Anonymity and its Prospects in the Digital World

Thorsten Thiel

November 2017

Anonymity and its Prospects in the Digital World

Thorsten Thiel

ABSTRACT

In this working paper I will trace the changes undergone by anonymity – and by the discourses surrounding it – in liberal Western societies. I will ask whether the current politicization of the issue is likely to have any impact on the gradual disappearance of opportunities for anonymity that we are currently witnessing and argue that anonymity is an ambivalent but critical feature of the democratic public sphere. The argument proceeds in three stages. I begin with a number of conceptual observations on anonymity. From these, a heuristic framework emerges with which the changes in anonymous communication, and in the role this communication plays in society, can be described. I then analyse the extent to which options for anonymity have been affected by the revolution in information and communication technologies and conclude by considering how anonymity is framed in public discourse and what impacts this has.

1. 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 (Kaye 2015). In it, he focused on the issues of encryption and anonymity, highlighting the important role these play in regard to privacy and the right to free expression. The mere fact that such a report has been produced, and the debate it has engendered, are indicative of the high profile which the issue of anonymity has recently acquired. Anonymity itself is, of course, nothing new in human history and has long been recognized as posing problems and providing solutions in a number of domains (investigative journalism and the handling of medical data are two such areas). But the intensity of the current debate has shown just how little we actually know about anonymity – either as a normative concept or as an everyday practice. It is only in the wake of the digital turn that the topic has become politicized, in other words has been 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 digital turn, this situation has changed radically. Discourse on the topic is now not just a scholarly but also a political battleground and anonymity is widely portrayed as a cornerstone of the (normative) order governing our digital lives.

In this working paper I will trace the changes undergone by anonymity – and by the discourses surrounding it – in liberal Western societies. I will ask whether the current politicization of the issue is likely to have any impact on the gradual disappearance of opportunities for anonymity that we are currently witnessing. I will argue that anonymity is an ambivalent but critical feature of the democratic public sphere. Political, technical, economic and social developments have undermined the broad de facto anonymity of modern societies. If we want to slow down or halt this trend, or actually reverse it, it will not be enough simply to politicize 'de-anonymizing' tendencies and whip up indignation at them. Only a radical overhaul of the governance-architecture through which we address and regulate the many issues affecting the transnational digital public will enable us to counter this powerful trend. All aspects – legal, political and economic – must be tackled simultaneously.

My argument proceeds in three stages. I begin with a number of conceptual observations on anonymity. From these, a heuristic framework emerges with which the changes in anonymous communication, and in the role this communication plays in society, can be described. I then analyse the extent to which options for anonymity have been affected by the revolution in information and communication technologies (ICTs) and I conclude by considering how

anonymity is framed in public discourse and what impacts this has. My aim in this last section is to show that none of the different layers of the anonymity discourse that have taken shape so far have generated any cogent ideas as to how the all-encompassing trend to de-anonymization outlined in the second part of the paper 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. We will need to address overarching issues relating to Internet governance and the inscription of values into digital infrastructures.

2. ANONYMITY: CONCEPTUAL OBSERVATIONS[1]

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/ responsible. Greater precision can be introduced into this broad definition if we take into account four closely interrelated facts.

Firstly, 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 too gives no clue to identity. Anonymity relates to the meta-information level, not to the level of information itself.[2]

Secondly, anonymity is situational in nature. 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 also distinct from invisibility.)

Thirdly, although anonymity can be produced intentionally (through disguise, for example, or the use of a pseudonym), it can also arise de facto from a situation (as when one finds oneself in a crowd). The essence of anonymity lies in indistinguishability and anonymity therefore only succeeds where there are multiple possible authors of an action. This being so, anonymity also always depends, at least indirectly, on others' accepting it and exercising restraint – by not insisting on identification, for example, or by not attempting to single out those performing an action. To this extent, anonymity is always uncertain and gradual. No individual can be sure that their action/ communication will in fact play out anonymously – especially since the possibility of identification persists after, or indeed arises from, the action/communication. Anonymity thus always remains open-ended. Strengthening it would mean taking measures that rendered identification more difficult – by, for example, removing information from a situation.

