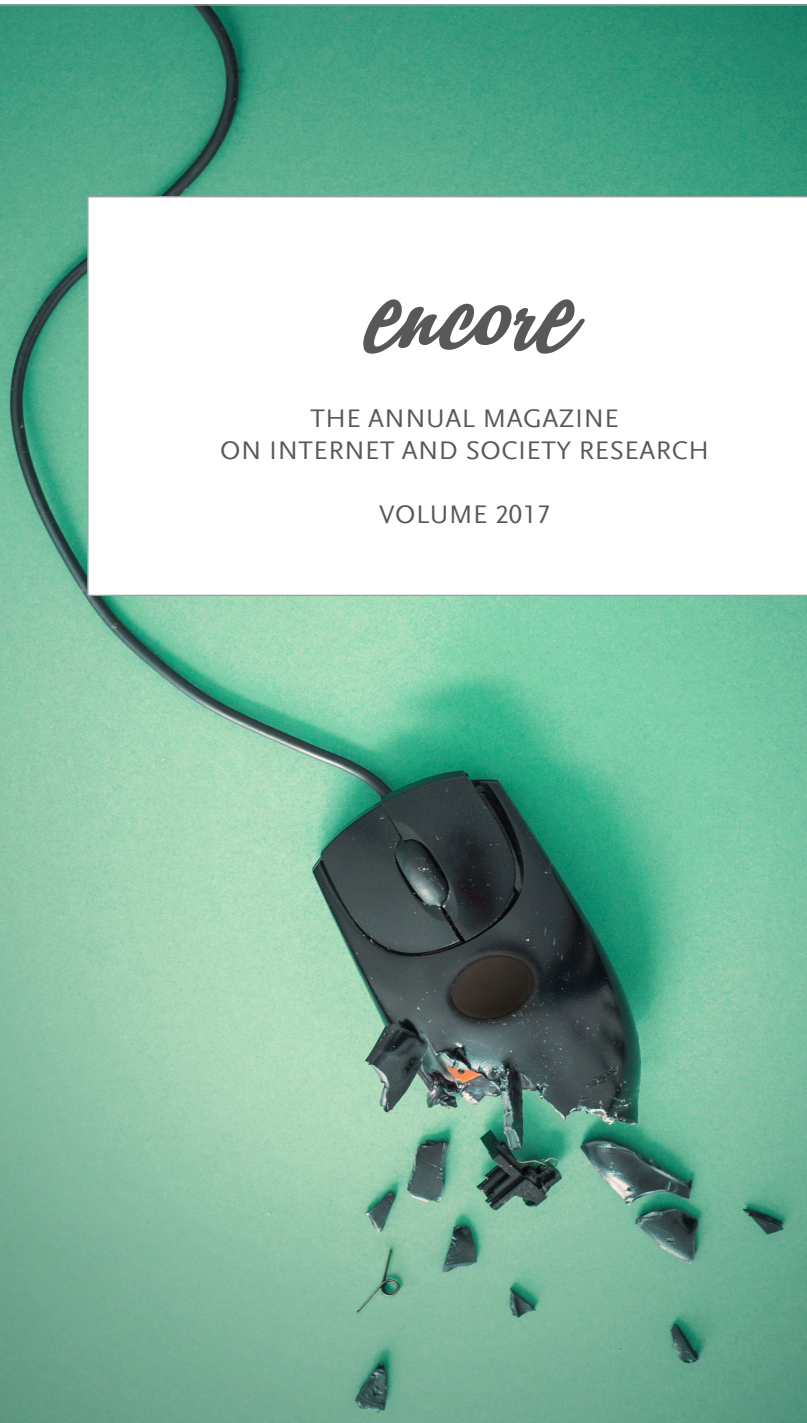
encore

THE ANNUAL MAGAZINE
ON INTERNET AND SOCIETY RESEARCH

VOLUME 2017



Metaphors shaping society · Artifical intelligence · Fake news and democracy · Open-access infrastructures · Political micro-targeting · Blockchain technology · Copyright law

encore

THE ANNUAL MAGAZINE
ON INTERNET AND SOCIETY RESEARCH

VOLUME 2017

EDITORIAL

The internet is an engine of the future. Its constantly emerging tools and infrastructures engender new ways of communicating, bring unknown kinds of information to the fore, and open up untrodden paths of interaction. Yet digital technologies are not only used to guide us in these uncharted times and to predict what comes next. They are, it seems, both predictive and progressive media. They don't wait for the future to happen but realise the utopian as well as dystopian visions that they have always already foreseen.

In these fast-forward times, *encore* cannot be a backward-looking enterprise either. Rather, it has to engage with the future-making capacity of networked services and devices. Its different formats and viewpoints assess key trends that will shape our digital lives in the days to come. With that, this year's issue presents itself as the relaunch of a successful format. The magazine highlights some of the many initiatives brought to life in the Alexander von Humboldt Institute for Internet and Society (HIIG), and it invites other scholars, practitioners and journalists to advance their perspectives on the interplay of internet and society.

The future, it seems, is materialising with increasing speed. Besides giving shape to the things to come, the social and technological environments of the internet are apparently also quickening the pace of political, cultural and economic transformations. As such, they are both welcomed and rejected as agents of acceleration. In this hurried era, finding moments to reflect upon the changes, to evaluate their impact, and to manage processes poses a formidable challenge for citizens, politicians and academics. With its broad palette of activities, HIIG is contributing to these ongoing developments. Though we occasionally seem to be riding an unstoppable juggernaut, we believe it is necessary to take the time and look to the future we want to inhabit.

Onwards and upwards!

Jeanette Hofmann
Director of the Alexander von Humboldt
Institute for Internet and Society (HIIG)

Christian Pentzold
Professor for Media Society at University of Bremen
and Associated Researcher at HIIG

CONTENT

INTERNET AND SOCIETY RESEARCH IN NUMBERS

Researchers agreeing to research data should be made publicly available in percent 76
Researchers that have made their data publicly available in percent 13

Average authors per paper in physics and astronomy 1,268
Academic article with most authors (arXiv:1503.07589) 5,154
Avg. words per author in above mentioned article 1.1

Number of words of Google Terms of Service 1,903
Number of words of Yahoo! Terms of Service 6,973
Number of words of Spotify Terms and Conditions of Use 7,909

Number of criminal requests from foreign government agencies to Evernote 3
Number of times Evernote responded with data 0

Number of requests received from governments and other parties to remove or to block access to content towards Reddit 21
Percent of requests that led to blocking/removing of content 21

Number of requests for information through legal process (search warrant) towards Slack 1
Number of requests for information through legal process (search warrant) towards Snapchat (January to June) 2,239

Value of 1 Bitcoin on 1 January 2017 in Euro	930.89
Value of 1 Bitcoin on 6 December 2017 in Euro	10,956.84
Value of 1 Bitcoin on 18 December 2017 in Euro	16,090.81
Avg. energy consumption per Bitcoin transaction in kWh	215.0000
Avg. energy consumption per Google search in kWh	0.0003
Avg. energy consumption to boil water for one cup of tea in kWh	0.0250
Number of webpages on archive.org	279,000,000,000
Number of books and texts on archive.org	11,000,000
Number of videos (including 160,000 live concerts) on archive.org	3,000,000
Number of Wikipedia articles in English	5,530,951
Number of Wikipedia articles in Cebuano*	5,382,965
Number of Wikipedia articles in Swedish	3,790,061
Number of Wikipedia articles in German	2,127,386
Number of Wikipedia articles in French	1,933,439
Number of articles written by bot Lsjbot (Cebuano*, Swedish, Wáray-wáray* articles)	9,400,000
Number of articles written by bot Cheers!-bot (Vietnamese articles)	562,000
Number of articles written by bot Joopwikibot (Dutch articles)	521,000

* Cebuano and Wáray-wáray are languages spoken on the Philippines.

CHRISTIAN KATZENBACH AND STEFAN LARSSON

Imagining the Digital Society – Metaphors from the Past and Present

The current rapid social and technological change is giving rise to enormous uncertainties – and a great need for explanation and sense-making. How do we understand the digital society? When we talk about the future that we cannot know and a present that we do not understand, we have no option but to use the conceptual apparatus of the past – with normative, social and economic implications. This primer introduces a series of essays on the politics of metaphors in the digital society. It aims to uncover the hidden assumptions and concepts within our discourses of the digital, piece by piece.

DIGITAL TRANSFORMATIONS – AND THE NEED FOR SENSE-MAKING

We are living in a time of transformation. The digitalisation of nearly every aspect of contemporary society is bringing about profound changes in politics, economics, culture, and our everyday lives. How can democracy be organised in the digital context? What are the implications of widespread automation and artificial intelligence for businesses and whole economies? What role do major internet companies play in organising and curating communication and information? The current rapid social and technological change is giving rise to enormous uncertainties – and a great need for explanations and sense-making.

When we talk about the future, we have no option but to talk in terms of the past and the present. Imagining the future is always mobilising the past. Hence, it is no surprise that we routinely use existing concepts and well-known phenomena to describe emerging things and developments, leading to a conceptual path dependence of sorts: should we understand Uber as a taxi company, an employer or merely a software developer? Should Facebook be understood as an algorithmically dependent platform, or as a publishing house that is liable for what it publishes? Should the file sharing site The Pirate Bay have been regarded as an infrastructure, a storage facility or a bulletin board? This is not merely playing with words; existing notions entail normative assumptions and create regulatory implications.

Emerging phenomena typically lack a name, so we apply existing words to a new thing, although they might technically not be applicable. But metaphors, as George Lakoff famously put it, are not merely figures of speech, they are figures of thought. In consequence, by talking about the ongoing transformations using the terms of the past, we are also making sense of the present future and the changes that come about with the conceptual apparatus of the past, with all the associated normative, social and economic implications.

A SERIES ON THE POLITICS OF METAPHORS

Against this backdrop, it is obvious why talking about the digital society and the ongoing transformations in politics, economics and culture is pervaded by metaphors. Indeed, metaphors such as cloud, platform and big data are already so much part of the current discourse that they are barely recognisable as such. In the early days of the internet, information superhighway or the world wide web itself were dominant notions to describe the emerging infrastructure.

The aim of this series is to learn something about the currently evolving digital society by unlocking the metaphors we apply. Our assumption is that this will shed light on the future that we cannot know – and even the present that we do not understand. And as metaphors are not merely words, this is a genuinely political process. Every notion, every metaphor is loaded: it provides a frame for understanding and evaluating a new phenomenon – but in many cases, we could just as easily use different notions, which in turn might be contested by competing frames and metaphors. In that way, our discourse on the digital society is contingent – it could be different. The copyright discourses have provided ample examples of this discursive struggle: piracy and stealing have strongly dominated the discourse on copyright reform, yet digital copying could easily be described differently, with vast political and regulatory implications. But what are the less obvious implications that metaphors like platform, cloud and big data entail?

The following three essays of the ongoing series will uncover the hidden assumptions and concepts within our discourses of the digital which circulate existing or establish new metaphors. This is not only important for understanding the emerging digital society: it is pivotal for shaping it. ◆

ESSAYS ON THE POLITICS OF METAPHORS IN THIS MAGAZINE

THIS IS AN ARTICLE BY **CHRISTIAN KATZENBACH AND STEFAN LARSSON**

This primer was first published on 15 May 2017 as the introduction to the dossier on How metaphors shape the digital society on the Science Blog of Alexander von Humboldt Institute for Internet and Society (HIIG). The series was edited by Christian Katzenbach, researcher at HIIG and Stefan Larsson from Lund University Internet Institute.

Christian Katzenbach's research addresses the intersection of technology, communication, and governance. He is a co-initiator of the open access journal Internet Policy Review and co-editor of the open access book series Digital Communication Research. He is head of the research department Internet Policy and Governance and lead researcher for the research programme The Evolving Digital Society at HIIG. Christian Katzenbach is co-chair of the section Digital Communication of the German Association for Media and Communication Research. He studied media and communication studies, philosophy, and computer science in Berlin, Madrid and Potsdam. Before joining the HIIG, he was a research associate and lecturer at the Institute for Media and Communication Studies at the Freie Universität Berlin where he received his PhD with a thesis on media governance and technology.

Stefan Larsson is an Associate Professor in Technology and Social Change at Lund University Internet Institute (LUii) in Sweden. He holds a PhD in the sociology of law as well as in spatial planning, and an LLM. His research is mostly related to digitally mediated socio-legal change, including issues of online traceability, big data and privacy as well as digital consumption, and theoretical combinations of cognitive theory and sociology of law. He is currently finishing a book called Conceptions in the Code: How Metaphors Explain Legal Challenges in Digital Times, published at Oxford University Press early 2017. He is a member of the scientific board of the Swedish Consumer Agency and was a visiting researcher at HIIG in Berlin in 2016.

TARLETON GILLESPIE

The platform metaphor, revisited

The most successful internet businesses are based on the idea of offering a platform. Tarleton Gillespie discusses the hidden meaning of this popular and widely accepted metaphor and reveals how it serves businesses.

