streets, by security cameras, or by our neighbors. Although, our neighbors

---

[5] Merriam-Webster, *transparent*; https://www.merriam-webster.com/dictionary/transparent, accessed on 23 February 2022.

[6] Cambridge Dictionary, *privacy*; https://dictionary.cambridge.org/de/worterbuch/englisch/privacy, accessed on 23 February 2022.

[7] Merriam-Webster, *privacy*; https://www.merriam-webster.com/dictionary/privacy, accessed on 23 February 2022.

might see us at the grocery store, they rarely remember what we bought, who we talked to, or how much we eventually paid. To them, our actions are ephemeral and will not result in a lasting record.

In the face of the beginning digital transformation, Lessig argued that "we are entering an age when privacy will be fundamentally altered" (Lessig, 1999, p. 57), given that the extent to which we are monitored and information about us is becoming searchable is far greater than ever before. When shopping online, our internet provider tracks our activity, the online shop monitors what we are looking at and what we eventually bought, and the credit card company has a record of all our purchases, including the exact date and time at which we used the card. All this information is searchable and, if combined with information from other sources, might allow the creation of a personal profile that can be sold to advertising companies. Accordingly, internet users are constantly tracked online, in many cases unnoticed by the users–they become transparent for advertisers and surveillance agencies, while the people monitoring remain concealed to the users.

However, one's privacy can be protected online by masking individuals' identities, making them anonymous, using different tools like proxy servers (hiding the user's IP address behind the address of the proxy), virtual private networks (VPN, creating a secure tunnel between the server and the user's PC), as well as The Onion Router (TOR, enveloping communication between a server and the user's PC in several layers of encryption), which offers the highest level of protection (Hoang, Pishva, 2014). Additionally, privacy can be achieved through end-to-end encryption (Winkel, 2003), as used by WhatsApp and other messaging services.

The reasons for individuals to remain anonymous differ: from enabling free speech in expressive regimes (Jardine, 2018) to the creation of cryptomarkets, illicit marketplaces based on cryptocurrencies (van Hardeveld et al., 2017). Accordingly, online anonymity can be a "double-edged sword," as whilst it offers protection to whistleblowers in autocratic regimes from repercussions, but also assists individuals in avoiding criminal prosecution (Sardá et al., 2019). While being anonymous on the internet can be justified, the use of privacy-enabling technology is frequently denounced. Use of the TOR network has publicly been singled out in this respect for being associated with criminality, "characterizing it as undesirable, immoral and illegal" (Sardá, 2020, p. 257).

The use of technology to conceal an individual's identity is only one way to remain anonymous on the internet. With the emergence of Web 2.0 and the widespread adoption of social networking sites (SNS), individuals became used to create online profiles that allow them to "actively construct a representation of how they would like to be identified" (Ellison, Boyd, 2013). While some contexts demanded a clear connection between online

and offline identity, e.g., online dating (Ellison et al., 2012), others where more lenient with their identification requirements. Privacy can therefore be achieved, in some contexts, by establishing pseudonyms.

Over the course of the last years, an increasing number of popular websites have dropped anonymity and added some form of identification, some websites like Twitter, Facebook, and Instagram focused on their connection to the real-life identity through various verification systems (e.g., credit card registration). Mark Zuckerberg even promotes an idea of "radical transparency," fundamentally providing the basis for marketers to identify and predict patterns as well as to track individuals online (Kirkpatrick, 2010; Knuttila, 2011). Reportedly, Zuckerberg even told an interviewer that "having two identities for yourself is an example of a lack of integrity" (Dibbell, 2010).

However, there is (at least) one prominent website that is fully commitment to keeping their users anonymous, and therefore serves as a case for how people use this anonymity online: the imageboard 4chan. Founded in 2003 by Christopher Poole, 4chan became known to a larger audience during the 2016 US election, where its users claimed to have "actually elected a meme as president" (Ohlheiser, 2016). 4chan's anonymity is by design; accounts don't exist, only an empty name field which users do not have to fill in and if a user decides to leave it empty, 4chan assigns the account name "Anonymous" (Bernstein et al., 2011). This anonymity "makes failure cheap—nearly costless, reputation wise" (Dibbell, 2010) and allows individuals to deviate from their normal behavior, allowing them to act in ways they would never do offline, as they "can be relatively certain that their actions will not come back to haunt them" (Bernstein et al., 2011, p. 55). In a 2010 interview with the New York Times, Poole explicitly stated that he frequently received emails thanking him for providing a place in which things can be said that wouldn't be discussed with friends or family members (Bilton, 2010). According to Poole, "people deserve a place to be wrong" (Dibbell, 2010, p. 84).

Although this anonymity can serve users' freedom of expression, the lack of long-term accountability comes at a price (Knuttila, 2011). 4chan has been involved in different scandals such as Celebgate and Gamergate, both instances of sexist transgressions of the community, as well as fake bomb threats and fake trends that have contributed to a resurgence in online eating-disorder communities (Dewey, 2014). Hate speech flourishes on 4chan's /pol/ (politically incorrect) forum, which prides itself on its fight against political correctness, as racist and bigoted content surges in the aftermath of violent attacks against specific community groups, such as the 2018 Pittsburgh synagogue shooting and 2019 Christchurch mosque attacks (Malevich, Robertson, 2020; Thompson, 2018; Zelenkauskaite et al., 2020).

4chan is furthermore seen by some scholars as the origin of conspiracy theories such as "Pizzagate" (Tuters et al., 2018). Pizzagate describes a con-

spiracy theory based on private e-mails belonging to Hillary Clinton's former campaign manager John Podesta, which were leaked by Wikileaks during the campaign phase of the 2016 US Presidential election. Users on /pol/ manufactured bogus claims about Podesta and other high-profile members of the Democratic Party being involved in a satanic pedophilia ring operated out of a Washington D.C. pizzeria. The conspiracy theory subsequently spread beyond 4chan to, among others, Facebook and Twitter as well as Turkish pro-government media outlets (Tuters et al., 2018; Wendling, 2016). This transition from 4chan to other SNS is no isolated incident (Zannettou et al., 2017). More recently, Pizzagate has re-emerged on TikTok, a SNS focused on short videos that has become popular since its 2016 launch and has a large global network of members, now including a variety of business, political and cultural elites, such as Bill Gates, Oprah Winfrey, and Ellen DeGeneres (Kang, Frenkel, 2020).

These examples illustrate the dark sides of privacy. While individuals have various legitimate reasons to protect their privacy online, e.g., to express their beliefs without fear of political oppression in autocratic regimes, some individuals use privacy, through means of anonymity, to disseminate hate speech and amplify conspiracy theories. This problem is not confined to 4chan with its focus on anonymity. Other SNSs such as Facebook, Instagram, Twitter and YouTube also struggle to contain the spread of disinformation. A number of SNSs enable users to register under a pseudonym, thus they are able to avoid being identified and held liable for their online behavior. And even if the account is banned, individuals are able to circumvent the ban by creating new accounts, although thereby violating Twitter's use policy (Twitter, 2020). The lack of accountability, that is associated with anonymously or pseudonymously posting content online, can therefore be seen as a reason for the surge of disinformation online.