The upshot of this, fourthly, is that anonymity is best understood and analysed in terms of its opposite – identification. Where an action or communication can be traced back to a subject susceptible of identification beyond the immediate context, the state of anonymity ceases to obtain.

---

1   On the wider debate as to how best to conceptualize anonymity, see Marx (1999); Nissenbaum (1999); Wallace (1999); Rössler (2003); Matthews (2010), and Ponesse (2014).

2   This is important when it comes to the debate about digital structural transformation, because the discussion about anonymity is directly related to the discussion about encryption, which has perhaps garnered even more interest. Although the two discussions often coincide – because content can also provide information about speakers and vice versa – the distinction between 'who' and 'what' or between information and meta-information will be maintained here for analytical purposes and attention will be focused solely on the discussion about anonymity.

Hence, anyone wishing to ascertain whether/to what degree anonymity exists in a particular situation must establish to what extent and by whom identification is possible.[3]

With these observations in mind, we can set about constructing a heuristic framework that will help us plot the course 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 in regard to peers and immediate surroundings. Such anonymity obtains 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 entities. Most notable amongst these are states, which have a broad range of means available to them to identify people, both as a situation occurs and after it. Such actors do not have to be present in the situation in order to make an identification.

This chronological aspect points to the second distinction, which relates to the fact that anonymity is not contained within present time and has necessarily also to look 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.[4] Our second distinction is therefore that between identification (which puts an end to anonymity within a situation) and identifiability (which implies/anticipates that anonymity can 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 actively to secure anonymity by introducing (effective, non-reversible) 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 recent times. Before we do this, however, we need to make a short detour through normative territory. Anonymity is, after all, most often discussed in relation to whether we have cause to fear either its spread or its demise. If, as previously proposed, anonymity is highly dependent on intersubjective constellations and situational specifics, mounting a hardline defence of it (for example, according it 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 of a general nature, these set-tos are better thought of as clashes between differing empirical expectations (examples of the kinds of contributions involved include: Akdeniz 2002; Baumann 2013; Pettit 2008; Brodnig 2013; Doyle/Veranas 2014; Gardner 2011; Christopherson 2007; Davenport 2002; Lim et al. 2011). The optimistic camp holds that facilitating anonymous communication will engender authenticity since power-relations can then be ignored and the

---

3   In this connection, it should be noted that anonymity, whilst closely related to privacy, is not reducible to it, nor is it simply a subordinate aspect of it. Thus privacy can be maintained even where identification is possible. In many ways privacy has more to do with issues of access and the control of information whereas anonymity is concerned with identification and linkage. Anonymity can serve as a powerful bulwark to privacy – including, most relevantly here, privacy of information in the digital domain – but it should be understood and discussed as distinct from it (Ponesse 2014).

4   This extension of anonymity into the future is one of the reasons why anonymity must be thought of as necessarily relative and gradual. One can never definitively exclude the possibility of being identified post eventum. Whilst all anonymization-techniques are capable of failing, the possibility of their doing so can be greater or less and – even more importantly – it is the likelihood or not of de-anonymization occurring that really drives behaviour.

individual will be able to speak freely and openly. The pessimists, by contrast, believe that giving up the possibility of holding someone to account will foster irresponsible and anti-social behaviour. These two sets of expectations are then tied into broader normative and/or theoretical 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 behaviour 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 (Gardner 2011). 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 shall follow the heuristic framework established above and trace developments in the possibilities for such communication in society. By establishing what has changed and why, we get a different view of what these developments entail and of what lessons might be learned as regards addressing them.

3. BUG OR FEATURE: A BRIEF HISTORY OF THE DEVELOPMENT OF ANONYMOUS COMMUNICATION SINCE THE DIGITAL TURN[5]

Guided by the conceptual framework laid down in the first section, we can now analyse the fortunes of anonymity since the digital turn. 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 the period in question – from, say, the 1950s to the 1980s – we have to turn our attention to the abstract matter of historical representation.