Sometimes a metaphor settles into everyday use so comfortably, it can be picked back up to extend its meaning away from what it now describes, a metaphor doing metaphorical service. Platform has certainly done that. When I first wrote about the term in 2010, social media companies like YouTube and Facebook were beginning to use the term to describe their web 2.0 services, to their users, to advertisers and investors, and to themselves. Now social media companies have embraced the term fully, and have extended it to services that broker the exchange not just of content or sociality but rides (Uber), apartments (AirBnB) and labour (Taskrabbit). The term so comfortably describes these services that critics and commentators can draw on the word to extend out for the purposes of argument. The past few years have witnessed a "platform revolution", (Parker, van Alstyne & Choudary, 2016) the rise of "platform capitalism" (Srnicek, 2016) driven by "platform strategy" (Reillier & Reillier, 2017), with the possibility of "platform cooperativism" (Scholz, 2016) all part of "the platform society" (van Dijck, Poell & DeWaal, forthcoming). These books need not even be referring to the same platforms (they all have their favourite examples, somewhat overlapping); their readers know what they're referring to.

FROM PROGRAMMABILITY TO OPPORTUNITY

As platform first took root in the lexicography of social media, it was both leaning on and jettisoning a more specific computational meaning: a programmable infrastructure upon which other software can be built and run, like the operating systems in our computers and gaming consoles, or information services that provide APIs so developers can design additional layers of functionality. The new use shed the sense of programmability, instead drawing on older meanings of the word (which the computational definition itself had drawn on): an architecture from which to speak or act, like a train platform or a political stage. Now Twitter or Instagram could be a platform simply by providing an opportunity from which to speak, socialise and participate.

At the time, some suggested that the term should be constrained to its computational meaning, but it's too late: platform has been widely accepted in this new sense – by users, by the press, by regulators, and by the platform providers themselves. I argued then that the term was particularly useful because it helped social media companies appeal to several

different stakeholders of interest to them. Calling themselves platforms promised users an open playing field for free and unencumbered participation, promised advertisers a wide space in which to link their products to popular content, and promised regulators that they were a fair and impartial conduit for user activity, needing no further regulation.

This is what metaphors do. They propose a way of understanding something in the terms of another; the analogy distorts the phenomenon being described, by highlighting those features most aligned with what it is being compared to. Platform lent social media services a particular form, highlighted certain features, naturalised certain presumed relations, and set expectations for their use, impact and responsibility. Figuratively, a platform is flat, open, sturdy. In its connotations, a platform offers the opportunity to act, connect, or speak in ways that are powerful and effective: catching the train, drilling for oil, proclaiming one's beliefs. And a platform lifts that person above everything else, gives them a vantage point from which to act powerfully, a raised place to stand.

WHAT METAPHORS HIDE

Metaphors don't only highlight; they also downplay aspects that are not captured by the metaphor. "A metaphorical concept can keep us from focusing on other aspects of the concept that are inconsistent with that metaphor" (Lakoff & Johnson, 1980, p. 10). We might think of this as incidental or unavoidable, in that any comparison highlights some aspects and thereby leaves others aside. Or we could think of it as strategic, in that those deploying a metaphor have something to gain in the comparison it makes, presumably over other comparisons that might highlight different aspects.

By highlighting similarities – social media services are like platforms – metaphors can have a structural impact on the way we think about and act upon the world. At the same time, metaphor cannot be only about similarity – otherwise the ideal metaphor would be tautological, "X is like X." Metaphor also depends on the difference between the two phenomena; the construction of similarity is powerful only if it bridges a significant semantic gap. Steven Johnson points out that "the crucial element in this formula is the difference that exists between 'the thing' and the 'something else.' What makes a metaphor powerful is the gap between the two poles of the equation." (Johnson, 1997, p. 58 – 59) Phil Agre goes further, suggesting that "metaphors operate as a 'medium of exchange'" (Agre, 1997, p. 37) between distinct semantic fields, negotiating a tension between elements that are, at least in some ways, incompatible. This structural bridge constructed by metaphor depends on choosing aspects of comparison that will be

continue reading on page 16 ▸▸

THIS IS AN ARTICLE BY **TARLETON GILLESPIE**

This essay was first published on 24 August 2017 within the dossier How metaphors shape the digital society on the Science Blog of Alexander von Humboldt Institute for Internet and Society (HIIG).

Tarleton Gillespie is a principal researcher at Microsoft Research, an affiliated Associate Professor in Cornell's Department of Communication and Department of Information Science, co-founder of the blog Culture Digitally, author of Wired Shut: Copyright and the Shape of Digital Culture (MIT, 2007), co-editor of Media Technologies: Essays on Communication, Materiality, and Society (MIT, 2014), and the author of the forthcoming Custodians of the Internet (Yale, 2018).

salient and rendering others insignificant. The platform metaphor does a great deal of work, not only in what it emphasises, but in what it hides:

Platform downplays the fact that these services are not flat. Their central service is to organise, structure and channel information, according both to arrangements established by the platform (newsfeed algorithms, featured partner arrangements, front pages, categories) and arrangements built by the user, though structured or measured by the platform (friend or follower networks, trending lists). Platforms are not flat, open spaces where people speak or exchange, they are intricate and multi-layered landscapes, with complex features above and dense warrens below. Information moves in and around them, shaped both by the contours provided by the platform and by the accretions of users and their activity – all of which can change at the whim of the designers. The metaphor of platform captures none of this, implying that all activity is equally and meritocratically available, visible, public, and potentially viral. It does not prepare us, for example, for the ability of trolls to organise in private spaces and then swoop together as a brigade to harass users in a coordinated way, in places where the suddenness and publicness of the attack is a further form of harm.

The platform metaphor also obscures the fact that platforms are populated by many, diverse, sometimes overlapping, and sometimes contentious communities. It is absurd to talk about Facebook users, as if two billion people can be a single group of anything; talk about the Twitter community only papers over the tension and conflict that has been fundamental and sometimes destructive to how Twitter is actually used. As Jessa Lingel (2017) argues, social media platforms are in fact full of communities that turn to social media for specific purposes, often with ambivalent or competing needs around visibility, pseudonymity and collectivity; then they struggle with how the platforms actually work and their sometimes ill fit with the aims of that community. When we think not of "Facebook users" but a group of Brooklyn drag queens, the relationship between users and platform is not an abstract one of opportunity, but a contentious one about identity and purpose.

Platform also helps elide questions about platforms' responsibility for their public footprint. Train platforms are not responsible for the passengers. Like other metaphors such as conduit and media and network, platform suggests an impartial between-ness that policymakers in the US are eager to preserve – unlike European policymakers, where there is more political will to push responsibility onto platforms, though in a variety of untested ways. When, as Napoli and Caplan (2016) point out, Facebook refuses to call itself a media company, they are disavowing the kind of public and policy expectations imposed on media. They're merely a platform. In the meantime, they

have each built up a complex apparatus of content moderation and user governance to enforce their own guidelines, yet these interventions are opaque and overlooked.

Finally, platform hides all of the labour necessary to produce and maintain these services. The audience is not supposed to see the director or the set decorators or the stagehands, only the actors in the spotlight. Underneath a platform is an empty, dusty space – it's just there. Social media platforms are in fact the product of an immense amount of human labour, whether it be designing the algorithms or policing away prohibited content. When we do get a glimpse of the work and the workers involved, it is culturally unexpected and contentious: the revelation, for example, that Facebook's Trending Topics might have been curated by a team of journalism school grads, working like machines. (Gillespie 2016a, 2016b) What if they make mistakes? What if they are politically biased? How are humans involved, and why does that matter? Platform discourages us from asking these questions, by leaving the labour out of the picture.

There is no use in discarding the term just to swap in another metaphor in its place. It is not as if it's impossible to think about these obscured aspects of platforms; the metaphor can downplay them, but cannot erase them. But we have to either struggle upstream against the discursive power of the term or playfully subvert it. A platform may hide the labour it requires, but in a different framework it could be asked to shelter that labour, protect it. If a platform lifts up its users, then there may be some manner of responsibility for lifting some people up over others. We might also play with other metaphors: are platforms also shopping malls, or bazaars? Amusement parks, or vending machines? Nests, or hives? Pyramids, or human pyramids? But mostly, we can scrutinise the metaphor in order to identify what it fails to highlight, how that may serve the interest of the metaphor's practitioners, and what design interventions and obligations might best attend to these gaps and obscurities. And, as Kuhn (1962) notes about scientific paradigms, any frame of understanding works to coalesce the phenomenon by leaving off aspects that do not fit – and these discarded aspects can return to challenge that frame and sometimes tear it down. Platforms downplay these aspects at their own peril. ◆

REFERENCES

Agre, P. (1997). *Computation and Human Experience*. Cambridge: Cambridge University Press.

van Dijck, J., Poell, T., & de Waal, M. (forthcoming). *The Platform Society: Public Values in a Connective World*. Oxford: Oxford University Press.

Gillespie, T. (2010). The politics of "platforms." *New Media & Society, 12*(3), 347 – 364.

Gillespie, T. (2016a, May 9). Facebook Trending: It's made of people!! (but we should have already known that). [Blog post]. Retrieved from http://culturedigitally.org/2016/05/facebook-trending-its-made-of-people-but-we-should-have-already-known-that

Gillespie, T. (2016b, May 18). Algorithms, clickworkers, and the befuddled fury around Facebook Trends. [Blog post]. Retrieved from http://culturedigitally.org/2016/05/facebook-trends

Johnson, S. (1997). *Interface Culture: How New Technology Transforms the Way We Create and Communicate*. San Francisco: HarperEdge.

Kuhn, T. S. (1962). *The Structure of Scientific Revolutions*. Chicago, IL: University of Chicago Press.

Lingel, J. (2017). *Digital Countercultures and the Struggle for Community*. Cambridge, MA: The MIT Press.

Napoli, P. M., & Caplan, R. (2016). When Media Companies Insist They're Not Media Companies and Why It Matters for Communications Policy. *Telecommunications Policy Research Conference, Arlington, VA*.

Parker, G. G., Alstyne, M. W. V., & Choudary, S. P. (2016). *Platform Revolution: How Networked Markets Are Transforming the Economy – And How to Make Them Work for You*. New York: W. W. Norton & Company.

Reillier, L. C., & Reillier, B. (2017). *Platform Strategy: How to Unlock the Power of Communities and Networks to Grow Your Business*. Routledge.

Scholz, T. (2016). *Platform Cooperativism. Challenging the Corporate Sharing Economy*. New York: Rosa Luxemburg Stiflung. Retrieved from http://ictlogy.net/bibliography/reports/projects.php?idp=3111

Srnicek, N. (2016). *Platform Capitalism*. Cambridge, UK: Polity.

JOSÉ VAN DIJCK

The platform as pizza: towards a taxonomy of platforms

The platform metaphor is at once inevitable and misleading. What's more, we no longer regard it as a metaphor. Following Tarleton Gillespie's proposal to diversify the discourse by adding other images, José van Dijck picks up the challenge playfully and comes up with another term. What she suggests sounds a little odd at first. However, when we ask ourselves what difficulties in understanding arise when using the term platform, it makes perfect sense.

For the past decade, many researchers in media and communication studies have used the term platform to theorise the technological, economic and/or socio-cultural constructions designed to organise both online and offline interactions between users. Gillespie's seminal article on the politics of platforms (2010) was the first to critically investigate the platform as a sweeping common denominator. Anne Helmond (2015), assistant professor of new media and digital culture at the University of Amsterdam proposed the term "platformisation" to signify the transformation of the web into a collection of interconnected APIs that allow platforms to more easily collect data beyond themselves. More recently, my colleagues Thomas Poell, Martijn de Waal and I have broadened platformisation so that it goes beyond just the technical transformation of the web and also connects economic, social, and political perspectives that inform its logic. As we argue in our forthcoming book, The Platform Society, the global assemblage of networked platforms and their underpinning mechanisms strongly affects the (re)organisation of societies and industries. In his article (page 12), Tarleton Gillespie emphasises why the platform metaphor is at once inevitable and misleading. While the term highlights certain aspects of online services (equality, openness, sturdiness), it dangerously downplays others (they are not flat, they are populated by diverse communities, and evade questions of responsibility). Perhaps the problem with platform is that the term is no longer regarded a metaphor. Tarleton does not want to jettison the platform metaphor altogether, arguing: "There is no use in discarding the term just to swap in another metaphor in its place." I could not agree more. There is not necessarily one right metaphor. Perhaps we have to play around with a few metaphors to figure out the various meanings and effects. So, let me attempt to pick up the challenge in this article and test a counter-metaphor – an alternative understanding of a common image in order to highlight heretofore invisible aspects of the phenomenon at hand. (I warn you, though: I will not succeed.)

NOT A LEVEL PLAYING FIELD

First of all, we need a metaphor that somehow refutes the platform's connotation of openness and equality. The online world is not a level playing field: some platforms are more equal than others. There is a difference between what we could call infrastructural information services (Platin, Lagoze, Edwards & Sandvig, 2016) and others. Many infrastructural services – but not all – are owned and operated by the big five tech companies (Alphabet-Google, Facebook, Amazon, Apple and Microsoft). They form the heart of the online system, on top of which many other layers of platforms can be built. Infrastructural services include search engines and browsers, data and cloud servers, email and instant messenger services, social networking services, advertising networks, app stores, payment systems, identification services, data analytics services, video services, streaming music stores, geospatial and navigation tools, and a growing number of other services.

