

BOOK
OF

ONYMITY

ONYMITY

ONYMITY

NONYMIT

NONYMI

ANONYM

Section A **INTRO**

16 Toward a Kaleidoscopic Understanding
of Anonymity

35 Artistic Research on Anonymity

Section B **RECONFIGURATION**

70 Anonymity and Transgression: Caste,
Social Reform, and Blood Donation in India

88 Anonymity: The Politicisation of a Concept

110 USAE

116 Big Data's End Run around Anonymity
and Consent

142 A List of Famous Artists Who Used
to Be Invigilators

151 Anonymity as Everyday Phenomenon
and as a Topic of Research

167 Anonymity on Demand: The Great Offshore

Section C

ASSAULT

- 188 DNA Works!
Merging Genetics and the Digital Realm
- 210 Sanitary Policy and the Policy of Anonymity:
Observations on a Game on Endocrine Disruptors
- 226 Where Do the Data Live?
Anonymity and Neighborhood Networks
- 255 Fraught Platform Governmentality:
Anonymity, Content Moderation, and Regulatory
Strategies over Yik Yak
- 275 Anonymity: Obsolescence and Desire
- 286 Policing Normality: Police Work, Anonymity,
and a Sociology of the Mundane

Section D

WEAPON

- 294 Amazonian Flesh: How to Hang in Trees during
Strike?
- 306 Proximity, Distance, and State Powers:
Policing Practices and the Regulation of
Anonymity
- 326 Dual Reality:
(Un)Observed Magic in the Workplace

336 A Provisional Manifesto for Invigilator-Friendly
Artworks, or Your Artwork Is an Invigilator's
Labor Conditions: Informally Sourced from Security
Guards at an Art Gallery in Central London

340 Care or Control?
Police, Youth, and Mutual Anonymity

346 She Remembers

Section E **DELIGHT**

356 Collective Pleasures of Anonymity:
From Public Restrooms to 4chan and Chatroulette

379 Transformella Malor Ikeae:
InnerCity Ikeality [4.4.6.11]

394 Authenticity

401 Longing for a Selfless Self and other
Ambivalences of Anonymity: A Personal Account

424 Speak their Endless Names

433 Bitcoin Anonymous? Of Trust in Code and Paper

447 Anonymity Workshop

466 List of Figures

470 List of Artworks

471 Contributors

481 Citation Guide

486 Acknowledgments

Anonymity: The Politicisation of a Concept

Introduction

In May 2015 David Kaye, UN special rapporteur on the promotion and protection of the right to freedom of opinion and expression, submitted his first report to the Human Rights Council.¹ It focused on issues of encryption and anonymity, highlighting the important role these play regarding privacy and the right to free expression. The mere fact that such a report has been produced, and the debate it has engendered, indicates that anonymity has become a high-profile issue. Anonymity is, of course, nothing new in human history and has long been recognized as posing problems and providing solutions in several domains (investigative journalism and the handling of medical data are two such areas). But the intensity

¹ David Kaye, “Report on Encryption, Anonymity, and the Human Rights Framework” (Geneva: United Nations Human Rights Council, 2015).

of the current debate has shown just how hard it is to pinpoint anonymity—either as a normative concept or as an everyday practice. Only in the wake of the digital turn has the topic become politicized, in other words, transformed from a largely unmanaged determinant of social communication into a political issue. Until the late 1990s, there was a near-total absence of academic literature examining anonymity from a political point of view. Since the turn of the millennium and the heightened awareness of the digital condition we live in, this situation has changed radically. Discourse on the topic has become a scholarly and political battleground, and anonymity is widely understood as a cornerstone of the (normative) order governing our digital lives.

This chapter traces the changing conditions of anonymity in liberal Western societies. Political, technical, economic, and social developments have undermined the broad de facto anonymity of modern societies, and I ask whether the current politicization of anonymity is likely to have any impact on the steady disappearance of opportunities for anonymous communication. I argue that anonymity is an ambivalent but critical feature of the democratic public sphere. If we want to slow down or halt this trend, or actually reverse it, it will not be enough simply to politicize “deanonymizing” tendencies and whip up indignation.

My argument proceeds in three stages. I begin with several conceptual observations on anonymity. From these, a heuristic framework emerges with which the changes in anonymous communication, and in the role this form of communication plays in society, can be described. In very broad brushstrokes, I then describe and analyze the extent to which options for anonymity have been affected by the revolution in information and communication technologies (ICTs). I conclude by considering how anonymity is framed in public discourse and what effects this has. My aim in this last section is to provide a sketch of the main lines in the debates and

show that none of the different layers of the anonymity discourse have generated any cogent ideas as to how the all-encompassing trend to deanonymization outlined in the second part of the chapter might be tackled. If we are to succeed in countering this trend, we will have to adopt a more political and institutional mode of thinking.