Chronicles of the modern age have often depicted it 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 are seen as precipitating the demise of community-life. Bureaucracy, pluralism and urban living are characterized as anonymous and are contrasted with trust-based communication in small-scale communities. (Even early scholars of sociology such as Weber, Durkheim and Simmel noted the ambivalent nature of this transition from community to society.) In modern society, anonymity has been experienced as negative but at the same time inevitable. It has come to be seen as a necessary by-product of the ongoing growth and differentiation of societies. Thus, although anonymity continues to be generally perceived as problematic – not just, as might be expected, by those who hold conservative world-views but also by the proponents of many, indeed most, progressive or emancipatory philosophies, which see solidarity as a potential counter to alienation – there has, at the same time, been a 'normalization' of anonymous communication. This finds expression in many of the practices and communication infrastructures of modern societies. Functional equivalents have been developed that aim to offset the drawbacks of impersonal communication. One such is juridification, which enables trust to be established in non-personalized communication-settings. Still speaking from an abstract standpoint, we also see that in the early debates, anonymity was mostly seen as relating to social structures. The conception of it as something individual and situational, and something one might voluntarily embrace, only emerges at a later stage.

Against this background, what is the situation of anonymous communication in pre-digital societies? Two facts stand out from the above account: firstly, anonymity is a feature of society that

---

points to broad development rather than intentional design; and secondly, anonymity is focused on the horizontal dimension, in other words on 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. Unless one is in a position of privilege, attempting to establish someone's identity is not only costly; it also violates social and legal norms. That said, there are (at least) two mechanisms in operation that modulate anonymity here. The first is the set of social norms which dictate that people identify themselves in certain communication-based settings (thus, not to introduce oneself is considered rude in the context of a formal conversation but not in a transaction at a news stand). The second is the presence of powerful 'gatekeepers' (such as media concerns) who control access to the wider public sphere (one-to-many communications), not only demanding identification but whittling the right of entry down even further by restricting it to the well-known or newsworthy.

Anonymity of the vertical kind also has a relatively robust profile in the pre-digital period. Although there are specific areas – such as travel and taxation – in which identification has long been mandatory and strictly enforced, outside of these contexts even well-resourced players exercise restraint in seeking to establish identity: besides being costly, it is a task that is feasible only for a limited number of individuals and has to be performed more or less openly (for example, with a straight request to the person). Whereas authoritarian regimes are keen proliferators of ID-checking opportunities, liberal states have come to recognize, and indeed to embrace, the limitations in this area. Vertically speaking also, identification has long been chiefly a matter for states and governments (in terms both of enforcement and of post eventum verification). Corporate actors play only a minor role here and are only able or inclined to enforce identification in very special circumstances. They do not have the means to identify consumers individually, nor is it vital to their commercial interests to do so.

A visual summary of the observations made so far is given in Figure 1. This points up the centrality of de facto anonymity in modern societies before the digital turn. Private, public and political spaces are mostly constituted in ways conducive to the preservation of anonymity (provided this preservation does not entail the breaking of certain written and unwritten rules). Particular privileged individuals – such as officials and celebrities – are excepted from these conventions (at least when they are moving in the public sphere) and any attempt to access a wider public brings with it a requirement for identification. At the same time, there are only a handful of actors 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 the societies of this period, 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 has to be tolerated for pragmatic reasons.

	Identification	Identifiability
Horizontal communication	- Regulated by social norms - Strong gatekeepers enforce identifiable communication in the wider public context	- Weak - Basically restricted to the immediate environment
Vertical communication	- Highly context-specific - Enforcement mainly by the state - Explicit and visible	- Low to medium - Very costly and resource-intensive - Mostly limited to states

Figure 1. Anonymous communication before the digital turn.