These infrastructural information services function as online gatekeepers through which data flows are managed, processed, stored and channelled; some have argued they function more or less as utilities or superstructures because they provide a crucial yet dynamic and ever-changing foundation upon which other apps can be built (Andersson Schwarz, 2017). Plantin, Lagoze, Edwards & Sandvig (2016) raise the question whether these central nodes operated and owned by a few builders should be considered platforms, infrastructures, utilities or all three at the same time. The quintessence of their argument is that all infrastructural information services are becoming "platformised", while major platforms are turning into essential infrastructures or even utilities.

A TAXONOMY OF PLATFORMS

Thousands of platforms are stacked onto this infrastructural core and have become more or less dependent on it to profit from its network effects. For instance, Airbnb embeds Google Maps as a standard feature in its interface; it also incorporates Facebook and Google+ identification services to clear hosts and guests. Spotify's services run on Google Cloud and Netflix is dependent on Amazon Web Services. Public and non-profit platforms often rely on Facebook or Google for their login facilities, search ranking visibility, and most importantly, to reach substantial groups of users. Distinguishing between 'infrastructural services and other platforms is far from trivial. It is important to provide a refined taxonomy of platforms to show how some information services are shaping societal order.

Any attempt to spell out such a taxonomy of platforms makes one aware of the term's slippery meanings. What exactly is the function of a platform: can it be characterised as

continue reading on page 24 ▸▸

THIS IS AN ARTICLE BY **JOSÉ VAN DIJCK**

This essay was first published on 5 October 2017 within the dossier How metaphors shape the digital society on the Science Blog of Alexander von Humboldt Institute for Internet and Society (HIIG).

José van Dijck is a professor of Comparative Media Studies at the University of Amsterdam and president of the Royal Netherlands Academy of Arts and Sciences. Within the research area of media studies and communication her work covers a wide range of topics in media theory, media technologies, social media, and digital culture. José van Dijck has been appointed a distinguished university professor at Utrecht University as of January 2017. She graduated from Utrecht University in 1985 and received her PhD in Comparative Literature from the University of California, San Diego (UCSD) in 1992. Van Dijck worked at the Universities of Groningen and Maastricht before she became a full professor at the University of Amsterdam in 2001. She served as Chair of the Department of Media Studies from 2002 – 2006, and was the Dean of the Faculty of Humanities at the University of Amsterdam between 2008 and 2012. In 2015 she was elected President of the Royal Netherlands Academy of Arts and Sciences where she will serve a 3-year term until June 2018. She is author of the book The Culture of Connectivity: A Critical History of Social Media and co-author of the book The Platform Society (with Thomas Poell).

tech infrastructure (utility), does it provide a connective service (connecting supply and demand) or is it a sectoral service? Can a platform be held responsible for products or services it connects but does not produce? For online businesses, there is a lot at stake in maintaining a vague, elusive cluster of concepts around platforms and operators as connectors of 'users.' Uber denies it is a taxi service – a case that is currently being tried in the European Court; and Facebook has long disavowed responsibility as a media company even though it is responsible for distributing almost half the news in the US. A precise taxonomy of platforms, which is so far lacking, could be used to help guide legislators in updating their regulatory frameworks, for instance, with regards to antitrust or competition law. More generally, it could help politicians and governments decide what responsibilities tech companies bear vis-à-vis their online services and products.

PLATFORM AS PIZZA

To dissect the now common term platform, which often positively connotes innovative disruption, we need to come up with a new and powerful image that highlights the unequal nature of the global platform constellation. Here is my imperfect attempt: the platform as pizza.

If the platform were a pizza, the pre-baked pizza crust would be made in the USA, most likely by the big five companies, and exported to the world for everyone to finish into a full-fledged pizza. The crust would contain a number of ingredients, including flour, salt and sugar, defining the taste of the finished product. Baked into the crust would be a value system that privileges proprietary data, commodification mechanisms and personalisation. Pre-baked crusts can be imported anywhere in the world to be turned into ready-made pizzas or other products. Toppings can be added by all kinds of individuals, organisations (for-profit, non-profit), and governments. Different kinds of toppings could be stacked onto the pizza crust and could be combined to accommodate idiosyncratic tastes. For instance, cheese and tomato sauce could first be added as connectors: they connect the crust with the subsequent toppings. Pepperoni, mushrooms, seafood, bell peppers or any other kind of topping represents the sectoral layers added onto the basics. The pre-baked dough has become indispensable as a foundation for professional and amateur chefs around the world; indeed, they can be very creative in preparing customised pizzas tailored towards everyone's taste. Although personalisation of pizzas is often in the variety of toppings we can add, they are invisibly standardised by certain mechanisms. Pizzas come nearly always on round plates, they are meant to be sliced in standardised portions and the pizza crust almost begs for the standard toppings that make them so popular around the world.

EACH METAPHOR IS LIMITED. WHAT'S YOUR TAKE?

The metaphor highlights some aspects of platformisation, but, like any metaphor, it is rather inadequate in other respects. For instance, the pizza made of crust and toppings helps explain the hierarchical difference between infrastructural and sectoral platforms stacked onto each other, but it does little to elucidate the power asymmetry between the base and the stacked toppings. And while the pizza metaphor rightly emphasises the endless dynamic between platform operators, users and (personalised) services, it is also limited in scope. For instance, the influence of platform mechanisms structuring user activity goes much deeper than the standardisation of round pizzas and slices. The platform as pizza is not nearly as powerful as the widely known concept of McDonaldisation. After all, people do not have to eat pizza for breakfast, lunch and dinner.

Food metaphors, perhaps, are always tricky when used to elucidate something that is more than a gastronomic concept. The complexity of platforms as technological, political, social and economic entities is what makes them so difficult to capture in a single simple metaphor. Counter-metaphors are important and potentially powerful. However, it may take another book to work out a stronger and more elaborate image to explain the complex constellation of platforms that has become our online world. ◆

REFERENCES

Anderson Schwarz, J. (2017). Platform logic: An interdisciplinary approach to the platform-based economy. *Policy & Internet*.

Helmond, A. (2015). The platformization of the web: Making web data platform ready. *Social Media & Society, 1*(2) 1 – 11.

Plantin, J. C., Lagoze, C., Edwards, P. N., & Sandvig, C. (2016). Infrastructure studies meet platform studies in the age of Google and Facebook. *New Media & Society*.

#COVFEFE

Coffee? Coughing? Or just press coverage? While the meaning of this hashtag used by Donald Trump in May 2017 might never be fully revealed, it was shared 100,000 times within six hours before it was deleted. This incident showcases how social media has pushed the boundaries of political communication online: from serious to emotional, announcement to obscenities, humorous to plain absurd. Everything goes and nothing counts?

CHRISTIAN DJEFFAL

AI – A metaphor or the seed of personality of machines in a digitised society?

Is artificial intelligence a metaphor, or can machines be intelligent in the same way human beings are? This has been a contested question ever since the concept was developed. While the so-called weak AI thesis has treated it as a metaphor, the strong AI thesis takes intelligence literally. The answer to this question might point to the future role of intelligent machines in the digital society.

Will computers, robots and machines one day be considered intelligent persons? Will automatic agents imbued with artificial intelligence become members of our society? The concept of personality is fluid. There were times when slaves had no personality rights. Recently, there has been a growing movement arguing that legal personality should be conferred upon animals. Hence, our concept of personality might change in the course of the digitisation of society. This might be due to advances in artificial intelligence, but also to the way the term is framed.

Is artificial intelligence a metaphor or a descriptive concept? This question cannot be answered in one way or another as there is a semantic struggle surrounding the concept of artificial intelligence. As will be shown, some people treat artificial intelligence rather as a broad metaphor for the ability of machines to solve specific problems. Others take it word for word and conceive of artificial intelligence as being the same as human intelligence. Some researchers go as far as to reject the concept completely. To shed more light on the issue, it is worth going back to the time when the term was coined.

HISTORICAL ORIGINS

Artificial intelligence was first used in 1956 in Dartmouth, New Hampshire, where John McCarthy, Claude Shannon and Marvin Minsky organised a six-week summer workshop supported by the Rockefeller foundation. They introduced their grant application in the following terms:

> "The study is to proceed on the basis of the conjecture that every aspect of learning or any other feature of intelligence can in principle be so precisely described that a machine can be made to simulate it. An attempt will be made to find how to make machines use language, form abstractions and concepts, solve kinds of problems now reserved for humans, and improve themselves" (McCarthy, Minsky, Rochester, & Shannon 1955).

Interestingly, even the organisers of the conference did not really approve of the term artificial intelligence. John McCarthy stated that "one of the reasons for inventing the term 'artificial intelligence' was to escape association with 'cybernetics'", as he did not agree with Norbert Wiener (Bloomfield, 1987). Yet, the term artificial intelligence was used frequently. Today, it constitutes a subdiscipline of computer science.

THE WEAK AI THESIS VS THE STRONG AI THESIS

As can be seen from the statement above, there has always been an ambiguity to the term. This statement can be taken to mean that every aspect of human intelligence can be replicated. Yet, it can also be interpreted as a conjecture, as the use of the word simulate suggests artificial and human intelligence remain different. The different interpretations of artificial intelligence have been conceptualised as the *strong* and *weak AI* thesis. The strong AI thesis suggests that such a simulation in fact replicates the mind and that there is nothing more to the mind than the processes simulated by the computer. On the contrary, the weak AI thesis suggests that machines can act as if they were intelligent. The weak AI thesis transfers the concept of intelligence to a context in which it normally would not apply. Therefore, the term intelligence is used in a metaphorical sense in the context of weak AI.

One of the active proponents of the concept of weak AI was Joseph Weizenbaum, a Jewish German-American computer scientist who was responsible for some important technical inventions, but who remained critical of the societal impacts of computers. He programmed the famous chatbot ELIZA (Manifestation.com, 1999). Weizenbaum used a few formal rules for the chatbot to keep the conversation going. The chatbot analyses the sentence structure and grammar of what its counterpart has just said and either rephrases it as a question or replies with a standard utterance.

The proponents of the thesis of strong artificial intelligence have tried to find ways to replicate processes in the brain, for example, by designing neural networks. The strong artificial intelligence thesis suggests that machines can be intelligent in the same way as human beings can. One of the proponents of the strong AI thesis, Klaus Haefner, once had an exchange with Weizenbaum (Weizenbaum, Haefner & Haller, 1992). They used arguments that were already foreseen by Alan Turing in his seminal text Computing, Machinery and Intelligence (Turing, 1950). He famously replaced the question "Can machines think?" with an imitation game. In this game, the interrogator has a written conversation with one human being and one machine, both of which are in separate rooms. The task Turing describes is to design a machine that acts

continue reading on page 32 ▸▸

THIS IS AN ARTICLE BY **CHRISTIAN DJEFFAL**

This essay was first published on 17 May 2017 within the dossier on Politics of metaphors in the digital society on the Science Blog of Alexander von Humboldt Institute for Internet and Society (HIIG).

Christian Djeffal is a legal scholar and his research interests lie in the fields of artificial intelligence, eGovernment, data protection and security, freedom of information as well as digitisation of scholarship. He works on artificial intelligence from the perspective of public law, covering different aspects from design to regulation. At HIIG he is project leader of the project IoT and eGovernment and coordinates the research department Global Constitutionalism. Christian Djeffal studied law at Ludwig-Maximilians-University Munich and at University College London. He received his PhD at Humboldt-University of Berlin for his thesis Static and Evolutive Treaty Interpretation while working as research assistant to Georg Nolte. He has been visiting scholar at University of Amsterdam, University of Cambridge, and the Max-Planck-Institute for Comparative Public Law and International Law in Heidelberg. Christian Djeffal is the coordinator of the German International Law in Domestic Courts Team that helps to build the transnational database Oxford Reports on International Law. He is member of the scientific advisory board of Goettingen Journal of International Law and member of the German National eGovernment Centre (NEGZ).

such that the interrogator cannot distinguish it from the human being based on its communication. Therefore, the goal is not to design a system that equals a human being, but one that acts in such a way that a human being cannot tell the difference. Whether this is achieved by replicating the human brain, or in any other way, was not important for Turing.

FLYING DIFFERENT THAN BIRDS

In the literature on AI, the possible advances of the field are compared to other technologies like aeroplanes. Early models tried to simulate birds, while in the end, airplanes manage to fly in a very different way. One aim of Turing's article was to shift the focus from a general and teleological debate to the actual problems to be solved. According to his approach, there is no great general solution to the question of what AI can achieve in the future, but there are many small improvements to machines.

There might be a day when we suddenly realise that in many respects the line between humans and machines is a blurry one. Games like chess or Go are examples of problems in which machines have surpassed humans. If this trend continues, it might give a completely different connotation to the term digital society. While we cannot say that we are there yet, does that mean it can never happen? Try "bot or not" (Schwartz & Laird, n.d.), an adaptation of the Turing test for poems (ibid.). You will find that even today, it can be tricky to distinguish machines from human beings. ◆

REFERENCES

Bloomfield, B. P. (1987). *The question of artificial intelligence: Philosophical and sociological perspectives.* London: Croom Helm.