3.2. Transparency

As previously stated, whilst privacy refers to the individual level, transparency is frequently discussed at the organizational level. In this respect, both concepts differ in their respective goals: with organizations frequently being more powerful than individuals, privacy protects individuals from those organizations, but also from the interference of other individuals, while transparency sheds light on the potential wrongdoings of these organizations. Accordingly, transparency can be seen as "the ability to look clearly through the windows of an institution" (den Boer, 1998, p. 105) while Albert Meijer (2009, p. 258) phrases it as "the general idea that something is happening behind curtains and once these curtains are removed, everything is out in the open and can be scrutinized". We will subsequently focus on two types of organizations for which transparency plays an important role, governments and corporations.

At the heart of the issue lies an inherent information asymmetry: government officials and corporate executives have direct access and control over the actions of their respective organizations, their assets and funds and other resources. From the perspective of principal agent theory, the principal (citizens, shareholders or stakeholders) delegate certain tasks to an agent who's interests either align with those of the principal, but frequently deviate from them (Jensen, Meckling, 1976). In these cases, the agent can exploit this information asymmetry for its own gains. This asymmetry holds for both relationships between citizens and the government as well as between corporate executives and shareholders (Stiglitz, 2002). This frequently results in corporate misconduct (Heath, 2009) and corruption, understood here as the misappropriation of state resources for the private gains of politicians and bureaucrats (Mungiu-Pippidi, 2006; 2013). Already in 1914, Louis Brandeis stated that "sunlight is said to be the best disinfectants; electric light the most efficient policemen" (Brandeis, 1914), making the case for transparency as an effective tool against those acting outside of the public eye. Establishing this transparency, however, comes at a cost, as measures need to be put in place to enable the principle to collect the necessary information that eventually makes the organization more transparent.

For corporations, transparency touches upon a variety of different areas– from financial disclosure to product safety requirements (Fung et al., 2007; Hermalin & Weisbach, 2007). Different approaches to corporate governance as measures to enable the principal to better control the agent have been developed (for an overview, see Anheier, Abels, 2020). Additionally, regulatory bodies and watchdog organizations take interest in corporate behaviour and data published by the corporations, adding an additional layer of corporate oversight. Still, in recent years there have seen a series of scandals that have revitalised interest in organisational transparency, e.g., the bankruptcy of financial service provider Wirecard (Barnert, 2021), various scandals related to privacy and mental health at Facebook (Vaidhyanathan, 2018), including the infamous Cambridge Analytica scandal (Granville, 2018), the crash of two Boeing 737 MAX that killed 346 people (Robinson, 2021) as well as the defrauding of customers and investors by the now defunct biotechnology company Theranos (Carreyrou, 2018). These examples illustrate the limits of transparency for corporate control, as frequently regulatory bodies fail to act upon their mandates and investigate problems, often with a human cost. In some cases, such as Wirecard, it was investigative journalists who disclosed the company's misconduct and prompted a broader investigation by German authorities (Storbeck, 2021).

While corporate scandals harm customers and shareholders, corruption of government officials can, aside from the immediate financial harm, damage citizens' trust in their leaders. In governments, transparency therefore serves as a constraint against corruption (Mungiu-Pippidi, 2015), but also as a way

to assess government performance (Stiglitz, 2002). Transparency is therefore often discussed in the context of government accountability. Yet, beyond that, access to information held by government or government agencies is increasingly seen as a human right, as an increasing number of constitutions and international courts have enshrined this right into treaties related to freedom of expression and information provision (Darbishire, 2010). To illustrate this development: at the time the Berlin Wall fell in 1989 only 12 countries had "access to information" or "Freedom of Information" laws (FOI), primarily in states with longer-established democracies (Darbishire, 2010). By 2019, 119 nations had implemented FOI laws (Feldman, 2019).

There are two ways on how the public can access information held by public institutions. Citizens can either submit requests for information (reactive disclosure) under FOI laws, or access via those institutions which proactively publish information without such requests. The result of this proactive disclosure is proactive transparency, which makes it more complicated for officials to manipulate information. Proactive transparency is especially effective in authoritarian regimes, where citizens lacking the necessary power to protect themselves from government misconduct or worse, might otherwise unable to request information which might expose vested interests of certain actors (Darbishire, 2010).

However, processes such FOI do not necessarily produce more actual transparency. As Hood (2007) points out, if politics and bureaucracy show a certain orientation for blame-avoidance, behavioral patterns can be observed that create circumstances in which different strategies are employed to limit the blame actors can receive, frequently with negative consequences for transparency. In the face of intentional maneuvering of bureaucrats and politicians to avoid blame by, among other approaches, reducing the degree of transparency through means such as unintelligible records of meetings (e.g., in form of PowerPoint presentations), telephone calls, or in person discussions that are not recorded at all (Hood, 2007), citizens who expect the state (elected politicians and bureaucrats) to work to increase their quality of life might end up frustrated and lose trust in their leadership. Furthermore, if bureaucrats choose to sabotage initiatives that would increase transparency and thereby accountability, it is unsurprising if citizens want to know what accountability these bureaucrats seek to avoid–and subsequently assume the worst.

3.3. Privacy and Transparency in the 4th Space

Privacy and transparency have several implications for the 4th Space. The means through which individuals enter the virtual world, the medium, remain largely opaque to many users—they lack, for example, the technical expertise to fully understand the device they use, how the software works,

who might be able to eavesdrop, and what data is collected. Accordingly, their degree of privacy differs substantially dependent on their understanding of the respective technology, which is in many cases superficial at best (Park, 2013). As a result, individuals might expect their privacy to be more strongly protected than it *de facto* is. In respect to anonymity, as a measure to establish privacy, expectations about the absence or presence of anonymity or pseudonymity might also differ from the situation individuals encounter in the communities they engage in. While some communities have implemented means to verify one's true identity, e.g., credit card registrations, others lack these approaches, despite existing platform policies that suggest the need for identity verification processes. Figure 1 illustrates these deviations.

Anonymity allowed by platform provider	Anonymity expected by platform user: Yes	Anonymity expected by platform user: No
Yes	4chan Discord Reddit Twitter	LinkedIn
No	Facebook	Tinder

Figure 1. Differences in expected and allowed privacy in online communities

On Facebook, for example, given its policy that demand registration with one's true name (Facebook, n.d.), individuals might expect every account on the platform to be connected to a similar identity in the actual world. However, there is little enforcement of the policy by Facebook, allowing individuals to use pseudonyms without disclosing this to other individuals. As a result, Facebook users must maintain a certain situational awareness when engaging with others on the platform, given that the lack of long-term accountability associated with pseudonymity can increase the chance of encountering individuals with potentially malign intentions, e.g., to spread conspiracy theories and spreading disinformation or engaging in cybercrime. On Twitter, however, as the self-ascribed "free speech wing of the free speech party" (Halliday, 2012), individuals cannot expect fellow users to disclose their actual world identity. Still, Twitter, among other SNS, has introduced a verification check for "accounts of public interest," e.g., journalists, government officials, and prominent persons, to increase the trust between users (Twitter, n.d.). However, this does not address the issue of

manipulation, as this only helps to identify those individuals which may want to be identified. Online dating sites, such as Tinder, have struggled for a long time with fake user profiles and being used for online scams (Drouin et al., 2016; Murphy, 2016).