How, then, has the rise of ICTs influenced the discourse in this area and what effect has it had on the 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 its de-personalization.

Just from a technical point of view, the cartoon makes sense: since digital communications have to be translated into bits and bytes and then transferred via a decentralized network using numbers and protocols, every instance of such communication is in some sense pseudonymous. This circumstance brings with it a host of possibilities for covering one's tracks – a tendency further encouraged by the fact that such transactions are not tied to a particular time or space. 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 of legal enforcement. In or own times, trolling and hate speech – both closely linked to anonymity – continue to be presented in these terms. In digital environments there is also a diminution in the status of gatekeepers. Communication with large audiences becomes possible even for those who do not want to disclose their identity (still a fairly common occurrence on Twitter, for example).

The view that the digital revolution has facilitated and normalized anonymous communication with a broad public is widespread and has been reinforced by changes in the shape of collective action, which has seen the demotion of intermediary organizations and the rise of individualized 'personal action frames' (Shirky 2008; Bennett/Segerberg 2013). (This trend is perhaps most strikingly exemplified in the 'Anonymous' protest-movement and its emblem of a Guy Fawkes mask.) Even so, I wish to 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.

3.1   Three De-Anonymizing Trends are of Critical Significance in this Regard.

The first 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 set-ups. Similarly, the increased potential for storing and analysing 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 (Barocas/Nissenbaum 2014; Ohm 2010).

The second trend is *economic* and involves a massive shift in the incentives for de-anonymization. In a digitalized economy, identity becomes a driver of profits – a situation aptly summed up in descriptions of data as the new gold or new oil (Kurz/Rieger 2011; Simanowski 2014). 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 (Dean 2005; Suarez-Villa 2009; Sevignani 2013). 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 endlessly reproducible (Bunz 2004). All these developments shift electronic communication out of individual control and make it dependent on intermediaries who make vast profits from analysing behaviour and personalizing their offers accordingly.

The third de-anonymizing trend results from changes in social practice, notably the rise of social networking, with its inbuilt spur to self-portrayal and its (often forced) reduction to a single fixed identity across the Net (Andrejevic 2011; Lovink 2011). 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 – see Farrall 2012.)

Together with other developments currently taking place, these trends are resulting in anonymous communication becoming much harder to achieve. Using our 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 on the open Internet, 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.

Of much greater significance are the changes relating to vertical anonymity, where 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 have similarly extended their reach – not least by developing means of gaining access to, and combining, private data-collections. Because the digital public sphere is almost entirely privately owned and because the corporations that grant access to it have enormous leverage when it comes to collecting all kinds of personal data, identifiability has burgeoned. At the same time, technological change has increased the capacity for data-analysis to such an extent that finding a technical solution that would reconcile big data and privacy has effectively been ruled out (Barocas/Nissenbaum 2014).

Figure 2 sums up these changes and allows comparison with conditions prior to the rise of ICTs.

	Identification	Identifiability
Horizontal communication	- Steady or decreasing - Weakening of social pressures	- Medium
Vertical communication	- Many contexts require identification or set it as a default - More actors are able to enforce identification	- Medium to high - Low costs - Easy to hide

Figure 2. Anonymous communication after the digital turn.

To sum up: over recent decades, the modalities of anonymous communication have undergone major change. Although this process has been a complex one, driven by many different factors and trends, the shift away from de facto anonymity and towards a 'goldfish-bowl' society has been unmistakable (Froomkin 2015). 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 which 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, in addition, the distinction between the online and offline world is increasingly being blurred. Anonymity is not something we achieve simply by switching off our computers (or mobiles or other devices): digitalization is all-pervading, even if we do have some power to shape it (Floridi 2014).