Manifestation.com. (1999). *Eliza, computer therapist.* Retrieved from http://www.manifestation.com/neurotoys/eliza.php3?log=&input=Hallo+Eliza

McCarthy, J., Minsky, M., Rochester, N., & Shannon, C. (1955). *A Proposal for the dartmouth summer research project on artificial intelligence.* Retrieved from http://www-formal.stanford.edu/jmc/history/dartmouth/dartmouth.html

Schwartz, O., & Laird, B. (n.d.). *Bot or not: The bot poet.* Retrieved from http://botpoet.com/

Turing, A. (1950). Computing, Machinery and Intelligence. *Mind, 59*(236), 433 – 460.

Weizenbaum, J., Haefner, K., & Haller, M. (1992). *Sind Computer die besseren Menschen? Ein Streitgespräch.* München, Zürich: Piper.

“Machines cannot be creative in the same way that artists can be creative.”

UNDERSTANDING ARTIFICIAL INTELLIGENCE
INTERVIEW WITH ALJOSCHA BURCHARDT

Artificial intelligence is a controversial and much-discussed topic of our digital future. Aljoscha Burchardt, lab manager at the Language Technology Lab of the German Research Center for Artificial Intelligence (DFKI), sees a huge gap between the machines of today, which are able to act intelligently, and the quest for actually being intelligent in a truly human sense. With a background in semantic language technology, his interests include the evaluation of (machine) translation quality and the inclusion of language professionals in the machine translation R&D workflow. Julia Ebert, affiliated at DFKI and member of the editorial team, discussed the perspectives and challenges in the field.

The definition of artificial intelligence (AI) is controversial to this day. Intelligence itself is not easy to define – human intelligence and understanding the human brain still leaves many questions unresolved. What is artificial intelligence from your point of view? What does machine learning have to do with human intelligence?

Artificial intelligence has to do with a number of factors such as language understanding, sensing and being aware of your surroundings, planning, acting and of course learning. Only if several of these factors come together would I be tempted to say that a system or machine has some kind of intelligence. Machine learning is a technique that is used to model intelligent behaviour.

What was your motivation for going into the field of language technology and AI? Which main research questions have accompanied you?

When I learned grammar and foreign languages in school I was always irritated that everything teachers taught about language was soft in a way. It seemed that apart from grammatical exceptions there were no strict rules. My interest in a more mathematical approach to language brought me to the research field of computation and linguistics. Language is such a fascinating interface between humans and human knowledge – and even today, we still don't understand how it really works. Most of the time, human learning processes are so effortless, especially when you look at small children. Actually we have no idea how we can teach machines with the same ease, efficiency and effectiveness.

A child that has seen three dogs has understood the concept. We are trying to get our feet a little bit on the ground concerning machine learning but that is just the tip of the iceberg.

Looking at the current state of AI and machine learning, machines are basically copying human behaviour, e.g. in the case of autonomous driving or smart translation systems. So in short, in what way are we dealing with intelligent programs which are not capable of understanding their actions? How far will the next generation of AI be able to understand, based on acquired knowledge?

It's a huge step between acting intelligently like machines do today and being truly intelligent. For example, a statistical translation engine is not intelligent in a human sense: it doesn't "know" why it should translate a specific word in some context in a certain way – it simply does it. The same goes for a machine that has learnt how to label objects in a picture, e.g. in image search on the web. Of course the machine can label an object but it can't say what this flower smells like or how much the car costs, etc. Don't get me wrong; the systems can really do amazing things on huge amounts of data in almost no time. But the gap between performing tasks like translating or labelling and having common sense like a four-year-old child is really big. That is why it is so important to have a human in the loop. Look at applications in the medical field, for example cancer screening: the dermatologist can derive a comprehensive diagnosis that takes into account what an algorithm has learnt from the data collected on thousands of screened birthmarks. But besides the result on some scale there is no further explanation by the machine. In the next generation of machine learning, machines will hopefully provide an explanation that will make it possible to retrace how the machine got to its conclusion by looking at various characteristics – in this case, colour, shape etc. – and what it has learned from the data. But still, this would be far away from providing any medical or biological explanation. The same in the field of autonomous driving: an autonomous car stops because there is an obstacle ahead – no matter if it's a child or a plastic bag. It doesn't know why it has to brake. Concerning the most advanced phase of machine learning with machines that really know – in a human way of knowing – what they are doing, I have not the faintest idea how we will ever get there.

Through the most recent developments of deep learning significant progress has been made in language technology, especially translation quality. How does deep learning work?

Deep learning is a statistical way of implementing machine learning. It is based on a mathematical structure inspired by the design of our human brain: neurons and links between neurons that are organised in layers. The machine works within an input-output scheme and learns which features and which connections are helpful to perform the task. There is no more manual work to be done and so the system calibrates itself. It might seem like a black box for many people but I think it is in a way comparable with many technologies: I don't know how my smartphone works inside but I accept it because it does what I want.

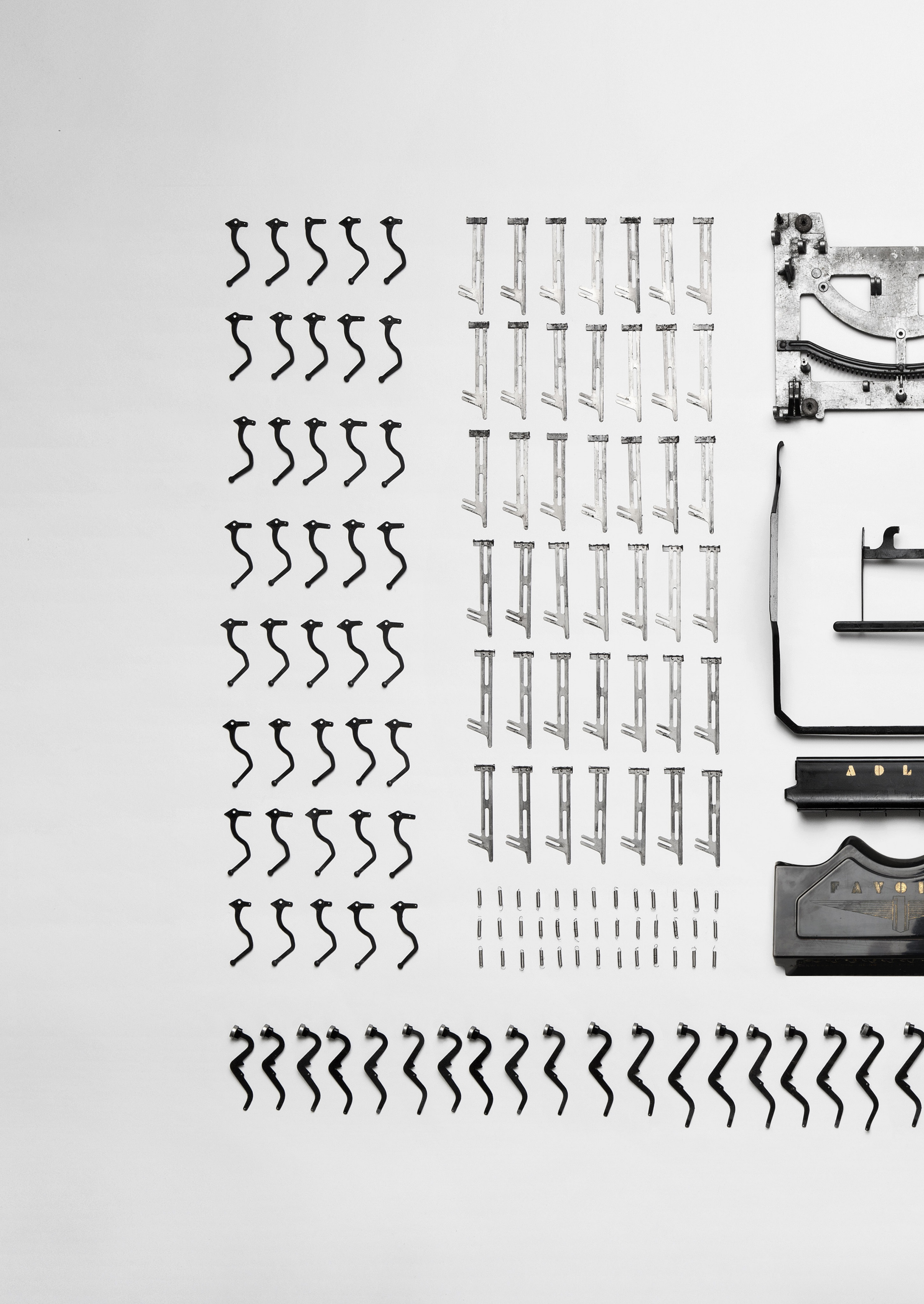
Creativity is probably one of the human abilities most difficult to automate. To what extent will machines be able to exhibit truly creative behaviour in future? Also, against the background of controllability of machines, what form of creativity is possible and reasonable?

I am convinced that machines cannot be creative in the same way that artists can be creative. Creating some new metaphor, style, images – this all has to do a lot with knowledge about cultural habits, dos and don'ts, expectations, etc. It's the same with humour, which doesn't even work cross-culturally. If we deal with machines, we want to control machines. But machines learn from the data we produce, they read through our articles and Wikipedia entries. So, it has happened that a chatbot learned a national-socialist jargon – this actually occurred when it was being used by mean users. It's difficult when dealing with machine learning to act in a normative way. The only thing one can do is to try to create and collect balanced and neutral data. That is the responsibility of data scientists. We humans have to be a good example to the machines and of course we need human control mechanisms. Concerning this matter, I talked to a person from a big insurance company lately. They modelled hundreds of features of people's lives, like their living conditions, incomes or other insurance policies, as features to model the decision whether they could grant them an insurance policy or not. Then, an algorithm was trained on the previous human decisions and learned to take the decision quite well. Later on

they checked on what grounds the algorithm made its decisions: the only one feature the machine used was the geolocation. So people from a poor neighbourhood tend to not to get the insurance but people from rich neighbourhoods had a high probability of getting the insurance. From the machine perspective, this was a useful basis for the decisions, because it is simple and works in most cases. This example shows that we need human control, especially in single, potentially problematic machine decisions. There we need to find a practicable mode of human-machine cooperation. And here again; it would be a great achievement if a machine would be able to explain why it came to a certain decision so that we could decide whether it was a good reason.

There are few topics as filled with hope and hysteria as AI and its impact on our daily lives. Where do you see that AI can deliver the benefits many have predicted? Where are the limits? To what extent can we trust AI?

People are not tempted to trust machines. Machines can seemingly take decisions that we don't understand. We understand if a tire breaks and the car goes in the wrong direction, as it is a physical problem which can be traced back. But if an algorithm steers an autonomous car in the wrong direction because there was some light or leaves on the camera, it is hard to accept this because you can't trace the decision back. There is less fault tolerance of machines than humans. I've seen this from human translators when they get machine translations: if there is a very stupid mistake in one sentence, the user tends to lose confidence in the machine right away – even if the next 100 sentences would have been translated perfectly. In the case of a human, this would probably be advisable: If someone makes such a stupid mistake, it is probably a good idea not to hire him as a translator. We need to find ways to establish trust with machines. But the question is from which point would one person trust a machine? Does it take one hour of driving, one day, one week or a month before I give the same trust to an autonomous car? With humans we are absolutely trained in assessing a human's capability in milliseconds. The same with physical objects: certificates and tests tell us what we can expect. Algorithms are so new that we have not yet learned when we can trust them. ◆



HANS RUSINEK

When human machines meet programmed people

While artificial intelligence is becoming more and more human, humans are becoming more and more controllable by their technological environment. Will man and machine soon meet in the middle? Or, to put it another way, what would a division of labour look like in which both use the optimum of their intelligences? A timely intervention.

When it comes to the future of artificial intelligence (AI), we don't shy away from horror scenarios. The scenarios always follow a pattern familiar from other fear fantasies: first the machines learn from us, then they take away our jobs and in the end, they even take our lovers (Kleeman, 2017). In this scenario, old analogues like us are mere spectators. How much of this fear is justified and are we really passive observers of these developments? One of the most famous anecdotes in the field of AI is the story of Robert Epstein and the chatbot Ivana (Kucklick, 2014). Professor Epstein, psychologist, computer scientist and one of the pioneers in the field of AI, chatted for months with a certain Ivana, whom he believed to be a good-looking Russian lady who was also looking for a partner. But then, the thing that had to happen actually happened: the Eastern European lady turned out to be a bot; the computer scientist had been duped. The moral of this story comes in two versions. In version one, the obvious one, Ivana is an amazing example of the now genuinely human-like communication abilities of chatbots. Machines are actually becoming more and more human. Whether this really is an indication that machines will overtake us with their intelligence, as Christoph Kucklick interprets this anecdote, is another question. What is interesting to note is this anecdote's second lesson, one that we completely overlook in the debates on human-machine interaction. It is not only that the machine, in the form of Ivana, was amazingly human. It is also that the human being, in the form of Robert, made over-hasty and uncritical judgements based on little input, and thus acted astonishingly mechanically. We're not just talking about an algorithm that's as smart as Robert. We're also talking about a Robert who is as unreflective as a computer program. For Robert Epstein believed himself to be in human company because his expectations of humans were so low. If he had invited the lady for blinis or even called her, the illusion would have vanished. There wouldn't have been anyone at the end of the line. So man and machine are meeting in the middle. What are the mechanisms behind it?