Time and engagement might furthermore implicitly increase the vulnerability towards manipulation attempts: the more information about a person becomes public, due to a lack of privacy or misunderstandings about the identity of other members in a community, the easier it is for malicious actors to exploit this information for manipulative or harmful purposes. This has been, for example, seen in recruitment efforts for ISIS (Callimachi, 2015), but also fraudulent online dating scams (Whitty, Buchanan, 2016). While time might lead to an unnoticed accumulation of information that allow for an identification of a person, this information can also be intentionally made public by others. This so called "doxing", understood as the unvoluntary disclosure of private information by a third party, can concern information related to a person's identity, location, or supposedly immoral activity (Douglas, 2016). Depending on its purpose, doxing can be "a tool for establishing accountability for wrongdoing, a means of intimidation and incitement to cause harm, and a way of silencing minority or dissenting views" (Douglas, 2016, p. 209). From the perspective of the 4th Space, doxing bridges the gap between the actual and the virtual world (involving all three axes, medium, place, and time), thereby negating any individuals' attempts for privacy protection.

Additionally, an individual's location (the place axis) can impact the relevance of understanding and protecting their privacy. Depending on political (autocracy vs. democracy) and cultural (liberal vs. conservative) contexts, some opinions can only be safely expressed or information obtained when one's true identity remains unknown. Correspondingly, in oppressive autocratic regimes, privacy might be a question of mitigating the potential for physical harm when speaking out against the government, yet sometimes virtual environments may simply offer a space for discussions on topics that are otherwise off-limits due to cultural sensitivities wherever an individual is situated, e.g., discussing marital issues or homosexuality in China (Wang, 2013). These social norms are highly context dependent, sometimes with differences within a country (e.g., abortion in rural and urban Germany) or between neighboring countries (e.g., assisted suicide in the Netherlands or France) and illustrate how physical location impacts the role of virtual communities that allow a certain degree of privacy for the free expression of thoughts (Tufekci, 2017). As a result of individuals being present in both the virtual and the actual world, transparency of governments and corporations also impact their perception of the actual world, which can spillover into the virtual environment.

4. CONSPIRACY THEORIES

Privacy and transparency can be seen as two sides of one coin: Privacy allowing individuals to act in concealment, transparency lifting that veil behind organizations could hide their actions. Both concepts therefore are related to the idea of secrecy–an important element of many definitions of conspiracy theories. Accordingly, Cass Sunstein and Adrian Vermeule (2008) define them as "an effort to explain some event or practice by reference to the machinations of powerful people, who have also managed to conceal their role" (p. 4). Brian L. Keeley (1999) focusses on the agents causing the event in question, seeing a conspiracy theory as "a proposed explanation of some historical event (or events) in terms of the significant causal agency of a relatively small group of persons–the conspirators–acting in secret" (p. 116).

However, definitions of conspiracy theories can also highlight their explanatory role. They can be understood as any explanation of an event that invokes a conspiracy as its cause (Dentith, Orr, 2018) or, in the sense of David Aaronovitch (2010), as "the attribution of deliberate agency to something that is more likely to be accidental or unintended" (p. 6). He furthermore expands his definition by arguing that the secret actions of the persons identified by the conspiracy theory as perpetrators are more reasonably explained by those that had overtly acted.

The conspirators themselves are also subject of debate. According to Keeley (1999), the group causing the event does not need to be powerful, its pivotal role is sufficient. But, given the limited power of conspirators, secrecy is needed to execute the conspiracy: If they would act in public, their plans would be obstructed by others. In the face of the pivotal role many conspiracy theories assume, a single person is frequently not enough for a conspiracy. Hence, as Matthew Dentith and Martin Orr (2018, p. 441) point out, a conspiracy is a social relationship–although fragile one, in which there is "a potential leaker, a potential whistleblower, and a potential turncoat."

In the following section, we discuss how transparency can advance conspiracy theories. Afterwards, we highlight the role of the 4th Space as an analytical framework to investigate these theories.

4.1. The role of transparency in advancing conspiracy theories

Communities in which conspiracy theories flourish are paradoxical: While some of the actors make outrageous claims that probably do not seem believable to most persons, fellow conspiracy theorists in many cases do not seem overly concerned with the validity of these claims. Although these people do

not trust the government and do not trust those attempting to debunk conspiratorial claims with evidence, they still believe in what are frequently unwarranted theories about covert agents acting against the common good. If their distrust is high enough to consider almost everything to be a conspiracy theory, except those theories most worthy of that description, why do they trust an anonymous person in an opaque virtual environment?

Government transparency may be one of the reasons. As several authors have pointed out (Fung, 2013; Margetts, 2011), making governmental action transparent, especially for the sake of accountability, might lead citizens to focus on missteps, policy failures, and corruption, in a manner that Fung and Weil (2010, p. 106) call "gotcha game." Citizens are actively looking for failures of those in power and feel confirmed once they found something. Some of the conspiracy communities, truthers, even refer to themselves explicitly as those that look behind the curtain and expose what is concealed by the government (Kay, 2011). As Bok (1989) has pointed out, secrecy–understood as the result of concealment—is strongly linked in many people's minds with deception. Beyond that, the idea frequently prevails that secrecy itself is discreditable, as people only conceal what they find "shameful or undesirable" (p. 8). Trying to expose the secrets governments hide from the people is therefore a value in itself, as only that is concealed which is diametral to the greater good of society.

With an ever-growing number of leaks from whistleblowers–Panama Papers, Pandora Papers, Paradise Papers, and very recently Suisse Secrets–conspiracy theorists can easily feel vindicated in their believe about widespread corruption of those in power. As evidenced by the recent Suisse Secret leaks, that shed light on one of the world's most important financial institutions, the Credit Suisse bank, there indeed is a powerful elite, ranging from the son of an Azerbaijani strongman, Egyptian intelligence officials, to various wealthy criminals, that is protected by laws and catered by institutions that both support and profit from them (OCCRP et al., 2022). Decades earlier, Tobacco corporations were either deliberately concealing or at least whitewashing the negative health consequences of smoking (Rabin-Havt & Media Matters, 2016). These are only some examples that illustrate the large number of scandals involving governments or corporations. Jointly, these incidents can undermine public trust and lead people in the hands of those sharing and subsequently nurturing their mistrust.

As a result, although transparency should make governments more accountable to the public, and through this accountability increase trust in their doings, the opposite can be the case, if transparency focusses public attention on misconduct by government officials. In the private sector, transparency can uncover criminal or norm-violating behavior, e.g., environmental pollution, corruption, customer endangering. In combination, both mechanisms can reinforce individuals' perception of powerful actors,

being it government or corporate leaders, frequently engaging in behavior that is in direct opposition to the public good.

4.2. The 4th Space as analytical framework for virtual conspiracy communities

Conspiracy theories seem to accompany humanity through its history. As Uscinski and Parent (2014, 3) point out, "naturally, conspiracy theories flourish across space just as much as they do across time." Yet, while they seem to be ever-present–from the antisemitic *Protocols of the Elders of Zion* in the 20th century (Aaronovitch, 2010) to the recent conspiracy theories involving the Covid-19 pandemic (Uscinski et al., 2020)–times of anxiety, paranoia, and a perceived loss of control in large parts of society seem to be the ideal environments for conspiracy theories (Douglas et al., 2019; van Prooijen, Douglas, 2017).