4.   THE POLITICIZATION OF ANONYMITY

Having outlined the general trends affecting anonymity, I would now like to narrow the focus and try to determine to what extent and in what ways these developments have been addressed in public discourse in liberal societies. As the present volume impressively demonstrates, the concepts and convictions surrounding privacy have undergone enormous change in recent decades. Consequently, if we are to understand governance in this area, we need to analyse the various shifts and struggles in public discourse. Efforts at governance and regulation in this area cannot be understood solely by looking at (external) challenges such as changes in technological capacity. They need to be analysed against the backdrop of changing expectations and demands. Anonymity is of particular interest in this regard: as noted previously, it is not something that can be treated as an absolute and is not viewed in an entirely positive light; at the same time, because the shifts in both the horizontal and vertical dimensions are seen and felt so widely, it has acquired a high profile in public discourse. Any attempt to counter the structural pulls that have diminished the possibility of anonymous communication must therefore include an appreciation of the argumentative landscape and not just deplore the changes. With this in mind, what I propose to do in the rest of this paper is to gauge how far attempts to politicize anonymity have been successful 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 are in order. As I use it here, 'politicization' will not have the restricted meaning of getting an issue onto the agendas of political decision-makers. Nor will it be used in the sense of the extreme polarization of an issue. (Both of these are very common understandings of the concept.) Instead, I shall use the term in the 'republican' sense of a topic of public discourse that gives rise to a variety of alternative positions and is amenable to, and stands in need of, political resolution. Interpreted thus, politicization is

not restricted to professional politics; it also 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 in which the issue of anonymity has become politicized – but has done so in very different ways. I will show what arguments and positions have taken shape and whether success in politicization has had any impact on the meta-trend of diminishing opportunities for anonymous communication. The four areas I have selected – technical, economic, legal and socio-political – suggest themselves from my previous analysis of the push-factors operating here. As I will explain, 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 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

Of the different discursive domains, this is undoubtedly the one in which anonymity has been around the longest as an issue. 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 amongst members of what is an active civil society of hackers, privacy advocates and the like (for an overview of digital civil society, see Bennett 2008 and Beckedahl 2015). At the same time, as explained earlier, underlying technical conditions have changed enormously as a result of the growth in networked communications and the commercialization of the Internet. The idea of Internet exceptionalism has had its day and the endeavour to maintain extensive anonymity finds itself up against the interests of those whose influence is on the rise in all things cyber.

Notwithstanding these developments, the technical basis of the Internet – protocols, routing logic, and so on – still leaves considerable room for anonymization. This means that 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. In order 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 for log-in, etc.). Nowadays, many services are available only to registered users and the processes used for verification are much more advanced. As already indicated, mobile technology and the app economy have been game-changers in this respect: log-ins here are often permanent and much more meta-data – notably regarding location – is collected by default (often with no real opt-out facility).

This re-shaping 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. Examples here include alternative social networks such as Diaspora, web-anonymizers such as JonDo, and other (mostly peer-to-peer) infrastructures. Probably the most significant endeavour in this regard is TOR (The Onion Router), an anonymization network which one of the NSA slides leaked by Edward Snowden described as 'the king of high-secure, low-latency Internet anonymity'. The Snowden revelations fuelled interest in TOR and in encryption technology, but the public reaction has been mixed.

Within public discourse, technical solutions that offer anonymity are mostly framed as a form of justified civilian self-defence. Anonymity itself is depicted as a weapon with which to resist state-based and commercial data-collection and thus 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. Although there had previously been attempts to criminalize traffic using these networks, the equation of anonymizing mechanisms with fraud and other crime became much more common after Snowden – witness the high-profile legal action against Silk Road and the reputed subjection of TOR users to general surveillance, thus creating an impression of deviancy. As Helen Nissenbaum pointed out early on in regard to the hacker community, the contested ontology of cyberspace brings with it massive shifts in the normative evaluation of communication-practices even in cases where these practices themselves change little (Nissenbaum 2004).

Apart from the debate as to whether the pursuit of anonymity is more criminal or more emancipatory in character, much discussion has taken place in the technological domain about the actual feasibility of anonymity. Even individuals (such as Jonathan Zittrain – 2009) who are sympathetic to early Internet values have asked whether the communication-related ideals inherent in the Internet's architecture are applicable in relation to a multi-purpose infrastructure that is no longer the preserve of a restricted technical community.