THE MAN-CHINE IS PROGRAMMABLE

The first mechanism consists in the fact that we are becoming more and more programmable. This programmability is increasingly forcing us into a mechanical corset without realising it. Techno-social engineering is what the authors Selinger and Frischmann, two leading experts in the field of "the social effects of artificial

intelligence" (Frischmann, 2015), call it. In techno-social engineering, technological and social tools are jointly used to influence our human behaviour on the web, to nudge it in the right direction or even to completely reconstruct it. Ivana is only a very primitive example of this, even if she nevertheless managed to trigger the very complex feeling of erotic interest. But a completely different level was reached when Facebook changed the feelings of 700,000 users in a gigantic social experiment in 2014. In this mood manipulation experiment, selected users saw distorted feeds from their friends and responded accordingly, with modified emotions. Then in December 2016, an article in the Swiss magazine *Das Magazin* described how, first, all you need is a few likes to judge a person (10, to be better than your work colleagues) and, second, how this can facilitate micro-targeting, which is thought to have influenced the US election. In both experiments, the user could be programmed.

However, techno-social engineering per se is not the problem: each culture persists by forming certain norms or rewarding certain behaviours. At work, at school, even in the family, a kind of engineering is always taking place. But while we can also distance ourselves from other areas where behaviour is shaped, because they are just some place, with digital techno-social engineering the presence is more total. Being offline is increasingly becoming an absurd, barely enforceable idea. The digital sphere is not a place, but rather a filter that is located between us and the environment and that constructs a digi-logue world, as the second mechanism will show.

THE MAN-CHINE IS MOUNTED TO THE ENVIRONMENT VIA INTERFACES

The first mechanism shows how programmability is made possible; the second mechanism builds on it and goes one step further. It is not just behaviour that is formed in the digital sphere; we also transfer our experiential spaces there. In so doing, we thus allow our perception to be filtered. When the first cooking shows were broadcast on television at the turn of the millennium, the highlight for the producers was that they were able to have the recipes emailed to viewers afterwards. But hardly anyone was interested. It turned out that it wasn't about cooking the recipes; it was about watching other people cook. Today, we are all aware of this: we watch other people's lives in reality shows, watch other people play video games in let's play videos, and watch others unpack new products like sneakers or records in unboxing videos. And we find this deeply satisfying.

The philosopher Robert Pfaller groups these phenomena under the term *interpassivity* (Pfaller, 2000). Interpassivity means delegating the actions that promise us pleasure and shifting them to external entities: for example, to the camera. It enjoys in our

continue reading on page 44 ▸▸

THIS IS AN ARTICLE BY **HANS RUSINEK**

This opinion piece was first published on 8 March 2017 on the Science Blog of Alexander von Humboldt Institute for Internet and Society (HIIG).

Hans Rusinek is an innovation consultant at the agency Sturm und Drang. He aims to give his clients technological innovation with human relevance while trying to find technological answers to human desires. He wonders what people will do in a car when it is driving by itself or how smart energy contracts could create a better customer experience. Additionally he is a member of Club of Rome's thinktank30, where he serves as an expert for the field Morality and Markets. He studied economics, philosophy and international politics in Bayreuth and at the London School of Economics, where he researched on AI-related topics such as formal logic, philosophy of mind and information ethics.

place the view of the beach, the ocean or the tourist attraction. This also includes the notorious compulsion to take a photo of the food you're about to eat. The act of eating is something we still have to do ourselves, but the camera eats first, as internet researcher Robert Simanowski so nicely puts it. Our true pleasure is the like button. For Pfaller, the reason is as follows: the individual does not want to be confronted with ultimate pleasure; she protects herself from genuine involvement. To be somewhere, live and direct, where you are not every day seems sometimes to be simply too much in light of interpassivity; it seems too intense and makes us too vulnerable.

Now, you can buy this justification, but you don't have to. What's important to note is that through this phenomenon of interpassivity, we insert intermediate levels into our world of experience. Like the camera, the chat program, the unboxing video. Enjoyment is already predigested. These intermediate levels make our shaping through techno-social engineering possible and thus facilitate the control of output and input between people and their social environment. And this is exactly what made it possible for the chatbot Ivana to unleash butterflies in the computer scientist's stomach. The conversation took place on a chat channel, which makes the differences between bot and human being disappear at first. Like a machine, we can be programmed because we are connected via other machines, through interfaces and production processes, to our environment.

THE JARGON OF THE MACHINES

If we hold, machine-like, an interface in the form of a screen between us and our environment, and this allows the feeding of these interfaces to increasingly control us, it is still only half of the story. One development occurring in parallel is that the expectations we have of each other and the behaviour thus triggered increasingly comes to resemble the kind of benchmarks we have for industrial production. We measure and optimise ourselves as the quantified self, like a Siemens engineer working on a gas turbine. How many likes will make me envied, how many kilometres run will make me healthy, how much alcohol in my blood will make for an enjoyable evening?

In this context, the essayist Florian Goldberg quotes the Romanian writer Virgil Gheorgiu. In 1951, Gheorgiu wrote of a future in which mankind ruled over an army of industrious robots. Humans consequently concluded: "We learn the laws and the jargon of our slaves in order to give them orders. And slowly, imperceptibly, we renounce our human qualities and laws. The first symptom of this dehumanisation is the disregard for the human condition" (Goldberg, 2016). 65 years later, this statement has a frightening gravity. Isn't this kind of performance thinking, a competitive thinking of battle cries like America First that fills the dark sides of our present

day? The psychologist Arno Gruen diagnosed a loss of empathy; for the sociologist Hartmut Rosa it is a lack of resonance with the environment. The French *Comité invisible* speaks of the estrangement of (Western) human beings from the world. This estrangement, for example, demands that humans become the masters and owners of things such as nature – for you only try to control what you fear. In such a completely constructed and engineered world focused on output from machines, we have difficulty in perceiving reality in a lived, compassionate and empathic way. In a brilliant essay, the philosopher Peter Bieri pointedly asks how would it be to be educated instead? (Bieri, 2005). And he determines that the educated person is the one who can freely shape his relationship with other people and himself. Isn't that what human intelligence is all about?

IF THAT'S INTELLIGENCE, IT'S A SLAVE INTELLIGENCE.

In the debate on artificial intelligence, a clarification of terms is absolutely essential. Namely: what is actually meant by intelligence here? To date, artificial intelligence has principally used brute force methods to simulate intelligent-seeming responses, despite significant progress in the deep learning area. Hence, Ivana compares Robert's messages with a database and then selects the correct answer. How close is that to human intelligence? What kind of thinking is going on in the field? The fact that we use the term intelligence so freely in relation to software also testifies to how simplistically we now understand this term. What about emotional intelligence, creative intelligence, rhetorical intelligence, moral intelligence; what about the intelligence not just to see patterns, but to create new ones? Intelligence is much more than the ability to adapt as efficiently as possible – or if that's intelligence, it's a slave intelligence.

The computer pioneer Ed Djikstra knew this before the term artificial intelligence was even invented. He was once asked if computers would ever think. He replied that asking this question was akin to asking if submarines could swim. Submarines are specifically built not to swim, and computers are built not to think as we do, but purely analytically. Perhaps it is time to recall this difference and to recognise and appreciate the value of non-artificial, associative, and intuitive intelligence. It is sad enough that machine-like humans now disparagingly term this "soft skills".

THE DIVISION OF LABOUR BETWEEN MAN AND MACHINE: FOR A REDISCOVERY OF HUMAN INTELLIGENCE

So before thinking about which robots take the job away from which clerk, craftsman, assembly line worker or university graduate, it would be good to turn our attention

to what is becoming increasingly difficult for many. This means dealing with each other reasonably, being able to engage in constructive discourses, and having the courage to venture into the unknown. The rediscovery of human intelligence also gains a strategic value through artificial intelligence: nothing else will help against the potential devaluation of human work by robots. One could say: human intelligence will become our unique selling point. The ability to judge humanly, to distinguish between wrong and right, to leave the world of rationality every once in a while and to think in images and analogies cannot and will not be taken away from us by any algorithm. And these skills will be of great value to us; they are far more than just soft skills. We are in a world that is looking for a moral compass and, in this confusion, is also creating great economic uncertainties. We are in a world where innovation cycles are becoming ever faster, in which new business models are emerging ever more quickly. And disappearing again. Human thinking means moral orientation in the sense of *recognising yourself*, creative entrepreneurship and taking risks. I would argue that no entrepreneur can survive without these skills.

The economist and researcher of the digital economy Jeremy Rifkin even goes so far as to speak of a future world where jobs requiring empathy will boom: "non-profit hospitals, non-profit schools, elder care, environmental protection, sport, the arts… so let's allow machines to do the work that human beings no longer have to, and our thinking can evolve, focus on generating more social capital." (Rifkin, 2014) A romantic vision, perhaps too romantic.

PERHAPS WE ARE SO AFRAID OF THE INTELLIGENCE OF MACHINES BECAUSE WE ARE LOSING TRACK OF OUR OWN HUMAN INTELLIGENCE?

Digitisation has revealed to us that humans and machines are converging. We are letting ourselves be programmed, shifting our perception to a world that is predigested for us, we are speaking and thinking in categories that could come from a production plant. As machines become more human, the threat is that humans will forget their unique abilities. Technology is neither bad, nor good, nor neutral, proclaimed the historian of technology Melvin Kranzberg (1986) in the last century. It's the same with artificial intelligence. It is important to make something meaningful out of it with the help of human intelligence. And for this, we need to preserve human intelligence, in education and cultural policy, in the labour market and not least in the debate on digitisation. ◆

REFERENCES

Bieri, P. (2005, November 4). Wie wäre es, gebildet zu sein? Festrede an der Pädagogischen Hochschule Bern. *Hochschule für Wirtschaft und Recht Berlin*. Retrieved from http://www.hwr-berlin.de/fileadmin/downloads_internet/publikationen/Birie_Gebildet_sein.pdf

Frischmann, B., & Selinger, E. (2015, August 10). Will the internet of things result in predictable people? *The Guardian*. Retrieved from https://www.theguardian.com/technology/2015/aug/10/internet-of-things-predictable-people

Goldberg, F. (2016, November 21). Die digitale Verformung. *Deutschlandfunk*. Retrieved from http://www.deutschlandfunkkultur.de/die-digitale-verformung-halten-wir-es-nicht-mehr-mit-uns.1005.de.html?dram:article_id=371892

Kleeman, J. (2017, April 27). The race to build the world's first sex robot. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2017/apr/27/race-to-build-world-first-sex-robot

Kranzberg, M. (1986). Technology and History: 'Kranzberg's Laws'. *Technology and culture, 27*(3), 544 – 560.

Kucklick, C. (2014). *Die Granulare Gesellschaft*. Berlin: Ullstein.

Pfaller, R. (2000). *Interpassivität. Studien über delegiertes Genießen*. Berlin, Heidelberg: Springer.

Rifkin, J. (2014, December 18). Die Wirtschaft trägt sich von selbst. *ZeitOnline*. Retrieved from http://www.zeit.de/2014/50/jeremy-rifkin-kapitalismus-revolution/seite-4

"We are enhancing our power while not developing the ethical, social, and political responsibility to manage that power to the same extent."

POWER AND COUNTER-POWER IN THE DIGITAL SOCIETY
INTERVIEW WITH MANUEL CASTELLS

How is power constituted in the digital society? Who is powerful – and how can power be countered and contested? On 12 December 2017, Manuel Castells held the opening lecture of the lecture series Making Sense of Digital Society, organised by Alexander von Humboldt Institute for Internet and Society (HIIG) in cooperation with the German Federal Agency for Civic Education (bpb). Castells's Information Age trilogy (1996 – 2003) is widely recognised as one of the most important and most cited works of social theory in the context of digitisation. Manuel Castells is Professor of Sociology at the Open University of Catalonia as well as University Professor of Communication Technology and Society at the University of Southern California. Prior to his lecture Jeanette Hofmann, Director of the HIIG and Professor of Internet Politics at the Freie Universität Berlin, met Professor Castells for an interview to discuss his work.

Professor Castells, you discovered the significance of digital networks quite early, in the 1990s. Now, 20 years later, we see more and more changes, both social and technological. How have the networks you studied changed?

First of all, the networks have expanded into every domain of activity and to every corner of the planet. The logic of networks, which was in an embryonic state back then, overwhelms every other logic now. Secondly, microelectronic digital networks are modified and transformed by the practice of their users. The fact that users are the producers is one of the key rules of the internet. In 1996 there were about 40 million users, now we have 4 billion users. Since user inputs modify and transform the networks, size means quality. At the same time technology has continued to evolve dramatically. Therefore, the speed and flexibility of networks in every domain has multiplied. So the logic of networks has modified itself through constant, almost real-time feedback loops. Virality is the key transformation of the internet. Now the issue with this logic is that networks are modified by unintended effects and that they create other unintended outcomes. Therefore, networks experience exponential growth with increasing uncertainty and irreversibility.

What would be an example of such an unintended effect with a strong impact?