Hence, conspiracy theories largely appear to be a response to a state of crisis. However, today's information environment allows actors to spread conspiracy theories for other purposes, e.g., because enjoy doing it (Buckels et al., 2014) or engage in state-sponsored disinformation operations (Rid, 2020). A substantial driver of this are virtual communities, in which individuals can encounter conspiracy theories and discuss them with like-minded others.

The 4th Space offers an analytical framework to investigate these encounters. Starting with the medium, individuals have a great choice of virtual communities they can engage with to exchange views on conspiracy theories and encounter new ones. From Facebook to Twitter and TikTok, in simple terms, every SNS proffers content that promotes conspiracy beliefs. Individuals can therefore not only engage with one community on a single platform but can be part of several discussions across platforms, thereby exchanging content between platforms. This is frequently seen on WhatsApp and Telegram, where links to YouTube and other Websites are shared. Given that not every individual is present on the majority of SNS, through this interconnection of virtual communities these individuals are still likely to encounter the most prominent conspiracy theories.

In the 4th Space, individuals are however not only exposed to information from the virtual world, as the remain anchored through their location in the physical world. Given conspiracy theories are oftentimes explanations for significant historical or political events, individuals are likely to discuss those events with their immediate social environment—at work, home, or in bars and restaurants, talking with their friends and family. Yet, as these individuals can be simultaneously present in their virtual communities, discussions from the actual world can migrate to the virtual one and vice versa. Assuming that the belief in conspiracy theories is by many seen as a deviation from normal behaviour—some authors even view conspiracy

belief as pathological (Hofstadter, 1965)—individuals might refrain themselves from disclosing their true beliefs about certain events, due to the fear of being socially stigmatized or excluded. The privacy of the virtual space can provide the necessary safety to freely articulate their views.

Location can also have a direct impact on the information entering the virtual space. Proximity to sites of emergencies can increase the quality of information shared online (Starbird, Palen, 2010; Thomson et al., 2012). The opposite was observed in New York City after the attacks on the World Trade Center: residents in the city strongly believed that the government knew about the attack in advance and failed to act, while this belief was less prevalent in the rest of the US (Sunstein, Vermeule, 2008).

If these individuals now encounter a government or corporate scandal, they can discuss the matter with their immediate environment in the virtual world, maybe also just learn about them from friends and family, and carry it over to their virtual communities. In these communities, they can then elaborate on the underlying causes of the scandal and investigate what the media, which frequently uncovers these scandals, has (deliberately) left unreported. Yet, their beliefs might remain concealed to both their actual social environment and the virtual one.

The 4th Space's third component, time, underlines the role of technological progress, the durability of conspiracy theories, and their long-term impact. As Uscinski and Parent (2014) point out, some individuals might be socialized into a worldview that has a stronger emphasis on conspiratorial thinking. One driver of that is today's presence of the high-choice media environment. While it was difficult in the past to encounter media that caters to certain ideologies and reinforces them, individuals can nowadays choose the media outlet that suits their ideological preferences best (Van Aelst et al., 2017). Additionally, with an increasing lifespan, individuals are also potentially more likely to experience a conspiracy.

Virtual environments furthermore make discussions less ephemeral. Conversations at work or in a bar do normally not leave a record.[8] On Facebook or Twitter, for example, every discussion and exchange with other users create a searchable record, until the users decide to delete it. However, even then, other users might have made a screenshot of the conversation and uploaded it to a Cloud server. Even in communities that are deliberately designed to be ephemeral, like 4chan, users can easily create copies of that conversation and therefore expand its lifespan.

[8] Sometimes, however, discussions might be recorded, intentionally or unintentionally. Yet, this is not what most people would expect nor how most situations are set up.

5. DISCUSSION

These examples show the complex web of interconnections between place, medium, and time that constitutes the 4th Space. They furthermore indicate how the 4th Space can be used as an analytical framework to investigate the implications of these interdependencies for the development and dissemination of conspiracy theories.

Beyond that, the 4th Space can be used to identify solutions to cope with the problems identified in this article. As already mentioned, there is little understanding of technology—the medium—on the part of the users who move, exchange, and create or use content in 4th Space. If, for example, users acquire a new hardware or software currently in use receives an update, they might be unaware of the impact on their privacy. This is understandable, as the speed of technological changes, especially in software, might overwhelm most users and pose an enormous task even for the more experienced ones. Nevertheless, it must be emphasized that a fundamentally better understanding of the necessary technology in the 4th Space and the impact on the user's experience within the 4th Space, especially regarding privacy, would also likely create more trust in the interaction.

The medium's affordances play a crucial role in this respect. For instance, as users can have multiple accounts in a certain 4th Space, the general idea of "one body, one identity" (Donath, 2020) does not apply in that specific environment. If these users are not aware of this or policies exist that create the illusion that every online persona is connected to a similar offline one, although the policy is not enforced (e.g., as it is frequently the situation on Facebook), users might be misled in their interaction with other individuals about their true identities. This makes it more difficult to identify incorrect information or even targeted false messages, as users' experiences on online dating sites make clear (Rege, 2009). To counteract this, virtual communities should incorporate design features that make the state of privacy policies more salient and support the situational awareness of their members. In the context of Covid-19-related disinformation, several SNS have added labels and other warning mechanisms to their platforms in order to protect individuals from falling for misleading information (Bond, 2020). A similar approach could be taken to increase an organization's transparency in relation to when and how they enforce existing privacy policies.

In the context of conspiracy theories, the role of anonymity, as a tool to establish privacy, needs to be discussed as well. Every 4th Space can be divided into one of three categories: full anonymity, partial anonymity, and no anonymity. The former category includes 4chan, where no registration of any kind is expected and the users themselves respect the anonymity and thus the privacy of others. On the contrary, any kind of connection to the actual world would ultimately undermine the basic idea of the 4th Space

that 4chan creates. At the same time, this also means that a user must take any information and interaction within the respective community with a grain of salt. The second category, partial anonymity, includes 4th Spaces such as reddit or Twitter. These require a registration for the interaction in them and thus also the deposit of corresponding data, such as a mail address. But there is no obligation to verify the actual world identity, and every user can create and use an unlimited number of accounts. Just as with 4chan, every user of these 4th Spaces must assume that here, too, every piece of information does not necessarily have to correspond to the facts. The last group, those that do not guarantee anonymity and want to combine the actual world identity with the virtual world identity, includes Facebook and LinkedIn. While the latter merely carries this claim with it, at least Facebook is also trying to enforce it legally, albeit not successfully. In the case of Facebook, this leads to the paradoxical situation that the platform's affordances tend to signal users to assume that most information on Facebook comes from real people and organizations, thereby creating the impression of accountability for the spread of misleading information, but at the same time claim to be allowed to remain anonymous. However, given that reality distortion might be the norm online, the mere perception of a user being who he or she claims to be is not enough to take the validity of information for granted (Zimbler, Feldman, 2011).