To sum up: in the technical domain, de-legitimization discourses are on the rise but technical elites have remained firmly on the side of anonymous communication and have come up with a number of technical innovations for preserving anonymity. Because these are mostly geared to individual self-defence, often reduce ease-of-use and entail regular checks and updates, their operation is restricted to a small group of technically literate elites. Nevertheless, these tools and mechanisms are of crucial importance and technical elites have succeeded in developing a political voice that commands a degree of attention. All in all, though, the impact of these endeavours is tempered by developments in other sectors.

The Economic Domain

In the economic domain, anonymity is, as it were, 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 centred on markets and acquire much of their legitimacy by linking market exchange to the idea of freedom. The success of that linkage depends, in its turn, on the market's being non-discriminatory – because anonymously structured.

The digital turn has clearly not resulted in the abandonment of the idea of markets. What it has done, rather, is reinforce a number of trends in capitalist economics that were already at work in post-industrialist societies generally – the increased personalization of products, for example, the localization of offers and the re-centring of economies as a whole on services rather than manufacturing. In this context, anonymity emerges as an obstacle to be overcome. The approach to this problem has not been to try to discredit anonymity but to highlight the virtues of identity and identification. Services have become increasingly personalized, the prime example of this being social networking. Advertising, data-mining and (because digital goods are easy to produce and can be duplicated virtually cost-free) identifying promising Web-based business-opportunities have become core activities. This process – particularly the shift from acquisition to right of use – has fostered the development and imposition of identificatory mechanisms and classifications.

The gradual disappearance of options for anonymous communication brought about by the changing behaviour of commercial players has been attracting the attention of privacy advocates for quite some time (and lately also that of law-makers). However, although these actors have

vigorously condemned the kind of all-encompassing data-collection pursued by business, they have mostly done so without referring to anonymity as such. Discussion here has generally taken place under the rubrics of data-protection, the responsible use of data and data-minimization. Privacy not anonymity is the rallying cry. So, whilst there is, and always has been, a powerful anti-consumerist 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 comes across, legally speaking, as a complex and persistent problem. Constitutionally, attempts have been made both to establish an abstract right to anonymity and to ban it (Froomkin 1999; Kerr et al. 2009; Farrall 2012).

Discourse in the legal sphere is more nuanced than in the others discussed here. In relation to digital issues, debates about recognizing anonymity as a right, or banning it, tend to develop out of specific contexts. Thus, the critique of copyright-enforcement led to a discussion about legal responsibility in the context of peer-to-peer networks and cloud storage (Megaupload comes to mind) and this in turn triggered a debate about anonymity and the necessity of identification. State-based attempts to secure de-anonymization have included a push to data-retention, with anonymity being framed as an obstacle to the application of the law (or to the prevention of its violation). These moves have been countered with a fierce defence of data-protection and the right to 'informational self-determination'.

In the legal discourse overall, 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 sceptical about proposals for an outright ban on anonymous communications. (Of course, this does not mean that the supporters of anonymity have won the political argument: discursive framing does not translate directly into political power.) A link has been established between privacy and anonymity and courts often regard the latter to be an appropriate means of protecting the former (perhaps a naïve view, given the discussions in the technological domain).

Even if legal battles are being won, however, and the democratic rationale appears to be allowing a degree of space for anonymity, for privacy advocates to focus solely on these battles is a risky and limited strategy. Risky because when it comes to the law, the attempt to achieve a balance between privacy rights, property rights and the claims of sovereign actors to control may not always end in victory for the champions of privacy; and limited because the kinds of legal tactics involved can only be applied to certain issues and because the use of legal instruments will be a route opted for chiefly by well-resourced players.

The Socio-Political Domain

Coming finally to the general political and social 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 the mass media. The way it is framed in the public discourse continues to be more negative than positive, emphasizing the risks which anonymous communication brings with it and the anti-social behaviour 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.