Anonymity: Conceptual Observations

The word “anonymity” literally means a condition of namelessness. But given that a name is only one—actually quite unreliable—identifier of a person, focusing on its absence does not exhaust the meaning of the concept of anonymity. A better way to understand the concept is to set it in a broader context of social communication. Viewed thus, anonymity describes a situation of intersubjective action in which it is not possible either to conclusively attribute a particular action or communication to an individual or subject or to render an individual or subject accessible and therefore accountable.² Greater precision can be introduced into this broad definition if we take into account four closely interrelated facts.

First, anonymity always relates to the question “Who?” It thus points to the combination of action/communication and actor. The “what”—in other words the object or content of the action/communication—can be known, provided it does not reveal the identity.

Second, anonymity is situational. It is not a characteristic of a person; it is the product of an intersubjective constellation and of the possibility/impossibility of identifying an actor in that constellation beyond the immediate context. This being the case, it is also an impermanent condition, always tied to specific delimitable actions, which themselves are visible as actions and produce effects. Anonymity is therefore distinct from invisibility.

² Helen Nissenbaum, “The Meaning of Anonymity in an Information Age,” *The Information Society* 15, no. 2 (1999): 141–44; Gary T. Marx, “What’s in a Name? Some Reflections on the Sociology of Anonymity,” *Information Society* 15, no. 2 (1999): 99–112; and Julie Ponesse, “The Ties That Bind: Conceptualizing Anonymity,” *Journal of Social Philosophy* 45, no. 3 (2014): 304–22.

Third, although anonymity can be produced intentionally (through disguise, for example, or the use of a pseudonym), it can also arise from a situation (as when one finds oneself in a crowd). Anonymity is generated by indistinguishability and therefore only succeeds where there are multiple possible authors of an action. This being so, anonymity always depends, at least indirectly, on others' either ignoring or accepting it and exercising restraint—by not insisting on identification, for example, or by not attempting to single out those performing an action. No individual can be sure that their action will in fact play out anonymously—especially since the possibility of identification persists after, or indeed arises from, the action. Anonymity therefore can never be established for good. Strengthening it would mean taking measures that render identification more difficult—by, for example, removing information from a situation.

The upshot of this, fourth, is that anonymity is best understood and analyzed in terms of its opposite—identification. Hence, anyone wishing to ascertain whether and to what degree anonymity exists in a particular situation must establish to what extent and by whom identification is possible.

With these observations in mind, we can set about constructing a heuristic framework that will help us trace the social and technological developments concerning the state of anonymity in liberal societies. To do this, we must first draw two distinctions.

The first differentiates horizontal from vertical anonymity. “Horizontal anonymity” refers to anonymity among peers and one’s immediate surroundings. Such anonymity is obtained where one is not, or cannot be, identified by those observing a particular act or conversation. This is the situation, for example, in a café or bar, where we tend not to know the people around us and have no way of finding out who they are short of asking them to identify themselves. “Vertical anonymity,” by contrast,

refers to anonymity vis-à-vis well-resourced institutions. Most notable among these are states, which have a broad range of means available to identify people in situ and retrospectively. Such actors do not have to be present in the situation in order to make an identification.

3 For a more thorough discussion, compare Thorsten Thiel, "Anonymität und Demokratie," *Forschungsjournal Soziale Bewegungen* 30, no. 2 (2017): 152–61.

This chronological aspect points to the second distinction, which relates to the fact that anonymity is not contained within the presence. On the contrary, it almost necessarily extends to the future. Being unidentified in a particular situation is different from being (or at least feeling) protected against later identification. We would not, for example, describe communication as anonymous if we were aware that it was possible, or even likely, that we would later be identified. Our second distinction is therefore between identification (which puts an end to anonymity within a situation) and identifiability (which implies that anonymity cannot be maintained beyond that situation). Whereas identification mostly has to be done overtly (a person presenting ID to board a plane is aware that they are not maintaining their anonymity), identifiability can be achieved without the knowledge or consent of those whose anonymity is being breached. Being aware of the possibility of later identification often prevents us from acting as if we were anonymous. It is possible to secure anonymity actively by introducing (effective, nonreversible) anonymizing procedures that restrict identifiability.

These two distinctions in themselves provide us with enough of a conceptual apparatus to trace the development of anonymity over the last three decades, in which we have experienced the advent of the public internet and the rise of mobile computing, triggering a deep mediatization of our now digital lives. Before we do this, however, we need to make a short detour through normative territory.³ Anonymity is, after all, most often discussed in relation to whether we have cause to fear its spread or demise. If, as previously proposed, anonymity is highly dependent on intersubjective constellations and