On the place axis, the situation is more complex. Privacy and transparency are not merely technical matters, but subject to legal, cultural, linguistic, and other factors. For instance, whether privacy is perceived as valuable depends on the individual's location. Privacy is certainly more helpful in oppressive autocracies, in which exercising free speech might pose an immediate threat to individuals well-being. Transparency of government and corporations also differs across countries, as some nations, although enacting FOI laws, have little interest in becoming more transparent. This difference between *de jure* and *de facto* transparency has been the cause for the development of new indicators to assess a government's objective level of transparency (Mungiu-Pippidi, Dadašov, 2016). Beyond that, whether the information provided by a government can be used to hold it accountable depends on the existence of civil society actors capable of analyzing the data and advocating for change (Fung, 2013). The same is true for corporations, as misconduct is frequently exposed by investigative journalists, e.g., in the case of Theranos, which has defrauded customers as well as investors (Carreyrou, 2018).

However, the push towards good governance through transparency can be act as a double-edged sword: although transparency can achieve greater trust in government and bureaucracy, repeated exposure to strategies to undermine these initiatives can have a lasting negative impact on trust in government, potentially increasing the likelihood of citizens to adopt conspiracy theories. In combination with large-scale leaks from whistleblowers

that expose the wrongdoings of powerful elites, a generalized mistrust towards anyone in power can be the result, providing fertile ground for conspiracy theories to flourish.

At the same time, also in contrast to the medium axis, individuals in some locations tend to have greater awareness of the importance of privacy and transparency, since the connection to the actual world of the respective users is much more direct here. Accordingly, there is a more reflection on the role of privacy and transparency in the 4th Space. Nothing illustrates this better than the debate surrounding the General Data Protection Regulation (GDPR), which was ultimately not a technical discussion, but a transfer of the European self-image of privacy and transparency into the 4th Space (Greenleaf, 2012). This underlines that the 4th Space is not limited to a single, clearly defined geographic area, but encompasses every place where users log in. Accordingly, different legal concepts of privacy and transparency from the actual world, but also socio-cultural, linguistic, economic, and religious ones compete in the 4th Space, each depending on the individual background of the users and the location in which they are located.

For example, a 4th Space may be primarily used by users and hosted by an organization from North America and Europe. However, as soon as a user from a completely different region, such as South Africa, enters and becomes part of the 4th Space, their respective definitions of privacy and transparency also become part of it, thus expanding the 4th Space on the place axis accordingly. At the same time, however, this user is also influenced by the already existing definitions of privacy and transparency within the 4th Space, which again impacts the individuals' actual world environment.

Which brings us back to the medium axis. Because even if legal and societal changes in the understanding of privacy and transparency in the 4th Space are possible, corresponding adjustments and improvements are also necessary on the technical and design level. It would, e.g., make sense on the part of those who are technical responsible for the respective 4th Spaces to create the possibility of more clearly tracing the development of information and discourse within the community. 4th Spaces such as Reddit and Twitter are less prone to be undermined by conspiracy theories, since here, a) the history of discourses can be tracked more directly, b) the community itself actively evaluates and shares information, and c) individuals know that there is no requirement of connecting the actual world to the virtual world identity, so they usually take every information with the required skepticism (Cinelli et al., 2021; Theocharis et al., 2021).

Our remarks here pose several questions that deserve further investigation. Concerning the medium, the issue of privacy might evolve over the course of the next years, given technological developments around deepfakes, manipulated multimedia content (Chesney, Citron, 2018; Verdoliva, 2020), and Facebook's so-called Metaverse. Through deepfakes, individuals

can, for example, alter videos about themselves to conceal their identity from others while pretending to show their true self. In the Metaverse, the increased degree of interaction, including virtual avatars that represents a person's behavior more directly, might alter privacy, as it is easier to observe patterns of behavior, speech, and other aspects that are more difficult to obscure. Accordingly, how these thinner privacy affects the spread of conspiracy theories in the Metaverse should be subject to future research.

Beyond that, further research is needed to investigate how conspiracy theories move from the actual world to virtual communities and vice versa. Although it is arguably more likely that individuals discuss these issues online, there is an increasing number of examples in which virtual communities around disinformation reach over into the actual world–the Querdenker movement in Germany, which largely organizes itself via Telegram and other platforms, is only one of the more recent examples (Koos, 2021). Other instances include Pizzagate (Tuters et al., 2018) and the storm on the US Capitol on January 6, 2021 (Barry et al., 2021).

Finally, the question of how government transparency can lead to the emergence or advancement of conspiracy theories demands further attention. While it seems intuitively convincing that the gotcha game (Fung, Weil, 2010) can lead to the emergence of conspiracy beliefs, as information are interpreted in the face of pre-existing beliefs and attitudes (Miller et al., 2016; Taber et al., 2009) and subsequently twisted and turned to fit into conspiracy beliefs (which is what happened in the case of Pizzagate on 4chan), the literature has so far hardly addressed this issue.

The 4th Space provides a holistic framework to analyze and combat the spread and development of conspiracy theories, by incorporating aspects of place, medium, and time. Following the Swiss Cheese model to mitigate disinformation online (Bode, Vraga, 2021), the 4th Space framework can help us to identify the relevant protective layers and allow us to shed light on the man or woman behind the curtain.

REFERENCES

D. Aaronovitch, *Voodoo Histories: The Role of the Conspiracy Theory in Shaping Modern History*, Riverhead Books, New York 2010.

C. M. Abels, *Everybody Lies: Misinformation and Its Implications for the 4th Space*, Proceedings, 68, 2022, in press.

H. K. Anheier, C.M. Abels, *Corporate Governance: What Are the Issues?*, in: Advances in Corporate Governance: Comparative Perspectives, H. K. Anheier, T. Baums (eds.), Oxford University Press, Oxford 2020, pp. 10–42.

J.-P. Barnert, *Wirecard Chapter Ends With Stock Set to Delist From Exchanges*, Bloomberg, 2021; https://www.bloomberg.com/news/articles/2021-11-12/wirecard-chapter-ends-with-stock-set-to-delist-from-exchanges; accessed 03 March 2022.

D. Barry, M. McIntire, M. Rosenberg, *"Our President Wants Us Here": The Mob That Stormed the Capitol*, The New York Times; https://www.nytimes.com/2021/01/09/us/capitol-rioters.html; accessed 03 March 2022.

M. Bernstein, A. Monroy-Hernández, D. Harry, P. André, K. Panovich, G. Vargas, *4chan and /b/: An Analysis of Anonymity and Ephemerality in a Large Online Community*, Proceedings of the International AAAI Conference on Web and Social Media, 5 (1), 2011, pp. 50–57.

N. Bilton, *One on One: Christopher Poole, Founder of 4chan*, The New York Times, 2010, https://bits.blogs.nytimes.com/2010/03/19/one-on-one-christopher-poole-founder-of-4chan/?_php=true&_type=blogs&_r=0; accessed on 03 March 2022.