The main triggers to the public debate about anonymity have been bad digital practices (such as cyber-bullying and hate-speech) and the exposure of certain state activities. Whilst the view in favour of anonymous communication is a minority one, the coalition of those espousing it is broad, extending from left-wing protest-groups to defenders of civil liberties. Although activists

often claim that not enough attention is paid to the arguments about anonymity and that there is little awareness of the problems that lie ahead, 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.

5. CONCLUDING REMARKS

The scope and diversity of discourse in these different areas is proof of the speed with which the debate on anonymity is evolving. Arguments on both sides – for and against anonymity – have become much more sophisticated and anonymity itself is now an object of political contestation rather than a minor determinant of modern life. Although politicization is clearly underway and alternative approaches for dealing with the changes entrained by digitalization are being developed, one can already foresee that establishing the connection between privacy and democracy, winning a legal battle or two and developing tools that enable us to stay one step ahead of the identifiers will not be enough to reverse the powerful trend towards de-anonymization. The forces driving us towards identification are to an extent isolated from public debate and shifting sensitivities. Hence politicization is a necessary step but not a sufficient one. To govern privacy effectively, we need to come up with configurations that allow society to retain the option of anonymity. Neither individual action (such as boycotting Facebook or the Internet as a whole) nor the imposition of strict laws will do the trick. Instead, we need to radically rethink the way the Internet is governed and develop responsive ways of building a global digital infrastructure. The goal should be an institutional set-up that facilitates the translation of public opinion into responsible policy and is robust enough to keep capitalist dynamics and governmental logic in check.

Rather than following the usual procedure in such cases and investing all hope in the centralized logic of sovereign states, consideration should be given to the creation of transnational decision-making forums that would take into account all the different debates about the benefits and risks of our digital world, and the transformations being wrought within it. The ongoing politicization of major issues affecting digital societies – as traced in the present paper – impels us to consider strong and innovative modes of governance for privacy. Fine-tuning these schemes and setting them on the road to political realization is the task of civil society and democratic politics.

References

Akdeniz, Y. 2002: Anonymity, Democracy, and Cyberspace, *Social Research*, 69(1), 223–237.

Andrejevic, M. 2011: Facebook als neue Produktionsweise, in: Leistert, Oliver/Röhle, Theo (eds.): *Generation Facebook. Über das Leben im Social Net*, Bielefeld: Transcript, 31–50.

Barocas, S./Nissenbaum H. 2014: Big Data's End Run around Anonymity and Consent, in: Lane, J./Nissenbaum, H./Stodden, V. (eds.): *Privacy, Big Data, and the Public Good*, Cambridge: Cambridge University Press, 44–75.

Baumann, Z. 2013: Das Ende der Anonymität. Was Drohnen und Facebook verbindet, *Blätter für deutsche und internationale Politik*, Oktober, 51–62.

Beckedahl, M. 2015: Die digitale Gesellschaft – Netzpolitik, Bürgerrechte und Machtfrage, *Journal of Self-Regulation and Regulation*, 1(1), 11–30.

Bennett, C.J. 2008: The Privacy Advocates: Resisting the Spread of Surveillance, Boston, MA: MIT Press.

Bennett, L.W./Segerberg A. 2013: The Logic of Connective Action: Digital Media and the Personalization of Contentious Politics, Cambridge: Cambridge University Press.

Brodnig, I. 2013: Der unsichtbare Mensch. Wie die Anonymität im Internet unsere Gesellschaft verändert, Vienna: Czernin.

Bunz, M. 2004: Die Utopie der Kopie, in: Maresch, Rudolf/Rötzer, Florian (eds.): *Rennaissance der Utopie. Zukunftsfiguren des 21. Jahrhunderts*, Frankfurt a. M.: Suhrkamp, 156–171.

Christopherson, K.M. 2007: The Positive and Negative Implications of Anonymity in Internet Social Interactions, *Computers in Human Behavior*, 23(6), 3038–3056.