situational specifics, mounting a hardline defense of it (for example, according to the status of a human right) or, alternatively, banning it altogether would seem to be equally unpromising approaches. Normative evaluations of anonymity generally take the form of discussions about the presumed effects of anonymous communication. Although the language in these debates is normatively charged and seemingly general, these setups are better thought of as clashes between differing empirical expectations. The optimistic camp holds that facilitating anonymous or at least pseudonymous communication will engender authenticity since power relations can then be ignored, and the individual will be able to speak freely and openly.⁴ The pessimists, by contrast, believe that giving up the possibility of holding someone to account will foster irresponsible and antisocial behavior.⁵ These two sets of expectations are then tied into broader normative debates, such as those on privacy (where anonymity can be seen either as crucial to the creation of an inviolable personal sphere or as likely to foster negative behavior such as hate speech) and those on democracy (where anonymity may figure either as a necessary bulwark against the state or as a mechanism that can both facilitate collective action and undermine public discourse). The fact that both sides have a wealth of anecdotal evidence to draw on suggests that rather than treating anonymity as being of value in and of itself, we should look at it in specific contexts.⁶ Indeed, to regard anonymity as being of inherent worth would seem, quite manifestly, to be a category error.

This being the case, rather than taking the abstract route and discussing potential effects of anonymous communication, I follow the heuristic framework established above and trace developments in the possibilities for such communication in society. By establishing what has changed, we get a different view of what these developments entail, and how we might respond.

4 For example, Tony Doyle and Judy Veranas, "Public Anonymity and the Connected World," *Ethics and Information Technology* 16, no. 3 (2014): 207–18; Alfred Moore, "Anonymity, Pseudonymity, and Deliberation: Why Not Everything Should Be Connected," *Journal of Political Philosophy* 26, no. 2 (2018): 169–92; and Dongwon Lim, Hangjung Zo, and Dukhee Lee, "The Value of Anonymity on the Internet," in *Service-Oriented Perspectives in Design Science Research: 6th International Conference, DESRIST 2011, Milwaukee, WI, USA, May 5–6, 2011, Proceedings*, ed. Hemant Jain, Atish P. Sinha, and Padmal Vitharana (Berlin and Heidelberg: Springer-Verlag, 2011), 452–64.

5 Ingrid Brodnig, *Der unsichtbare Mensch* (Vienna: Czernin, 2013).

6 James Gardner, "Anonymity and Democratic Citizenship," *William & Mary Bill of Rights Journal* 19, no. 4 (2011): 927.

A Brief Overview of the Development of Anonymous Communication in the Digital Constellation

Guided by the conceptual framework laid down in the first section, we can now analyze the fortunes of anonymity in the digital constellation. To do this, we first need to ascertain the nature of anonymity—or more precisely, of the options for anonymous communication—prior to these events. Before we can focus on the specific scope and structure of anonymity in Western liberal societies in most of the second half of the twentieth century, we have to turn our attention to the abstract matter of historical representation.

Founding sociological text like those of Weber, Durkheim, and Simmel have often depicted modernity as an age of anonymity. In these accounts, the accelerated pace of life and the spread of impersonal modes of production and communication brought about by the Industrial Revolution has been precipitating the demise of community life. Bureaucracy, pluralism, and urban living are characterized as anonymous and contrasted with trust-based communication in small-scale communities. Overall, anonymity is described as ambivalent and often demanding for the individual but at the same time seen as inevitable, a necessary byproduct of the ongoing growth and differentiation of societies. Anonymity is conceptualized as a condition of modern life, less as something individual and situational that deserves protection.

Against this sociological background, what is the situation of anonymous communication in societies for most of the twentieth century? Two facts stand out from the above account: first, anonymity is a feature of society that points to broad development rather than intentional design; and second, anonymity is focused on the horizontal dimension, on societal experiences and peer-to-peer relations. Staying anonymous in a public setting

is easily achieved, given that peers are not obliged to identify themselves, and it is not difficult to withhold information. Attempting to establish someone's identity is not only costly; in most situations, it also violates social and legal norms. Regarding vertical anonymity, there are specific areas—such as travel and taxation—in which identification has long been mandatory and is strictly enforced. Outside of these contexts, even the (liberal) state most often opts for modes of governance that are not based on establishing individual identities: besides being costly, it is a task that is feasible only for a limited number of individuals and that has to be performed more or less openly. Corporate actors play a minor role and are only able or inclined to enforce identification in very special circumstances.

A visual summary of the observations made so far is given in Table 1. This points to the centrality of de facto anonymity in societies before the last decade of the twentieth century. Private, public, and political spaces are mostly constituted in ways conducive to the spread of anonymity—provided this preservation does not entail the breaking of certain written and unwritten rules, and attempts to reach out to a wider public often brings with it a requirement for identification. At the same time, only a handful of actors are capable of breaching anonymity and curtailing the privacy it can afford to individuals moving in public spaces. Any actors (states, for example) who do seek to “unmask” an individual are often constrained by laws and social norms or deterred by the high cost and visibility of identification procedures. Even though anonymity, and the possibility of anonymous communication, is deeply inscribed in Western liberal societies of the twentieth century, the notion itself is viewed as negative and dangerous. As a result, social and legal norms aim chiefly to delimit anonymous spaces and tend to frame anonymity as a problem that must be tolerated for pragmatic reasons.