L. Bode, E. Vraga, *The Swiss cheese model for mitigating online misinformation*, Bulletin of the Atomic Scientists, *77*(3), 2021, 129–133. https://doi.org/10.1080/00963402.2021.1912170

S. Bok, *Secrecy: On the Ethics of Concealment and Revelation*, Vintage Books, New York, 1989.

S. Bond, *Twitter Expands Warning Labels To Slow Spread of Election Misinformation*, NPR, 2020; https://www.npr.org/2020/10/09/922028482/twitter-expands-warning-labels-to-slow-spread-of-election-misinformation?t=1648567293523; accessed on 04 March 2022.

L. Brandeis, *Other People's Money and How the Bankers Use It*. Frederick A. Stokes, New York, 1914.

E. E. Buckels, P. D. Trapnell, D. L. Paulhus, *Trolls just want to have fun*, Personality and Individual Differences, *67*, 2014, 97–102; https://doi.org/10.1016/j.paid.2014.01.016

R. Callimachi, *ISIS and the Lonely Young American*, New York Times, 2015; https://www.nytimes.com/2015/06/28/world/americas/isis-online-recruiting-american.html?searchResultPosition=1

J. Carreyrou, *Bad Blood: Secrets and Lies in a Silicon Valley Startup*. Penguin Random House, New York 2018.

R. Chesney, D.K. Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, No. 692; Public Law Research Paper), 2018; https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3213954

B. C. K. Choi, A. W. P. Pak, *Multidisciplinarity, Interdisciplinarity and Transdisciplinarity in Health Research, Services, Education and Policy: 1. Definitions, Objectives, and Evidence of Effectiveness*, Clinical and Investigative Medicine, 29 (6), 2006, pp. 351–364; http://www.ncbi.nlm.nih.gov/pubmed/17330451

M. Cinelli, G. De Francisci Morales, A. Galeazzi, W. Quattrociocchi, M. Starnini, *The Echo Chamber Effect on Social Media*, Proceedings of the National Academy of Sciences, 118 (9), 2021; https://doi.org/10.1073/pnas.2023301118

H. Darbishire, *Proactive Transparency: The Future of the Right to Information?*, The World Bank, Washington, DC 2010; https://openknowledge.worldbank.org/bitstream/handle/10986/25031/565980WP0Box351roactiveTransparency.pdf?sequence=1&isAllowed=y; accessed 21 February 2022.

M. den Boer, *Steamy Windows: Transparency and Openness in Justice and Home Affairs*, in: Openness and Transparency in the European Union, V. Deckmyn, I. Thomson (eds.), European Institute of Public Administration, Maastricht, 1998, pp. 91–105.

M. R. X. Dentith, M. Orr, *Secrecy and Conspiracy*, Episteme, 15 (4), 2018, pp. 433–450; https://doi.org/10.1017/epi.2017.9

C. Dewey, *Absolutely Everything You Need to Know to Understand 4chan, the Internet's Own Bogeyman*, The Washington Post, 2014; https://www.washingtonpost.com/news/the-intersect/wp/2014/09/25/absolutely-everything-you-need-to-know-to-understand-4chan-the-internets-own-bogeyman/; accessed 18 February 2022.

J. Dibbell, *Radical Opacity*, Technology Review, 113 (5), 2010, pp. 82–86.

J. S. Donath, *Identity and Deception in the Virtual Community*, in: Communities in Cyberspace, P. Kollock, M. Smith (eds.), Routledge, London 2020, pp. 37–68; https://doi.org/10.4324/9780203194959-11

D. M. Douglas, *Doxing: a Conceptual Analysis*, Ethics and Information Technology, 18 (3), 2016; 199–210. https://doi.org/10.1007/s10676-016-9406-0

K. M. Douglas, J. E. Uscinski, R. M. Sutton, A. Cichocka, T. Nefes, C.S. Ang, F. Deravi, *Understanding Conspiracy Theories*, Political Psychology, 40 (S1), 2019, pp. 3–35; https://doi.org/10.1111/pops.12568

M. Drouin, D. Miller, S. M. J. Wehle, E. Hernandez, *Why Do People Lie Online? "Because Everyone Lies on the Internet,"* Computers in Human Behavior, 64, 2016, pp. 134–142; https://doi.org/10.1016/j.chb.2016.06.052

N. B. Ellison, D.M. Boyd, *Sociality Through Social Network Sites*, in: W. H. Dutton (ed.), Sociality Through Social Network Sites, Oxford University Press, Oxford, 2013. https://doi.org/10.1093/oxfordhb/9780199589074.013.0008

N. B. Ellison, J. T. Hancock, C. L. Toma, *Profile as Promise: A Framework for Conceptualizing Veracity in Online Dating Self-presentations*, New Media and Society, 14 (1), 2012, pp. 45–62; https://doi.org/10.1177/1461444811410395

Facebook, *What Names Are Allowed on Facebook?,* n.d.; https://www.facebook.com/help/112146705538576; accessed 07 March 2022.

S. Feldman, *Where Do Freedom of Information Laws Exist?* Statista—The Statistics Portal, 2019; https://www.statista.com/chart/17879/global-freedom-of-information-laws/; accessed 20 February 2022.

L. Floridi, *The 4th Revolution: How the Infosphere is Reshaping Humanity*, Oxford University Press, Oxford 2016.

A. Fung, *Infotopia: Unleashing the Democratic Power of Transparency*, Politics and Society, 41 (2), 2013, pp. 183–212; https://doi.org/10.1177/0032329213483107

A. Fung, M. Graham, D. Weil, *Full Disclosure: The Perils and Promise of Transparency*, Cambridge University Press, Cambridge 2007.

A. Fung, D. Weil, *Open Government and Open Society*, in: Open Government, D. Lathrop, L. Ruma (eds.),O'Reilly Media, Sebastopol, 2010, pp. 105–114.

K. Granville, *Facebook and Cambridge Analytica: What You Need To Know as Fallout Widens*, The New York Times, 2018; https://www.nytimes.com/2018/03/19/technology/ facebook-cambridge-analytica-explained.html; accessed 10 February 2022.

G. Greenleaf, *The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108*, International Data Privacy Law, 2 (2), 2012, pp. 68–92. https://doi.org/10.1093/idpl/ips006

J. Halliday, *Twitter's Tony Wang: "We Are the Free Speech Wing of the Free Speech Party,* The Guardian, 2012; https://www.theguardian.com/media/2012/mar/22/twitter-tony-wang-free-speech; accessed 10 February 2022.

D. Hardegger, *A First Holistic "4th Space" Concept*, Proceedings, 81(1), 2022; https://doi.org/10.3390/proceedings2022081072

J. Heath, *The Uses and Abuses of Agency Theory*, Business Ethics Quarterly, 19 (4), 2009, pp. 497–528; https://doi.org/10.5840/beq200919430

B. E. Hermalin, M.S. Weisbach, *Transparency and Corporate Governance*, National Bureau Of Economic Research, 2007; http://www.nber.org/papers/w12875

N. P. Hoang, D. Pishva, *Anonymous Communication and Its Importance in Social Networking*, 16th International Conference on Advanced Communication Technology, 2014, pp. 34–39; https://doi.org/10.1109/ICACT.2014.6778917

R. Hofstadter, *The Paranoid Style of American Politics and Other Essays*, Knopf, New York 1965.

C. Hood, *What Happens When Transparency Meets Blame-avoidance?,* Public Management Review, 9 (2), 2007, pp. 191–210; https://doi.org/10.1080/14719030701340275

E. Jardine, *Tor, What Is It Good for? Political Repression and the Use of Online Anonymity-Granting Technologies*, New Media and Society, 20 (2), 2018, pp. 435–452; https://doi.org/10.1177/1461444816639976

M. C. Jensen, H. Meckling, *Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure*, Journal of Financial Economics, 3, 1976, pp. 305–360.