Davenport, D. 2002: Anonymity on the Internet: Why the Price May be too High, *Communications of the ACM*, 45(4), 33–35.

Dean, J. 2005: Communicative Capitalism: Circulation and the Foreclosure of Politics, *Cultural Politics*, 1(1), 51–74.

Doyle, T./Veranas, J. 2014: Public Anonymity and the Connected World, *Ethics and Information Technology*, 16(3), 207–218.

Farrall, K. 2012: Online Collectivism, Individualism and Anonymity in East Asia, *Surveillance & Society*, 9(4), 424–440.

Floridi, L. 2014: The 4th Revolution. How the Infosphere is Reshaping Human Reality, Oxford: Oxford University Press.

Froomkin, M.A. 1999: Legal Issues in Anonymity and Pseudonymity, *The Information Society*, 15(2), 113–127.

Froomkin, M.A. 2015: From Anonymity to Identification, *Journal of Self-Regulation and Regulation*, 1(1), 121–138.

Gardner, J.A. 2011: Anonymity and Democratic Citizenship, *William & Mary Bill of Rights Journal*, 19(4), 927–957.

Kaye, D. 2015: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx; 13.11.2017.

Kerr, I./Lucock, C./Steeves, V. (eds.) 2009: Lessons from the Identity Trail. Anonymity, Privacy and Identity in a Networked Society, Oxford: Oxford University Press.

Kurz, C./Rieger, F. 2011: Die Datenfresser, Frankfurt a. M.: Fischer.

Lim, D./Hangjung, Z./Dukhee, L. 2011: The Value of Anonymity on the Internet, in: Jain, H./Sinha, A.P./Vitharana, P. (eds.): *Service-oriented Perspectives in Design Science Research*, Heidelberg: VS Springer, 452–464.

Lovink, G. 2011: Anonymität und die Krise des multiplen Selbst, in: Leistert, Oliver/Röhl, Theo (eds.): *Generation Facebook. Über das Leben im Social Net*. Bielefeld: Transcript, 183–198.

Marx, G.T. 1999: What's in a Name? Some Reflections on the Sociology of Anonymity, *The Information Society*, 15(2), 99–112.

Matthews, S. 2010: Anonymity and the Social Self, *American Philosophy Quarterly*, 47(4), 351–363.

Nissenbaum, H. 1999: The Meaning of Anonymity in an Information Age, *The Information Society*, 15(2), 141–144.

Nissenbaum, H. 2004: Hackers and the Contested Ontology of Cyberspace, *New Media & Society*, 6(2), 195–217.

Ohm, P. 2010: Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, *UCLA Law Review*, 57, 1701–1777.

Pettit, P. 2008: Trust, Reliance, and the Internet, in: Van den Hoven, J./Weckert, J. (eds.): *Information Technology and Moral Philosophy,* Cambridge: Cambridge University Press, 161–174.

Ponesse, J. 2014: The Ties that Blind: Conceptualizing Anonymity, *Journal of Social Philosophy*, 45(3), 304–322.

Rössler, B. 2003: Anonymität und Privatheit, in: Bäumler, H./von Mutius, A. (eds.): *Anonymität im Internet. Grundlagen, Methoden und Tools zur Realisierung eines Grundrechts*, Wiesbaden: Vieweg, 27–40.

Sevignani, S. 2013: The Commodification of Privacy on the Internet, *Science and Public Policy*, 40(6), 733–739.

Shirky, C. 2008: Here Comes Everybody, London: Penguin Books.

Simanowski, R. 2014: Data Love, Berlin: Matthes & Seitz.

Suarez-Villa, L. 2009: Technocapitalism. A Critical Perspective on Technological Innovation and Corporatism, Philadelphia, PA: Temple University Press.

Wallace, K.A. 1999: Anonymity, *Ethics and Information Technology*, 1(1), 23–35.

Zittrain, J. 2009: The Future of the Internet. And How to Stop It, London: Penguin.