Anonymous communication before 1995

	Identification	Identifiability
Horizontal communication	<ul style="list-style-type: none"> - Regulated by social norms - Identifiable communication in the wider public context enforced by strong gatekeepers 	<ul style="list-style-type: none"> - Weak - Basically restricted to the immediate environment
Vertical communication	<ul style="list-style-type: none"> - Highly context specific - Enforcement mainly by the state - Explicit and visible 	<ul style="list-style-type: none"> - Low to medium - Very costly and resource intensive - Mostly limited to states

Tab. 1

How, then, has the rise of ICTs influenced the discourse in this area, and what effect has it had on opportunities for anonymous communication? As early as 1993, in one of the best-known cartoons of the nascent internet age, Peter Steiner pictured two dogs in front of a computer, one of whom was saying to the other, “On the Internet, nobody knows you’re a dog.” This image sums up what the internet and ICTs were thought to be doing to social communication—namely, accelerating depersonalization.

From a technical point of view, the cartoon very much captures the idea of end-to-end communication and the fact that digital communications always have to be translated into bits and bytes and then transferred via a decentralized network using numbers and protocols. Therefore, every instance of such communication is in some sense pseudonymous. This circumstance brings with it a host of possibilities for covering one’s tracks. As a result of these factors, early perceptions of digital communication assumed a wide gap between “the real world” and “cyberspace.” In the latter, different norms seem to apply; social conventions and obligations appear less binding and less susceptible to legal enforcement. Today’s debates about trolling and hate speech are still

often understood in these terms and unsurprisingly often linked to the anonymous nature of the web.

The view that the digital constellation has facilitated and normalized anonymous communication with a broad public is widespread and has been reinforced by changes in the shape of collective action. This trend is perhaps most strikingly exemplified in the Anonymous protest movement and its emblem of a Guy Fawkes mask.⁷ Even so, I argue that the assumption that digitalization fosters anonymity is misguided and does not take sufficient account of the further shifts that have occurred in technical infrastructure and political and social context.

Three Deanonymizing Trends of Critical Significance

The first deanonymizing trend is *technological*. The current ubiquity, locational capability, and 24/7 operation of technological devices seriously expand the potential for identification. Mobile computing precludes the levels of anonymous communication that were possible with stationary setups. Similarly, the increased potential for storing and analyzing data has hamstrung anonymization strategies to the point where attempts to resolve the tensions between big data and privacy through measures based on anonymity and consent are breaking down completely.⁸

The second trend is *economic* and involves a massive shift in the incentives for deanonymization. In a digitalized economy, identity drives profits—a situation aptly summed up in descriptions of data as the new gold or oil.⁹ Alongside a growth in data mining, there has been a rise in the kinds of information monopolies that thrive on economies of scale and hence are hard to forgo.¹⁰ In addition, new modes of digital communication—apps, streaming, SaaS (software as a service), and so on—reinforce the “identification and registration” logic and erode the notion of digital data as impersonal and

7 Hans Asenbaum, “Cyborg Activism: Exploring the Reconfigurations of Democratic Subjectivity in Anonymous,” *New Media & Society* 20, no. 4 (2018): 1543–63.

8 Solon Barocas and Helen Nissenbaum, “Big Data’s End Run around Anonymity and Consent,” in *Privacy, Big Data, and the Public Good: Frameworks for Engagement*, ed. Helen Nissenbaum, Julia Lane, Stefan Bender, and Victoria Stodden (Cambridge: Cambridge University Press, 2014), 44–75; and Paul Ohm, “Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization,” *UCLA Law Review* 57 (2010): 1701–77.

9 Constanze Kurz and Frank Rieger, *Die Datenfresser: Wie Internetfirmen und Staat sich unsere persönlichen Daten einverleiben und wie wir die Kontrolle darüber zurückerlangen*, 2nd ed. (Frankfurt: S. Fischer Verlag, 2011).

10 Jodi Dean, “Communicative Capitalism: Circulation and the Foreclosure of Politics,” *Cultural Politics* 1, no. 1 (2005): 51–74; and Sebastian Seignani, “The Commodification of Privacy on the Internet,” *Science and Public Policy* 40, no. 6 (2013): 733–39.

endlessly reproducible. All these developments shift electronic communication out of individual control and make it dependent on intermediaries who make vast profits from analyzing behavior and personalizing their offers accordingly.