Financial markets. No one really thought that financial markets could evolve by themselves, independently of human decision-making. It's not that computers make decisions by themselves, which has been prohibited since 1987. The complexity of the derivatives is so enormous that no one can control it, not the regulators and none of the financial agents. They hope it will evolve in one particular direction, but it's impossible to actually control it. No deliberate action was ever taken to create a financial market that is independent of everything.

We are noticing a widespread sense of lack of control and understanding when we talk about machine learning. I'm wondering whether this is a new situation emerging in which we are facing more and more phenomena clearly outside of our control. Would you say that this is something new?

Absolutely. If you look at the internet of things you can see that networks are now multiplying in a way in which we not only connect networks enacted by humans but also networks enacted by machines between different machines. There is some programming by humans at the origin. But what is out of control is that these machines are subsequently programming and reprogramming each other and are literally making decisions alone.

These networks make formatting decisions, or programming decisions as you put it.

Yes, they make programming decisions. They do have some rules to make things more efficient, broader, and cheaper. I was always critical of trying to understand the transformation of technologies and our technological environment through science fiction because it would put social scientists out of work, to the benefit of science fiction writers. However, science fiction writers intuitively foresaw many of the developments that actually happened later on because they are not constrained by data and use their imagination instead. Thus they actually anticipated certain things like machines programming machines. For networks this means that the interaction is still one between agents, but some of the agents are machines. This changes everything. We are only at the beginning of this development and it is continuing at an incredible speed.

Do you think we have become the victims of our own success?

I don't think that success is the right word for the development of technology. Any technology that humanity has developed will ultimately be used, like nuclear bombs. So success is relative. We are enhancing our power while not developing the ethical, social, and political responsibility to manage that power to the same extent.

Let me rephrase that question. If all technology is about extending control …

No, it's about extending power. The ability to do more and more things. In my empirical analyses I find that the more you extend power, the more you lose control.

Yes, that is perhaps the point. I would say the intention is very often to extend control. Take predictive analytics: It is the attempt to control future events, but the effect of trying to extend control creates new types of uncontrollable situations. That's probably the paradox we are observing at the moment.

Absolutely.

Let's talk about identity. In your early work you defined identity as an important resource for opposition. At the same time you saw the ambivalence in identity: Movements can be progressive but also very oppressive. What do you make of the fact that oppressive identity-based movements seem to become more powerful at the moment?

If we look at what has happened in political and geopolitical terms in the past 15 years, I would say that the logic of identity building has been more important in shaping politics, people's lives and society than the logic of networks and technological innovation. Today we live in a world dominated by fear, fear of the other. And this fear of the other starts with the definition of us and the other, which is the essence of identity. Technologies are now used to strengthen this opposition. The network society seems to strive for more productivity, efficiency, et cetera. But at the same time there are segments of the population that do not recognise themselves in that logic, whose values are excluded, and who have no power. They try to turn things around and stoke new identity-based conflicts. This is now the most powerful force shaping our societies. We now find ourselves in a complete contradiction between our capacity to unify humanity through the logic of networks on the basis of cooperation, and the reality of different cultures fighting each other on the basis of different principles, be it religious, territorial, or ethnical. These identity-based movements are networked as well and use network technologies very efficiently. Therefore, the logic of networks has penetrated the logic of cultural identity.

What is the relationship between technology and manipulation in that context?

The more technologically enhanced power you have, the more you have the possibility to manipulate information. This is what is happening with bots in social networks, for instance.

But such a technique will only work for a limited time? As soon as everyone knows about bots, they are likely to lose their impact?

Exactly. It is not a linear process. It is a contradictory process between the extension of a logic and our capacity to counter this logic consciously. Ultimately human consciousness prevails. ◆

—

This is an abridged transcript of the conversation. The full transcript will be published on the HIIG Science Blog.

PARADISEPAPERS

The Paradise Papers are a set of 13.4 million confidential electronic documents that throw light on the top end of the world of offshore finance. Reporters from the newspaper Süddeutsche Zeitung shared the documents with the International Consortium of Investigative Journalists and a network of more than 380 journalists. The papers prove how politicians, multinational corporations, celebrities and high-net-worth individuals use complex structures to protect their cash from higher taxes.

UTA MEIER-HAHN

The internet was built on trust. But what does it run on?

One of the most exalted narratives about the internet is that it is built on trust. This refers to the understanding that trust mitigates the basic uncertainties imposed on the internet's operators by its architecture. To this day, network engineers cannot generally be certain about the validity of the routing announcements that they receive from interconnected networks, and they have little insight into the legitimacy of the traffic that they are mandated to transmit.

In the early days of the internet, network operators knew and trusted each other, and, as a result, the internet worked in spite of uncertainties. The assumption that trust serves as a kind of social glue is generally in line with academic research. Several disciplines have stressed positive associations with trust as a means of overcoming uncertainties. Economic sociology in particular has linked trust to cooperation (Granovetter, 2001, p. 5). But what is the state of trust in today's internet? If the internet was built on trust, is it still maintained on trust? Updating our understanding of the foundations of Internet connectivity is important to preserve and foster it. 50 networkers from around the globe shared their views on this very topic with me. The most important finding may come as a surprise – but perhaps not: networkers both trust and distrust each other. However, as I will argue later, that is not necessarily a bad thing.

TRUST AND DISTRUST ARE NOT OPPOSITES

First, let me clarify what I mean by trust and by distrust. Along with Lewicki & Bunker, we can think of trust as positive expectations and distrust as negative expectations regarding another person's conduct. Trust and distrust should be treated as separate dimensions, not as opposites on the same scale. A low level of trust does not imply distrust, and conversely, the absence of distrust does not imply trust. One may simply feel indifferent towards another person. To complicate things further, we can differentiate between two ways in which both trust and distrust can be anchored: in identity or in calculation. Trust based on identity is signified by common values, goals or emotional attachment; calculated trust, however, refers to positive "outcomes resulting from creating and sustaining a relationship relative to the costs of maintaining or severing it" (Lewicki & Bunker as cited in Lewicki, Tomlinson, & Gillespie, 2006, p. 1007).

The important takeaways here are that trust may be anchored in different ways and that it is possible to both trust and distrust the same person depending on the situation. For instance, we may trust the cashier at a bank to forward our payment (calculated), but we may not trust her to separate the trash in an environmentally aware way (identity). Or, we may trust in someone's good intentions (identity), but distrust his competence (calculated).

FIREFIGHTERS OF THE INTERNET

So how do these general thoughts apply to trust among networkers? In what follows, I present some findings about identity-based and calculative trust and distrust among networkers. I first identify the values, goals or emotional themes that enable trust or prompt distrust among networkers. I then highlight the rationales that networkers typically rely on when they come to trust or distrust other networkers in a calculative way.

Identification-based trust among networkers revolves around the idea that the internet is "a people thing". The computer network is, at the same time, a social network. Statements such as, "the internet is a bunch of people who all trust each other" indicate this. Interconnected counterparts are regarded as partners. The act of interconnecting networks is equated with a personal relationship. Furthermore, trust is created through a common understanding that networkers form a community of practice. They unite behind the idea of a "technical legacy", which is an engineering ideal of a tightly meshed internet. But it also refers back to earlier times, when cooperation was necessary in order to create the internet – the time when the narrative that the internet runs on trust originated.

Another basis for trust is expertise. Demonstrating expertise is highly valued and fosters trust among networkers. However, traditional seals of quality, such as university degrees, do not necessarily apply in this professional sphere. Many networkers, including many of the most prominent ones, dropped out of higher education to enter the industry on a learning-by-doing basis (and they are hesitant to admit this). Venues that allow networkers to show off their expertise are important, not only for sharing knowledge, but also for trust to emerge. These include events, such as Regional Internet Registry meetings, as well as remote venues, such as email lists or instant messaging channels for ad-hoc coordination.

There is also a common commitment to mutual 24/7 availability. Several networkers emphasise that they make sure to respond immediately when fellow networkers reach out. Demand for swift responsiveness may arise both when someone's network causes trouble for others, such as in the infamous "Pakistan-Youtube" case, and when someone needs help in battling irregularities in her own network. Comparing networkers to firefighters or emergency room personnel fits this picture:

> "Trusting the routing guys on the other side and them having an idea that you know what you're doing as well [...]. Because **when troubles occur**, and they always do, **you will want both sides to be able to not waste time and firefight the bug.**" (emphasis added)

This statement implicitly highlights another expectation: networkers must not abuse the knowledge about other networks gained through collaborative maintenance and repair. They must honour this implicit agreement – namely that what happens at the core of the internet stays at the core of the internet – so that they can obtain trust. Note that trust runs across company boundaries.

One source of identification-based trust that is not to be underestimated is the symbolic dimension, comprised of cultural codes such as humoristic clues or even clothing. The following anecdote from a representative of the information technology magazine IX reveals how powerful such codes can be:

> "I used to sell to enterprises. I dressed up looking a bit like a banker [laughs]. So I'd wear the pinstripe suit and I said: 'This is easy. It is a free product.' And I was in [company name, ed.] for about four months and I am thinking: 'No one is signing up for me. It's a free product. No one is connecting. I mean, how bad can I be? It's free! Why is nobody doing this?' And the smallest thing is: I changed my outfits to jeans and a casual top and yes, a smart jacket. **But just by changing interestingly enough to a pair of jeans, suddenly I started to see more people wanting to engage with me, talk to me. Because now they felt that it's not something, that I meant to sell them something.** Let's have a conversation around your strategy and network. Very, very small thing. But to this day, it still blows my mind. And ever since I did that, then **I realised: 'Okay, there is a little bit more to it than just connect and get free capacity basically, or free peering.'**" (emphasis added)

The fact that a business outfit can create suspicion also suggests that broadcasting a commercial intent is at odds with this identity-oriented type of trust.

SOCIAL CONNECTION AS A CURRENCY

Calculation-based trust, on the other hand, is less binding and much more transactional. In internet operations, it predominantly rests on one form of reasoning: the internet is a shared resource. All networks have a basic incentive to act in favour of connectivity because of the interconnected nature of the internet. As one networker put it,

> "The internet is 40,000 competitors. But if they don't work together, then none of them have a product."

Networkers assume that damaging connectivity is against each operator's self-interest; therefore, no operator has an incentive to engage in such behaviour. This reasoning

gives rise to a very basic level of confidence in each other. It may not be high, but it is widely shared. Some networkers also see trust in a very strategic way. Here, the rationale is to aim for repeated interaction with colleagues, because personal relationships are regarded as substitutes for the exchange of money:

> "Once you cooperate [...] and there is no contractual relationship, then the best way of keeping that relationship is by having some kind of a social connection **which acts as a currency** almost, you could say." (emphasis added)

Fostering relationships with others is thus not incompatible with a commercial trajectory. Trust may mean harmony, but more so, it is valuable.

"YOU CAN TRUST YOUR WIFE, NOT THE PEERING PARTNER"

Now let's look at distrust. Not all networkers cherish the above-mentioned values. Some reject outright the idea that common goals or beliefs among networkers could be meaningful at all:

> "There is nothing about trust. You can trust your wife, not the peering partner."

However, from those who do acknowledge that personal relationships underpin the internet, there are more specific reasons to distrust. One potential reason is the networker's absence from face-to-face meetings. This especially holds true for large companies that impact many others. Not providing a "personal interface" to the community creates distrust. Apparently, there is one Tier 1 network that is notorious for avoiding encounters on a personal level. When individual networkers gain a reputation for being self-centred and egotistical, these characteristics are understood as strong indicators of incompatible values. What is even worse is if they appear to break with the technical legacy. Here, distrust may even become actionable, as this ominous quote shows:

> "**If the trust is broken** that is one of the very, very few things that will unite 99 % of the internet. If you are a bad actor and betray the trust, if you lie and say: 'Well, I am Youtube,' then **the rest of the internet is going to come down on you like a ton of bricks.**" (emphasis added)

It is unclear how commonly such vigilante-justice sanctioning mechanisms are used, but this quote shows how easily identification-based trust can turn into distrust. Distrust also sets in when networkers discover that their counterpart masks de facto business decisions in what could be called architectural uncertainty. Several

continue reading on page 60 ▸▸

THIS IS AN ARTICLE BY **UTA MEIER-HAHN**

This article was first published on 5 July 2017 on the RIPE Labs platform.