C. Kang, S. Frenkel, *'PizzaGate' Conspiracy Theory Thrives Anew in the TikTok Era*, The New York Times, 2020; https://www.nytimes.com/2020/06/27/technology/pizzagate-justin-bieber-qanon-tiktok.html; accessed 07 March 2022.

J. Kay, *Among the Truthers: A Journey through America's Growing Conspiracist Underground*, HarperCollins, New York 2011.

B. L. Keeley, *Of Conspiracy Theories*, Journal of Philosophy, 96 (3), 1999, pp. 109–126.

D. Kirkpatrick, *The Facebook Effect: The Inside Story of the Company that Is Connecting the World*, Simon & Schuster, New York 2010.

J. T. Klein, *Evaluation of Interdisciplinary and Transdisciplinary Research*, American Journal of Preventive Medicine, 35 (2), 2008, pp. 116–123; https://doi.org/10.1016/j.amepre.2008.05.010

L. Knuttila, *User Unknown: 4chan, Anonymity and Contingency*, First Monday, 16 (10), 2011; https://firstmonday.org/ojs/index.php/fm/article/view/3665/3055

S. Koos, *Forschungsbericht: Die "Querdenker". Wer nimmt an Corona-Protesten teil und warum?* [Research report: The Querdenker. Who attends Corona protests and why?], Universität Konstanz 2021; https://kops.uni-konstanz.de/bitstream/handle/123456789/52497/Koos_2-bnrddxo8opad0.pdf?sequence=1

K. Lee, M. C. Ashton, J. Wiltshire, J.S. Bourdage, B.A. Visser, A. Gallucci, *Sex, Power, and Money: Prediction from the Dark Triad and Honesty–Humility*, European Journal of Personality, 27(2), 2013, pp. 169–184; https://doi.org/10.1002/per.1860

L. Lessig, *The Architecture of Privacy: Remaking Privacy in Cyberspace*, Vanderbilt Journal of Entertainment & Technology Law, 1 (1), 1999, pp. 56–65.

S. Malevich, T. Robertson, *Violence Begetting Violence: An Examination of Extremist Content on Deep Web Social Networks*, First Monday, 3, 2020; https://doi.org/10.5210/fm.v25i3.10421

H. Margetts, *The Internet and Transparency*, Political Quarterly, 82 (4), 2011, pp. 518–521. https://doi.org/10.1111/j.1467-923X.2011.02253.x

A. Meijer, *Understanding Modern Transparency*, International Review of Administrative Sciences, 75 (2), 2009, pp. 255–269; https://doi.org/10.1177/0020852309104175

J. M. Miller, K. L. Saunders, C. E. Farhart, *Conspiracy Endorsement as Motivated Reasoning: The Moderating Roles of Political Knowledge and Trust*, American Journal of Political Science, 60 (4), 2016, pp. 824–844; https://doi.org/10.1111/ajps.12234

A. Morisson, *A Typology of Places in the Knowledge Economy: Towards the Fourth Place*, in: New Metropolitan Perspectives. ISHT 2018. Smart Innovation, Systems and Technologies, F. Calabrò, L. Della Spina, C. Bevilacqua (eds.), Springer, Cham, 2019, pp. 444–451; https://doi.org/10.1007/978-3-319-92099-3_50

A. Mungiu-Pippidi, *The Quest for Good Governance*, Cambridge University Press, Cambridge, 2015; https://doi.org/10.1017/CBO9781316286937

A. Mungiu-Pippidi, R. Dadašov, *Measuring Control of Corruption by a New Index of Public Integrity*, European Journal on Criminal Policy and Research, 22(3), 2016, pp. 415–438; https://doi.org/10.1007/s10610-016-9324-z

A. Mungiu, *Corruption: Diagnosis and Treatment*, Journal of Democracy, 17 (3), 2006, pp. 86–99. https://doi.org/10.1353/jod.2006.0050

K. Murphy, *In Online Dating, 'Sextortion' and Scams*, The New York Times, 2016; https://www.nytimes.com/2016/01/17/sunday-review/in-online-dating-sextortion-and-scams.html?searchResultPosition=11; accessed 01 March 2022.

OCCRP, Daraj, Süddeutsche Zeitung, NDR, *Historic Leak of Swiss Banking Records Reveals Unsavory Clients*, Suisse Secrets, 2022; https://www.occrp.org/en/suisse-secrets/ historic-leak-of-swiss-banking-records-reveals-unsavory-clients; accessed 02 March 2022.

A. Ohlheiser, *"We Actually Elected a Meme as President": How 4chan Celebrated Trump's Victory*, The Washington Post, 2016; https://www.washingtonpost.com/news/the-intersect/wp/2016/11/09/we-actually-elected-a-meme-as-president-how-4chan-celebrated-trumps-victory/; accessed 02 March 2022.

R. Oldenburg, *The great Good Place: Café, Coffee Shops, Community Centers, Beauty Parlors, General Stores, Bars, Hangouts, and How They Get You Through the Day*, Paragon House, New York 1989.

Y. J. Park, *Digital Literacy and Privacy Behavior Online*, Communication Research, 40 (2), 2013, pp. 215–236; https://doi.org/10.1177/0093650211418338

R. D. Putnam, *Bowling Alone: America's Declining Social Capital*, Free Press, 2000; https://doi.org/10.4324/9780203805749

A. Rabin-Havt, Media Matters, *Lies, Incorporated: The World of Post-Truth Politics*, Anchor Books, New York 2016.

A. Rege, *What's Love Got to Do with It? Exploring Online Dating Scams and Identity Fraud*, International Journal of Cyber Criminology, 3(2), 2009, pp. 494–512; http://

ra.ocls.ca/ra/login.aspx?url=http://search.ebscohost.com/login.aspx?direct=true&db=i3h&AN=59256420&site=eds-live

T. Rid, *Active Measures: The Secret History of Disinformation & Political Warfare*, Profile Books, London 2020.

P. Robinson, *Flying Blind: The 737 MAX Tragedy and the Fall of Boeing*, Doubleday, New York 2021.

T. Sardá, *The Dark Side of the Internet: A Study about Representations of the Deep Web and the Tor Network in the British Press*, Doctoral thesis, Loughborough University, Loughborough 2020.

K. Starbird, L. Palen, *Pass It On?: Retweeting in Mass Emergency*, Proceedings of the 7th International ISCRAM Conference, 2010; http://idl.iscram.org/files/starbird/2010/970_Starbird+Palen2010.pdf

J.E. Stiglitz, *Transparency and Government*, in: The Right to Tell: The Role of Mass Media in Economic Development, R. Islam, S. Djankov, C. McLiesh (eds.), The World Bank, Washington, DC 2002, pp. 27–44.