The third deanonymizing trend results from changes in *social practice*, notably the rise of social networking, with its in-built spur to self-portrayal and its (often forced) reduction to a single fixed identity across the Net.¹¹ Mirroring these developments are various political attempts to make the web more “secure”—by, for example, requiring verification of identity in all sorts of digital settings. (A significant example here is the introduction by many countries of mandatory ID verification in internet cafes—one of several trends linking real and online identities.¹²)

Together with other developments currently taking place, these trends are resulting in anonymous communication becoming much harder to achieve. Using my heuristic framework, we can determine where the relevant changes have occurred. In the horizontal dimension, the changes to anonymity have been less far reaching and, in terms of the present account, of less relevance than those in the vertical dimension. Although the possibilities for anonymous interaction appear, at first glance, to have multiplied (thanks to chat rooms, Twitter, and so on), and although the importance of gatekeepers in facilitating access to the broader public sphere has diminished, people’s presence in social networks, and the data trails they leave behind, have in fact brought an increase in identifiability. Identification remains context dependent, and we see a simultaneous proliferation of contexts where all participants to a conversation are identified (as on Facebook) and contexts that permit peer-to-peer anonymity. It is the discourse surrounding horizontal anonymity that has largely shaped our public conception of the internet as a place where anonymity is still possible but may also pose a problem.

11 Marc Andrejevic, “Facebook als neue Produktionsweise,” in *Generation Facebook: Über das Leben im Social Net* (Bielefeld: Transcript-Verl, 2011); and Geert Lovink, “Facebook, Anonymität und die Krise des multiplen Selbst,” in *Das halbwegs Soziale*, ed. Geert Lovink (Bielefeld: Transcript-Verl, 2011).

12 See Kenneth Farrall, “Online Collectivism, Individualism and Anonymity in East Asia,” *Surveillance and Society* 9, no. 4 (2012): 424–40.

Of much greater significance are the changes relating to vertical anonymity. Here the shifts have been not only more substantial but also distinctly one sided. The requirement for identification has become much more widespread and is now often mandatory for those seeking access to digital communication platforms. The result has been a proliferation in the number of private actors who are able—and motivated—to enforce identification. States too have extended their reach—not least by developing means of gaining access to, and combining, private data collections. Because the so-called digital public sphere is almost entirely privately owned and because the platform companies that grant access to it have enormous leverage when it comes to collecting all kinds of personal data, identifiability has burgeoned. Table 2 sums up these changes and allows comparison with conditions prior to the 1990s.

13 A. Michael Froomkin, "From Anonymity to Identification," *Journal of Self-Regulation and Regulation* 1 (2015): 121–38.

Anonymous communication in the digital constellation

	Identification	Identifiability
Horizontal communication	<ul style="list-style-type: none"> - Steady or decreasing - Weakening of social pressures 	<ul style="list-style-type: none"> - Medium
Vertical communication	<ul style="list-style-type: none"> - Many contexts require identification or set it as a default - More actors are able to enforce identification 	<ul style="list-style-type: none"> - Medium to high - Low costs - Easy to hide

Tab. 2

To sum up: over recent decades, the modalities of anonymous communication have undergone major change. Although this complex process has been driven by many different factors and trends, the shift away from de facto anonymity toward a “goldfish bowl” society has been unmistakable.¹³ One particularly salient feature has been the growth in the identificatory powers wielded by

well-resourced actors (whether states or private players). Given the added incentive that the falling costs of data storage and processing have created for generating personalized data, there seems little likelihood of this trend being reversed—particularly at a time when the distinction between the online and offline world is increasingly blurred. Digitalization is all pervading, even if we do have some power to shape it, and anonymity can no longer be achieved by switching off our computers or other devices.

The Politicization of Anonymity

Having outlined the general trends affecting anonymity, I now focus on how these developments have been taken up in the public discourse of Western liberal societies over the last twenty years. The concepts and convictions surrounding privacy have undergone enormous change, as the present volume demonstrates. Consequently, if we are to understand governance in this area, we need to analyze the various shifts and struggles in public discourse. Efforts at governance and regulation cannot be understood solely by looking at (external) challenges, such as changes in technological capacity. They need to be analyzed against the backdrop of changing expectations and demands. Therefore, the rest of this chapter gauges how successful attempts to politicize anonymity have been and whether there is any likelihood of current trends (particularly the diminution of vertical anonymity) being halted or reversed.

Before I embark on this task, a few remarks on terminology. As I use it here, “politicization” does not have the restricted meaning of getting an issue onto the agendas of political decision makers. Nor is it used in the sense of the extreme polarization of an issue. (Both of these are very common understandings of the concept.) Instead, I use the term in the “republican” sense of a topic of public discourse that gives rise to various alternative positions

and is amenable to, and stands in need of, political resolution. Interpreted thus, politicization is not limited to professional politics but equally relates to the type, quality, and variety of arguments in the public sphere. From a normative point of view, politicization is here conceptualized as inherently positive, since reflexivity is encouraged (rather than discouraged), social conflicts are articulated, and inclusion is made possible. Empirically, too, this interpretation of politicization may have its advantages, given that acceptance becomes likelier and solutions can be verified by argumentation before they are implemented. That said, politicization does not mean that policies necessarily change, only that they become the object of contestation.