Uta Meier-Hahn is a doctoral researcher who is interested in all things infrastructure. In her doctoral thesis she looks at how internet engineers manufacture Internet connectivity. Uta also maintains an interest in the governance aspects of emerging networked technologies such as the Internet of Things as well as blockchain. From 2013 to 2015 Uta was the first academic editor at Internet Policy Review, a peer-reviewed online journal on internet regulation in Europe. In this role she contributed to establishing a hybrid form of publication at the crossroads of journalism and academia. Before joining the institute, Uta worked as an online journalist for the public broadcasting company Norddeutscher Rundfunk. She studied cultural studies at the University of Lüneburg and at the Marmara University in Istanbul.

interviewees reported incidents in which interconnected partners placed the blame on network irregularities, when in fact, they had been de-peered, i.e. the interconnection session had been shut down deliberately. These networkers made it very clear that they will not forget the person who sought to deceive them. Distrust can also relate to internet exchanges (*IXPs*). This is an interesting case because internet exchanges often explicitly emphasise their neutrality. Neutrality is treated as one indicator of quality; however, by doing so, internet exchanges can feed both trust and distrust. For some, neutrality facilitates trust because networkers like the idea that all members will be treated equally. For others, the very fact that internet exchanges do not check their members' intentions causes distrust. This can even lead to a general refusal to peer at an internet exchange, as this networker, who represented an incumbent ISP at the time, recalls:

> "We'd never push traffic across them. [...] You never know who your neighbours are in an exchange. Because when you go into an exchange, they're busy selling more neighbour slots. **You have no idea who's on the same fabric and what their motives are!**" (emphasis added)

It is likely that any network intermediary probably has to deal with this ambiguity. In a calculative way, networkers distrust those colleagues who appear incompetent. This judgement, as well as the distrust, is strengthened through repeated interaction. Beyond that, networkers who openly articulate a competitive strategy or who are seen as seeking undue advantages will cause others to distrust them as well. This is an impersonal, objective form of distrust that is probably omnipresent in all market environments.

COPING WITH DISTRUST

When distrust exists, does it prevent networkers from interacting with each other? Not necessarily. Networkers use at least two strategies to cope with distrust. The first strategy is to engage heavily in monitoring their networks to detect irregularities. It is a way of trying to be on top of things. Strategy number two involves initiating contracts and service level agreements, at least for meaningful interconnections.

> "Where we need a contract is where it's A, very important that we have this connection for our business and B, we do not trust 100 percent that the other party will not change their decision in a way that will hurt our business. And then that's the case where you need a contract. A contract is basically where you say: We know that for as long as this contract runs, you are not going to change anything beyond what we agree in this contract is going to happen."

Contracts allow networkers to create bounded transactions despite distrust. They help stabilise a relationship, albeit at higher costs. In practice, however, the power of peering contracts is unclear. Because no one pays anyone else in free peering, there is probably no way to enforce the contract in a court of law. Yet contracts certainly have the effect of solidifying a relationship.

What is notable is that both coping strategies tend to eliminate informal, personal aspects of internet interconnection. Distrust here seems to foster formalisation. In itself, this is neither good nor bad – it just means change. However, it allows us to identify more generally how both trust and distrust serve as resources for ordering processes. They exist in generative interplay with one another. Looking at it this way, even distrust can become a productive force for the good of the internet. To achieve that, distrust needs to be transformed into improvements for all. The security extension for the *Border Gateway Protocol BGPsec* or frameworks for *resource public key infrastructures (RPKI)* seem to be good examples. In my view, these ongoing routing security innovations are actually materialised expressions of distrust that ultimately are able to generate trust. It is safe to say that today's internet not only runs on trust, but also on distrust. The more we acknowledge this, the easier it will be to let distrust point us to aspects of internet operations that need our attention. ◆

REFERENCES

Granovetter, M. (2001). A Theoretical Agenda for Economic Sociology. In *Economic Sociology at the Millennium*. New York: Russell Sage Foundation.

Lewicki, R. J., Tomlinson, E. C., & Gillespie, N. (2006). Models of Interpersonal Trust Development: Theoretical Approaches, Empirical Evidence, and Future Directions. *Journal of Management, 32*(6), 991 – 1022.

KIRSTEN GOLLATZ AND LEONTINE JENNER

Hate speech and fake news – how two concepts got intertwined and politicised

On 1 October 2017, the so-called *Network Enforcement Act (Netzwerkdurchsetzungsgesetz*, or *NetzDG*) came into force with a transitional regulation. The law applies to operators of social media platforms and their handling of the phenomena of *hate speech* and *fake news*. As the jury for the *Anglicism of the Year 2016* award wrote, these two terms served as a "crystallisation point for societal debates on how to deal with this phenomenon, which is not entirely new but has entered the public consciousness with force." We ask: how did it come about that the debates around these terms actually led to a law in Germany?

To answer this question, we will first reconstruct the trajectories of the two discussions in the media. The debates on hate speech and fake news are first considered separately from each other; then, we examine how they came into contact with one another. We will subsequently turn our attention to the increasing politicisation of the discussions, which culminated at the end of the year in a convoluted discourse on the regulation of two very different phenomena. Our accounts here are based on an analysis of more than 900 articles published in the German-language media in 2016.

TRAJECTORY OF THE HATE SPEECH DISCUSSION IN 2016

At the beginning of 2016, Facebook itself shaped the media agenda by announcing several measures to combat hate speech, with a focus on Germany. At the end of May, the question of how to deal with hate speech also became an issue for European institutions. The European Commission reached an agreement with Facebook, Google, Microsoft and Twitter on a code of conduct on hate comments. In Germany, a local case of right-wing agitation against Green Party MEP Stefanie von Berg once again put the topic on the media agenda. Hamburg's senator of justice, Till Steffen (Green Party), then pushed the discussion about a possible tightening of the law on hate crimes. Over the summer of 2016, the media interest was fuelled by a larger discussion broadening the scope of the issues to society as a whole. In these months, various actors initiated public campaigns against hate speech, and projects to observe hate speech on the internet were set in motion. The first figures and statistics based on scientific research were published. The wider public interest strengthened the drive to political action.

The enormous increase in reporting in November and December was primarily the result of the superimposition of another discourse onto this debate. The US presidential election and the question of how fake news on social media had influenced it reactivated the debate on online hate comments at the end of 2016 as just another category of unwanted content on the internet. As an overview,

the first visualisation on page 67 shows the trends on the hate speech discussion in 2016.

TRAJECTORY OF THE FAKE NEWS DISCUSSION IN 2016

At the beginning of 2016, reports of defamatory, false stories about refugees increased. Our analysis shows, however, that these false reports were not yet the focus of a separate discourse; instead, the lines of conflict were based more on positions in the refugee debate.

We again note an increased focus on false reports during the shooting spree in Munich on 22 July 2016. The term *Falschmeldung* (literally false report) used in this context primarily referred to rumours that were spread as purported facts during the chaos. Nevertheless, the killing spree in Munich marked an important point in the development of the fake news discussion in several respects. It was here that key subjects and objects of discourse formed: on the one hand, there was social media platforms, which is where false reports were primarily spread. On the other hand, there were traditional media organisations, which were accused of allowing an information vacuum to emerge, thus giving the false reports on Twitter or Facebook more opportunity to spread. Calls for state intervention were voiced for the first time with reference to the coverage of the killing spree, but considerations remained abstract.

The issue finally came to the public's attention along with the entry of the English term fake news into the German language – this occurred when Facebook was accused of aiding President Trump's election victory. While the debate had previously centred on concrete cases of false reports and problematised their dissemination, now Facebook's handling (or non-handling) of fake news was the subject of discussion. There were calls for measures that would go beyond a mere voluntary commitment on the part of Facebook. In December, the problem was then also applied to the forthcoming federal elections in Germany in 2017. As the second visualisation on page 67 shows, this resulted in yet another rise in reporting.

CONVERGENCE OF TWO DISCUSSIONS INTO ONE DISCOURSE

At the beginning of 2016, both phenomena arose simultaneously but individually in certain contexts: for example, there were increasing numbers of false reports against refugees that were deliberately being spread to incite hatred. However, in terms of terminology, the term that was being used was exclusively false reports with defamatory content *(Falschmeldungen mit diffamierenden Inhalten)*.

continue reading on page 66 ▸▸

THIS IS AN ARTICLE BY **KIRSTEN GOLLATZ AND LEONTINE JENNER**

This piece is based on two articles published on 2 and 8 May 2017 on the Science Blog of Alexander von Humboldt Institute for Internet and Society (HIIG).

Kirsten Gollatz is currently conducting research with a focus on the conditions for exercising freedom of expression on the internet and the relevance of private transnational governance, as well as online participation. Along this line, Kirsten is interested in how public discourses, for instance on hate speech and fake news on digital platforms in Germany, manifests itself in institutions, new organisational processes or practices. Kirsten Gollatz is Project Manager at HIIG working at the interface between the institute's research agenda and a growing international research community. Kirsten also coordinates the institute's academic visitor programs. Since 2014 Kirsten has been writing her doctoral thesis at the University of Zurich. In her thesis she investigates the evolution of transnational governance regimes that private social media companies apply to user content on their platforms.

Leontine Jenner is a student assistant for the Internet Policy and Governance research team at HIIG. She is currently studying sociology at the Technical University of Berlin with an emphasis on sociological technology studies and computer science as her minor field. Prior to her studies she has worked in the games industry in the field of game design. Leontine is particularly interested in new forms of digitally mediated interaction and qualitative and digital research methods.

By the end of the year, two Anglicisms had established themselves in the German language: hate speech and fake news. In this phase, the hate speech discussion almost never appears in isolation. The intermingling of the two discussions is particularly apparent in December. Of the 49 articles on hate speech published in December, 37 articles also deal with fake news. The hate speech discussion was increasingly subsumed under the new fake news debate.

At the end of 2016, the factor that connected these two, previously separate discussions was not that they occurred simultaneously in relation to certain incidents, but that both phenomena arose in the same place. Social media platforms, especially Facebook, were seen as the breeding ground for fake news and hate speech and were increasingly criticised. Two distinct categories of unwanted content had now become the subject of the same regulatory efforts. The third visualisation on page 67 depicts the convergence of the discussions in 2016.

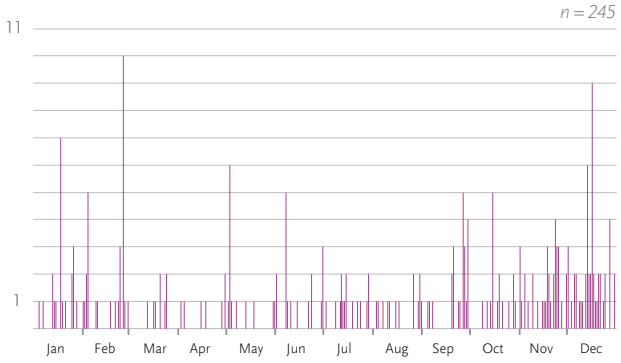
POLITICISATION OF THE DISCUSSION: A WAY STATION ON THE PATH TO THE LAW

The above explanations mark the way stations on the path to the Network Enforcement Act: platforms launched initiatives and made voluntary commitments regarding hate comments in early 2016, there was a broader societal discussion of the topic during the summer months, an increased focus on the role of digital platforms in spreading hate comments and false reports, and finally the election victory of Trump, which firmly anchored the English terms fake news and hate speech in the German discourse and united the two debates in their criticism of Facebook's deletion practice.

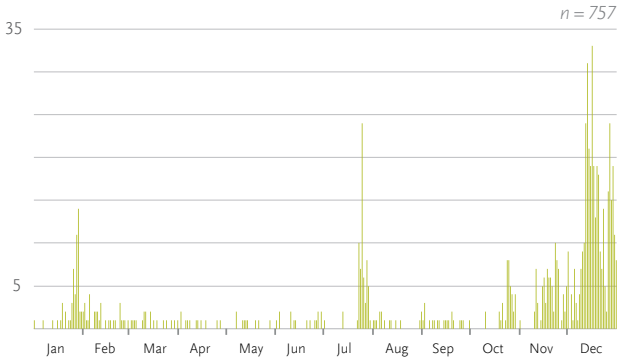
The politicisation of these two discussions was fuelled in particular by three factors. First, politicians (e.g. Renate Künast, Stefanie von Berg) were themselves victims of false statements or hate tirades in social networks. Second, the initial measures in the fight against hate speech, which were mainly based on platforms' own initiatives and voluntary commitment, were increasingly perceived as ineffective. And third and finally, the discourse about hate speech and fake news on social media platforms was situated in a relationship with other political issues, in particular the refugees, the killing spree in Munich, alleged disinformation campaigns by foreign governments, and finally, the federal parliamentary elections in Germany following the US elections.

These factors prompted a shift in the debate towards legislative solutions. At the same time, the emerging narrative of fake news as a threat to German democracy in the face of the forthcoming elections led to an increased sense of urgency within politics. In this context, the new fake news problem was quickly linked to the old hate speech issue. A longer discussion, of the kind that emerged on hate speech, in which participants first attempted to better understand, define and evaluate the problem, did

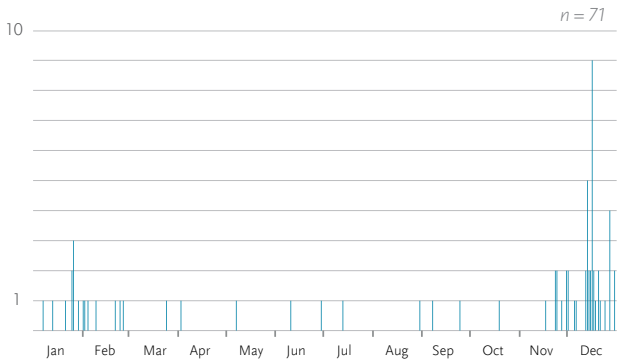
continue reading on page 68 ▸▸



Number of media documents per month concerning hate speech



Number of media documents per month concerning fake news



Number of media documents concerning hate speech **and** fake news

not happen in the case of fake news. Because voluntary measures taken by platform operators against hate speech had purportedly led to disappointing results, politicians now sought to solve the fake news problem by directly legislating.