O. Storbeck, *BaFin Boss "Believed" Wirecard Was Victim until Near the Ned*, Financial Times, 2021; https://www.ft.com/content/a021012e-bd2e-44d5-a160-96d997c662f1; accessed 03 March 2022.

C. R. Sunstein, A. Vermeule, *Conspiracy Theories*, University of Chicago Public Law & Legal Theory Working Paper, No. 199, 2008; http://ssrn.com/abstract=1084585

C. S. Taber, D. Cann, S. Kucsova, *The Motivated Processing of Political Arguments*, Political Behavior, 31 (2), 2009, pp. 137–155; https://doi.org/10.1007/s11109-008-9075-8

Y. Theocharis, A. Cardenal, S. Jin, T. Aalberg, D.N. Hopmann, J. Strömbäck, L. Castro, F. Esser, P. Van Aelst, C. de Vreese, N. Corbu, K. Koc-Michalska, J. Matthes, C. Schemer, T. Sheafer, S. Splendore, J. Stanyer, A. Stępińska, V. Štětka, *Does the Platform Matter? Social Media and COVID-19 Conspiracy Theory Beliefs in 17 Countries*, New Media & Society, 2021; https://doi.org/10.1177/14614448211045666

A. Thompson, *The Measure of Hate on 4Chan*, Rolling Stone, 2018, https://www.rollingstone.com/politics/politics-news/the-measure-of-hate-on-4chan-627922/; accessed 02 March 2022.

R. Thomson, N. Ito, H. Suda, F. Lin, Y. Liu, R. Hayasaka, R. Isochi, Z. Wang, *Trusting Tweets: The Fukushima Disaster and Information Source Credibility on Twitter*, ISCRAM 2012 Conference Proceedings — 9th International Conference on Information Systems for Crisis Response and Management, 2012; https://www.emknowledge.org.au/ISCRAM2012/ proceedings/112.pdf

Transparency International, 25 Corruption Scandals that shook the world, 2019, https://www.transparency.org/en/news/25-corruption-scandals; accessed 02 March 2019.

Z. Tufekci, *Twitter and Tear Gas: The Power and Fragility of Networked Protest*, Yale University Press, New Haven 2017.

M. Tuters, E. Jokubauskaitė, D. Bach, *Post-Truth Protest: How 4chan Cooked Up the Pizzagate Bullshit*, M/C Journal, 21(3), 2018, pp. 1–18; https://doi.org/10.5204/mcj.1422

Twitter, *About Verified Accounts*, n.d.; https://help.twitter.com/en/managing-your-account/about-twitter-verified-accounts; accessed 04 March 2022.

Twitter, *Ban Evasion Policy*, 2020; https://help.twitter.com/en/rules-and-policies/ban-evasion; accessed 04 March 2022.

J. E. Uscinski, A.M. Enders, C. Klofstad, M. Seelig, J. Funchion, C. Everett, S. Wuchty, K. Premaratne, M. Murthi, *Why Do People Believe COVID-19 Conspiracy Theories?*, Harvard Kennedy School Misinformation Review, 1 (April), 2020; https://doi.org/10.37016/mr-2020-015

J. E. Uscinski, J. M. Parent, *American Conspiracy Theories*, Oxford University Press, Oxford 2014.

S. Vaidhyanathan, *Anti-social Media: How Facebook Disconnects Us and Undermines Democracy*, Oxford University Press, Oxford 2018.

P. Van Aelst, J. Strömbäck, T. Aalberg, F. Esser, C. de Vreese, J. Matthes, D. Hopmann, S. Salgado, N. Hubé, A. Stępińska, S. Papathanassopoulos, R. Berganza, G. Legnante, C. Reinemann, T. Sheafer, J. Stanyer, *Political Communication in a High-choice Media Environment: a challenge for democracy*, Annals of the International Communication Association, 41 (1), 2017, 3–27; https://doi.org/10.1080/23808985.2017.1288551

G. J. van Hardeveld, C. Webber, K. O'Hara, *Deviating From the Cybercriminal Script: Exploring Tools of Anonymity (Mis)Used by Carders on Cryptomarkets*, American Behavioral Scientist, 61 (11), 2017, pp. 1244–1266; https://doi.org/10.1177/ 0002764217734271

J. W. van Prooijen, K. M. Douglas, *Conspiracy Theories as Part of History: The Role of Societal Crisis Situations*, Memory Studies, 10 (3), 2017, pp. 323–333. https://doi.org/ 10.1177/1750698017701615

L. Verdoliva, *Media Forensics and DeepFakes: An Overview*, IEEE Journal on Selected Topics in Signal Processing, 14 (5), 2020, pp. 910–932; https://doi.org/10.1109/ JSTSP.2020.3002101

T. Wang, *Talking to Strangers: Chinese Youth and Social Media*, Doctoral Thesis, University of California, San Diego 2013.

M. Wendling, *The Saga of "Pizzagate": The Fake Story that Shows How Conspiracy Theories Spread*, BBC News, 2016; http://www.bbc.com/news/blogs-trending-38156985; accessed 03 March 2022.

R. White, *A Third Place*, New Zealand Geographic, 2018; https://www.nzgeo.com/stories/a-third-place/; accessed 03 March 2022.

M. T. Whitty, T. Buchanan, *The Online Dating Romance Scam: The Psychological Impact on Victims — Both Financial and Non-financial*, Criminology and Criminal Justice, 16 (2), 2016, pp. 176–194; https://doi.org/10.1177/1748895815603773

J. Wideström, A Seeing Place—Connecting Physical and Virtual Spaces, Doctoral Thesis, Chalmers University of Technology, Gothenburg 2020.

O. Winkel, *Electronic cryptography—Chance or threat for modern democracy?*, Bulletin of Science, Technology and Society, 23(3), 2003, 185–191; https://doi.org/10.1177/ 0270467603023003006

S. Zannettou, T. Caulfield, E. De Cristofaro, N. Kourtelris, I. Leontiadis, M. Sirivianos, G. Stringhini, J. Blackburn, *The web centipede: Understanding how web communities influence each other through the lens of mainstream and alternative news sources*, Proceedings of the 2017 Internet Measurement Conference, Part F1319, 2017, pp. 405–417; https://doi.org/10.1145/3131365.3131390

A. Zelenkauskaite, P. Toivanen, J. Huhtamäki, K. Valaskivi, *Shades of Hatred Online: 4chan Duplicate Circulation Surge during Hybrid Media Events*, First Monday, 26 (1–4), 2020; https://doi.org/10.5210/fm.v26i1.11075

I. X. Zhang, *Economic Consequences of the Sarbanes-Oxley Act of 2002*, Journal of Accounting and Economics, 44 (1–2), 2007, pp. 74–115; https://doi.org/10.1016/j.jacceco. 2007.02.002

ABOUT THE AUTHORS:

Christoph M. Abels — Doctoral Researcher, Hertie School, Friedrichstraße 180, 10117 Berlin, Germany.

Email: c.abels@phd.hertie-school.org

Daniel Hardegger — PhD, Research Fellow, ZHAW School of Management and Law, Gertrudstrasse 15, 8401 Winterthur, Switzerland.

Email: daniel@hardegger.eu