In what follows, I pick out four areas—technical, economic, legal, and sociopolitical—in which the issue of anonymity has become politicized, if in very different ways. I sketch what arguments and positions have taken shape and whether success in politicization has had any impact on the metatrend of diminishing anonymous communication. Interest in issues of anonymous communication has grown in all four areas, but the growth in each case has taken very different turns. My purpose here is not to carry out a comprehensive discourse analysis and map the entire argumentative field. What I am aiming for, rather, is an anecdotal overview that may serve as a starting point for a more thorough empirical investigation.

The Technical Domain

The technical domain is the one in which anonymity has been politicized for the longest time. Anonymity has been a concern from the early days of the internet, and sensitivity to changes in the normative fabric and the institutional and technical infrastructure of the Net is widespread among members of the active civil society of hackers, privacy advocates, and the like. The technical

basis of the internet—protocols, routing logic, and so on, as well as advancing techniques of encryption—still leaves considerable room for anonymization, although the commodification of the Web and the framing of digital communication as a critical infrastructure (cyber security) has tightened control.¹⁴ Still, every attempt to enforce personalized, verified identification necessitates the creation and acceptance of additional layers of communication. Cookies are one example of this—and also illustrate the characteristic “cat and mouse” game in which identification mechanisms are created and then repeatedly circumvented and refined. To secure acceptance of these kinds of identification mechanisms, the organizations concerned have mostly avoided directly raising the issue of anonymity, instead focusing on the benefits of identification (ease of use, elimination of the need to log in, etc.). Nowadays, many services are available only to registered users, and the processes used for verification are much more advanced. Mobile technology and the app economy have been game changers in this respect: logins here are often permanent, and much more metadata—notably regarding location—is collected by default. This reshaping of online communications has been met with vocal opposition. It has also triggered the development of alternatives that subvert or supplement the offers described above. Probably the most significant endeavor in this regard is TOR (The Onion Router), an anonymization network that one of the NSA slides leaked by Edward Snowden described as “the king of high-secure, low-latency Internet anonymity.”

14 Laura DeNardis, “Hidden Levers of Internet Control,” *Information, Communication & Society* 15, no. 5 (2012); and Yochai Benkler, “Degrees of Freedom, Dimensions of Power,” *Daedalus* 145, no. 1 (2016): 18–32.

Within public discourse, technical solutions that offer anonymity are mostly framed as a form of justified civilian self-defense. Anonymity itself is depicted as a weapon with which to resist state-based and commercial data collection to preserve the capacity to organize collective action and hold monopolies of force in check. It is thus represented as inherently democratic in both a participatory and a civil liberties sense. This framing has been met with attempts to criminalize traffic using

anonymous networks or the equation of anonymizing mechanisms with fraud. As Helen Nissenbaum pointed out in regard to the hacker community, the contested ontology of cyberspace brings with it massive shifts in the normative evaluation of communication practices, even when these practices themselves change little.¹⁵

To sum up: in the technical domain, delegitimization discourses are on the rise, but significant factions in the tech community, especially in countries like Germany, have mostly remained on the side of anonymous communication. Several technical innovations for preserving anonymity have proliferated, although application rates in the wider public stay low. Because these tools are mostly geared to individual self-defense, often reduce ease of use, and entail regular checks and updates, their operation is restricted to a rather small group of technically literate users. Nevertheless, these tools and mechanisms are crucial, and internet-focused civil society has in Europe and the United States mostly succeeded in developing a political voice that commands a degree of attention.¹⁶ All in all, though, the impact of these endeavors is tempered by developments in other sectors.

The Economic Domain

In the economic domain, anonymity is a latecomer and still “under construction.” On the face of it, this is surprising, given the importance of anonymity in classical liberal theory. Here, markets are assumed to operate anonymously, and identification is regarded as unnecessary (or indeed likely to disrupt proper functioning), since goods can be exchanged by means of a mediation technique (money) that makes it irrelevant who is doing the buying and selling. In addition, modern economies are still viewed as being centered on markets, and they acquire much of their legitimacy by linking market exchange to the idea of freedom. The success of that

15 Helen Nissenbaum, “Hackers and the Contested Ontology of Cyberspace,” *New Media and Society* 6, no. 2 (2004): 195–217.

16 Thorsten Thiel, “Turnkey Tyranny? Struggles for a New Digital Order,” in *Resistance and Change in World Politics*, ed. Svenja Gertheiss, Stefanie Herr, Klaus Dieter Wolf, and Carmen Wunderlich (Basingstoke: Palgrave Macmillan, 2017), 215–42.

linkage depends, in its turn, on nondiscriminatory, anonymous markets.

Digitalization has clearly not resulted in the abandonment of the idea of markets. Instead it has reinforced a number of trends in capitalist economics that were already at work in postindustrialist societies generally; for example, the increased personalization of products, the localization of offers, and the shift from manufacturing to services. In this context, anonymity emerges as an obstacle to be overcome. The approach in the economic domain, therefore, has often been not to discredit anonymity but to highlight the virtues of identity and identification. Services have become increasingly personalized, social networking being the prime example.

The gradual disappearance of options for anonymous communication brought about by the changing behavior of commercial players has concerned privacy advocates and more recently also lawmakers. Although these diverse actors have vigorously condemned the kind of all-encompassing data collection pursued by business, they have mostly done so without referring to anonymity. Discussion here has generally taken place under the rubrics of data protection, responsible data use, and data minimization. Privacy, not anonymity, is the rallying cry. So, while there is, and always has been, a powerful anticonsumerist critique of the commercial internet, the argument is about collective goods and control of information and not about options for anonymous communication.

The Legal Domain

Because the issue of anonymity crops up in connection with many of the fundamental rights of liberal democracy, it presents a complex and persistent legal problem. Constitutionally, attempts have been made both to establish an abstract right to anonymity and to ban it.¹⁷

17 A. Michael Froomkin, "Legal Issues in Anonymity and Pseudonymity," *Information Society* 15, no. 2 (1999): 113–27; Ian Kerr, Carole Lucock, and Valerie Steeves, eds., *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society* (Oxford and New York: Oxford University Press, 2009).

Discourse in the legal sphere tends to be more nuanced than in the other domains discussed here. In relation to digital issues, debates about recognizing anonymity as a right, or banning it, tend to develop out of specific legal concerns. The critique of copyright enforcement, for example, led to a discussion about legal responsibility in the context of peer-to-peer networks and cloud storage, and this in turn triggered a debate about anonymity and the necessity of identification for these kind of services. State-based attempts to expanding law enforcement pushed for data retention, framing anonymity as an obstacle to the application of the law (or to the prevention of its violation). These moves have at least in Germany been countered with a fierce defense of data protection and the right to “informational self-determination.”

In legal discourses, those who support (qualified) rights to anonymity appear to be winning the argument. In regard to copyright infringement and data retention at least, a significant proportion of the relevant publics in democratic societies have become skeptical about proposals for an outright ban on anonymous communications. Still discursive framing does not translate directly into political power, and the current awareness might be temporal and specific to certain contexts and cases.

The Sociopolitical Domain

Within the wider sociopolitical domain, we find that many of the arguments from the other three areas also make an appearance here. The issue of anonymity has begun to excite interest and has been taken up by mass media. The way anonymity is framed in the public discourse continues to be more negative than positive, emphasizing the risks that anonymous communication brings with it and the antisocial behavior it is expected to engender. Attention is focused on the horizontal

dimension and on the harm that can be done to private individuals in situations of direct interaction.

While the main triggers to the public debate about anonymity are still bad digital practices (such as cyberbullying and hate speech), the exposure of surveillance activities by states and corporations, such as the Snowden revelations or the Cambridge Analytica scandal, have given rise to counter-discourses. Although civil society activists often claim that not enough attention is paid to arguments about anonymity, issues relating to anonymity, privacy, and surveillance have undoubtedly gained considerable traction in the public sphere and have graduated from niche concern to major political battleground.

Concluding Remarks

The scope and diversity of discourse in these four different areas demonstrates the speed with which the debate on anonymity has evolved in the last decade. Arguments on both sides—for and against anonymity—have become much more sophisticated, and anonymity is now an object of political contestation rather than a minor determinant of modern life. Although politicization is clearly under way, one can foresee that the current attempts might not be enough to counter the powerful trend toward deanonymization. Politicization itself can only be a necessary step not a sufficient one—especially since the forces driving us toward identification are to an extent isolated from public debates and shifting sensitivities. Therefore, those who want to ensure that anonymous communication has a secured place in digitized societies will have to more radically rethink the way our digital societies are governed. The focus should be less on techniques of anonymization and more on a legal and an institutional setup that is robust enough to keep capitalist dynamics and governmental overreach in check. Ensuring that the horizontal and vertical

dimension of anonymity are kept apart is as important as acknowledging the socioeconomic drivers of the development toward deanonymization. How and by whom the digital public sphere should be regulated is an open question and a major task of civil society and democratic politics.

Bibliography

- Andrejevic, Marc. "Facebook als neue Produktionsweise." In *Generation Facebook: Über das Leben im Social Net*, edited by Oliver Leistert and Theo Röhle, 31–49. Bielefeld: Transcript-Verl, 2011.
- Asenbaum, Hans. "Cyborg Activism: Exploring the Reconfigurations of Democratic Subjectivity in Anonymous." *New Media and Society* 20, no. 4 (2018): 1543–63. <https://doi.org/10.1177/1461444817699994>.
- Barocas, Solon, and Helen Nissenbaum. "Big Data's End Run around Anonymity and Consent." In *Privacy, Big Data, and the Public Good: Frameworks for Engagement*, edited by Helen Nissenbaum, Julia Lane, Stefan Bender, and Victoria Stodden, 44–75. Cambridge: Cambridge University Press, 2014. <https://doi.org/10.1017/CBO9781107590205.004>.
- Benkler, Yochai. "Degrees of Freedom, Dimensions of Power." *Daedalus* 145, no. 1 (2016): 18–32. https://doi.org/10.1162/DAED_a_00362.
- Brodnig, Ingrid. *Der unsichtbare Mensch*. Vienna: Czernin, 2013.
- Dean, Jodi. "Communicative Capitalism: Circulation and the Foreclosure of Politics." *Cultural Politics* 1, no. 1 (2005): 51–74. <https://doi.org/10.2752/174321905778054845>.
- DeNardis, Laura. "Hidden Levers of Internet Control." *Information, Communication and Society* 15, no. 5 (2012): 720–38. <https://doi.org/10.1080/1369118X.2012.659199>.
- Doyle, Tony, and Judy Veranas. "Public Anonymity and the Connected World." *Ethics and Information Technology* 16, no. 3 (2014): 207–18. <https://doi.org/10.1007/s10676-014-9346-5>.
- Farrall, Kenneth. "Online Collectivism, Individualism and Anonymity in East Asia." *Surveillance and Society* 9, no. 4 (2012): 424–40. <https://doi.org/10.24908/ss.v9i4.4344>.

- Froomkin, A. Michael. "From Anonymity to Identification." *Journal of Self-Regulation and Regulation* 1 (2015): 121–38. <https://doi.org/10.11588/josar.2015.0.23480>.
- Froomkin, A. Michael. "Legal Issues in Anonymity and Pseudonymity." *Information Society* 15, no. 2 (1999): 113–27. <https://doi.org/10.1080/019722499128574>.
- Gardner, James. "Anonymity and Democratic Citizenship." *William and Mary Bill of Rights Journal* 19, no. 4 (2011): 927.
- Kaye, David. "Report on Encryption, Anonymity, and the Human Rights Framework." Geneva: United Nations Human Rights Council, 2015. <https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx>.
- Kerr, Ian, Carole Lucock, and Valerie Steeves, eds. *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*. Oxford: Oxford University Press, 2009.
- Kurz, Constanze, and Frank Rieger. *Die Datenfresser: Wie Internetfirmen und Staat sich unsere persönlichen Daten einverleiben und wie wir die Kontrolle darüber zurückerlangen*. 2nd ed. Frankfurt: S. Fischer Verlag, 2011.
- Lim, Dongwon, Hangjung Zo, and Dukhee Lee. "The Value of Anonymity on the Internet." In *Service-Oriented Perspectives in Design Science Research: 6th International Conference, DESRIST 2011, Milwaukee, WI, USA, May 5–6, 2011, Proceedings*, edited by Hemant Jain, Atish P. Sinha, and Padmal Vitharana, 452–64. Berlin, Heidelberg: Springer-Verlag, 2011. <https://doi.org/10.1007/978-3-642-20633-7>.
- Lovink, Geert. "Facebook, Anonymität und die Krise des multiplen Selbst." In *Das halbwegs Soziale. Eine Kritik der Vernetzungskultur*, edited by Geert Lovink, 53–68. Bielefeld: Transcript-Verl, 2012.
- Marx, Gary T. "What's in a Name? Some Reflections on the Sociology of Anonymity." *Information Society* 15, no. 2 (1999): 99–112. <https://doi.org/10.1080/019722499128565>.
- Moore, Alfred. "Anonymity, Pseudonymity, and Deliberation: Why Not Everything Should Be Connected." *Journal of Political Philosophy* 26, no. 2 (2018): 169–92. <https://doi.org/10.1111/jopp.12149>.
- Nissenbaum, Helen. "Hackers and the Contested Ontology of Cyberspace." *New Media and Society* 6, no. 2 (2004): 195–217. <https://doi.org/10.1177/1461444804041445>.
- Nissenbaum, Helen. "The Meaning of Anonymity in an Information Age." *Information Society* 15, no. 2 (1999): 141–44. <https://doi.org/10.1080/019722499128592>.

- Ohm, Paul. "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization." *UCLA Law Review* 57 (2010): 1701–77. <https://papers.ssrn.com/abstract=1450006>.
- Ponessa, Julie. "The Ties That Blind: Conceptualizing Anonymity." *Journal of Social Philosophy* 45, no. 3 (2014): 304–22. <https://doi.org/10.1111/josp.12066>.
- Sevignani, Sebastian. "The Commodification of Privacy on the Internet." *Science and Public Policy* 40, no. 6 (2013): 733–39. <https://doi.org/10.1093/scipol/sct082>.
- Thiel, Thorsten. "Anonymität und Demokratie." *Forschungsjournal Soziale Bewegungen* 30, no. 2 (2017): 152–61. <https://doi.org/10.1515/fjsb-2017-0036>.
- Thiel, Thorsten. "Turnkey Tyranny? Struggles for a New Digital Order." In *Resistance and Change in World Politics*, edited by Svenja Gertheiss, Stefanie Herr, Klaus Dieter Wolf, and Carmen Wunderlich, 215–42. Basingstoke: Palgrave Macmillan, 2017. https://doi.org/10.1007/978-3-319-50445-2_7.