WHAT WILL REMAIN THE SAME, WHAT WILL CHANGE?

In the spring of 2017, these developments culminated in a draft law presented by then Justice Minister Heiko Maas. In June of the same year, despite harsh criticism, the draft was accepted by the Bundestag and finally implemented on 1 October 2017 – albeit in watered-down form. Supporters and critics of the law see the actual problem quite differently: while proponents see hate speech and fake news as a threat to German democracy and the law as a way of defending against this, critics see the law itself as a threat to democratic opinion-formation. These critics fear that platforms may proactively delete content on a large scale to avoid fines. In addition, they are concerned that the law could be abused by governments. In both cases, there would be a threat of censorship and thus a restriction of freedom of expression. While our analysis is limited to the year 2016, based on these contradictory positions, we can predict that the NetzDG, its controversial norms and legality, and the concrete effects of the law will continue to be a subject for debate. ◆

REFERENCES

Anglizismus des Jahres. (2016). Retrieved from http://www.anglizismusdesjahres.de/anglizismen-des-jahres/adj-2016

***Netzwerkdurchsetzungsgesetz vom 1. September 2017* (BGBl. I S. 3352)** (Germany). Retrieved from https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html

"In the attempt to save democracy, it may be a good idea to stop spreading the false notion that we are living in an undemocratic place."

QUALITIES OF DEMOCRACY
INTERVIEW WITH WOLFGANG GRÜNDINGER

Against the backdrop of populist uprisings, filter bubbles and emerging fake news, democracies' strengths and stability are being put to the test. Although there are reasons for concern, Wolfgang Gründinger, policy officer at the German Association of the Digital Economy (BVDW), encourages readers not to underestimate the resilience of democracy in the following interview. He is author of the book *Alte-Säcke-Politik* (Grumpy Old Men Politics), which was honoured as political book of the year 2017. He attended the Oxford Internet Leadership Academy, is board member at the German Social Democratic Party's forum on internet policy and is European Digital Leader of the World Economic Forum (WEF).

In the past, voting was an act of affirmation that reflected a collective identity. Now, it is increasingly becoming a punitive, anti-establishment act. Given this loss of collective identities and a decreased perception of self-efficacy within the established political system, can you identify new patterns of identities or do you see the need for a more radical change of structures in order to revive political conviction and engagement?

We sometimes tend to romanticise the good old times when democracy supposedly worked better than today. There is little evidence to support the – admittedly popular – claim of a post-democracy that would reduce elections to a meaningless spectacle while an entrenched elite would make all decisions behind closed doors. Quite the contrary, the quality of democracy today is probably better than in the 1950s or 1960s in most Western nation states. The flipside of the alleged loss of collective identity is an enormous gain in individual freedom and self fulfillment, independent from social constraints. We are certainly observing a worrying uprise of right-wing populist movements across country borders, but this has also spurred their opponents to engage in very dynamic counter-movements. There is reason for concern, but we should not underestimate the self-healing powers of democracy.

The internet was introduced as the medium of freedom and empowerment. The current discourse around fake news, filter bubbles and algorithmic decision-making seems to limit its original promise. What chances do you still see in the internet for democracy? Internet as infrastructure?

Indeed, its early protagonists embraced the internet as an autonomous sphere for free and equal deliberation, independent of control or oversight by governments or corporations. We've had to learn from bitter experience that today's internet is very far from this early utopian idea. Melvin Kranzberg's first law of technology is true: technology is neither good nor bad, nor is it neutral – i.e., technology depends on the very social context in which it is being used. In Western democracies, we worry that the internet or – more specifically – social media are helping spread hate speech, propaganda and misinformation. In authoritarian regimes, on the other hand, social media is a tool to circumvent censorship and help civil society to articulate and organise. It is not by accident that authoritarian regimes so often attempt to ban Twitter and Facebook.

In particular right wing movements base a large part of their visibility on emotion-driven populist narratives and algorithmically boosted outreach. How do you reach such movements while committing to a fair-play, fact-driven way of communicating?

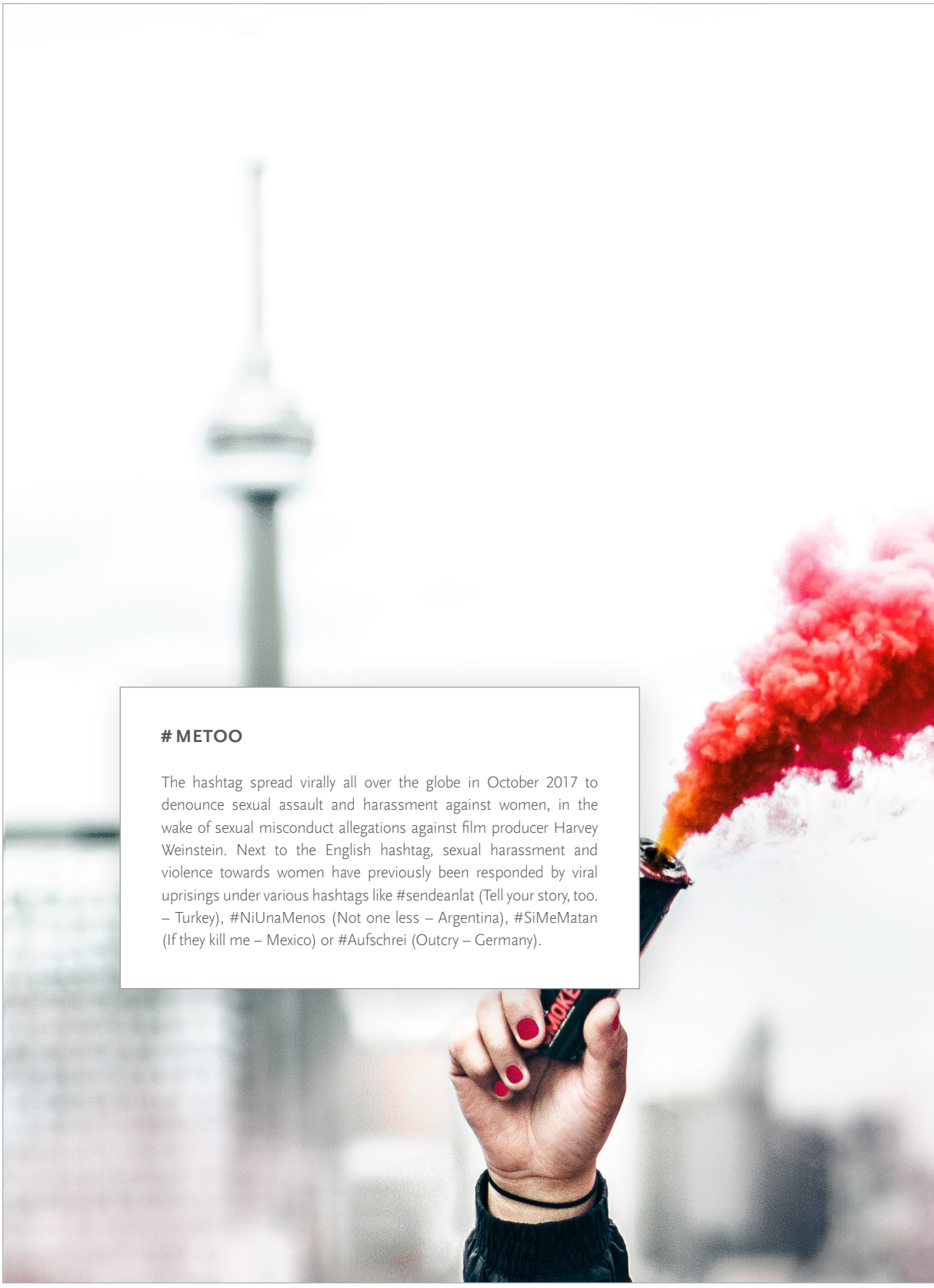
Emotions are usually a stronger driver than sheer facts, and it is illusory to believe that just referring to the facts and thinking would make people change their minds. Substantial parts of the population have proven incapable of differentiating even the most obvious false news from actual facts, and even despite that, people unconsciously choose whom and what they want to believe and what they'll rather ignore. On top of that, people seek simple explanations and solutions for difficult problems in an increasingly complex world, and for self-affirmation by belonging to a *chosen* community in distinction from *others*. This is the very reason why fact-checking alone will be quite ineffective in eradicating fake news. Instead, left-wing and mainstream movements need to pierce the filter bubbles and offer counter-narratives that must take up, understand and address the prejudices and concerns of the target group.

Are we still citizens of one state or already citizens of an interconnected, digital world? How do you define citizenship in the 21st century?

The digital world or cyberspace is not a parallel universe but only a technology. Hence, there is also no digital nation and no digital citizenship. In Europe, many young people define themselves both as European and, say, German or French, at the same time. Online technologies certainly foster international communication around the globe but thus far I don't see any evidence that people are starting to consider themselves internet citizens, for good reasons.

Many people see modern liberal democracy in a state of crisis: those who try to defend it argue based on its legitimate procedures, the value of which makes up for the sub-optimal outcomes. However, one of these sub-optimal outcomes has been the increase in populists, who contest the intrinsic value of liberal democracy by arguing that it fails to bring about the desired outcomes. If both sides have a point, how can one balance democracy's input and output legitimacy in a way that bridges this divide? How would you advocate for democracy in the light of such opinions?

It's all but new that liberal democracy is subject to fierce criticism. Contemporary right-wing movements argue that our democracy has been captured by a corrupt elite and that we have ceased to live in a "true" democracy that represents the "will of the people", whereby the latter is recognised as a homogeneous state defined a priori rather than an outcome that needs to be produced. Many mainstream intellectuals and opinion leaders, however, indeed share this argument, blaming lobbyists (of course, always the lobbyists on the other side!), parties (of course, always the other parties!) or EU bureaucrats ("Brussels") for having stolen democracy from the people. In the attempt to save democracy, it may be a good idea to stop spreading the false notion that we are living in an undemocratic place. ◆



METOO

The hashtag spread virally all over the globe in October 2017 to denounce sexual assault and harassment against women, in the wake of sexual misconduct allegations against film producer Harvey Weinstein. Next to the English hashtag, sexual harassment and violence towards women have previously been responded by viral uprisings under various hashtags like #sendeanlat (Tell your story, too. – Turkey), #NiUnaMenos (Not one less – Argentina), #SiMeMatan (If they kill me – Mexico) or #Aufschrei (Outcry – Germany).

TONY ROSS-HELLAUER AND BENEDIKT FECHER

Journal flipping or a public open access infrastructure? What kind of open access future do we want?

Open access is a question of innovative, public science infrastructure. Tony Ross-Hellauer and Benedikt Fecher present two possible scenarios for an open access future, and consider the relative merits and viability of each.

Open access is advocated by science funders, policymakers and researchers alike. It will most likely be the default way of publishing in the not-so-distant future. Nonetheless, the dominant approach to achieving open access at the moment – journal flipping – could have adverse long-term effects for science. In essence, this journal flipping strategy intends to transform the traditional publishing model – in which libraries pay for journal subscriptions – to models whereby researchers and their institutions pay for the publication of their results. One could say that instead of paying to read, academia is now heading for a solution in which it pays to be published. To try to stir debate, the authors present two dichotomous scenarios for open access in 20 years' time.

PRELUDE

The movement for open access seems to have entered a new phase, in which debates are centring more on how than why. The arguments about the social, economic and academic benefits of open access seem to have largely been won, at least at the policy level of governments, policymakers, institutions and funders. As mandates and policies proliferate, the build-up of political pressure is making open access seem like an inevitability, although it is worth remembering that researchers, despite apparently agreeing that open access is a good idea, have proven much less likely to adopt it for their own publications, where the prestige of appearing in brand-name journals remains the main motivation (Fecher, Friesike, Hebing, & Linek, 2017).

The success of open access at the political level is bringing about an urgent moment of choice. Policymakers want open access quickly – the European Commission's competitiveness council infamously called for full, immediate open access to all scientific publications by 2020 (Enserink, 2016). Although that target is almost certainly unrealistic, as a statement of intent it is powerful. Such sudden urgency sets the scene for pragmatic solutions. And the most pragmatic of solutions currently on the table is the one proposed by the OA2020 initiative, which aims to accelerate the transition to open access by transforming the existing corpus of scientific journals from their current subscription system to open access (Schimmer, 2015). This so-called big flip of the current journal ecology would have the advantages of not requiring researchers to change their practices too much and building upon tried and tested infrastructure – the journal-based publishing system. In previous op-eds on the topic, the authors already made the argument in favour of a public open access infrastructure and

against the big flip of subscription journals (Fecher, Friesike, Peters & Wagner, 2017; Ross-Hellauer, 2017). Here, the authors would like to explore in more detail the possible consequences for scholarly communication if either of these two scenarios come to pass. The authors present these scenarios for discussion, in the hope that sketching these possible futures will help achieve consensus on the best way forward.

TWO SCENARIOS FOR OPEN ACCESS

There are, of course, many possible scenarios for how open access publishing will look in 20 years' time. The authors decided to present two tentative ending points of a dichotomy. Scenario 1 follows the adopted strategy of many European countries – offsetting agreements and journal flipping. Scenario 2 follows a strategy that is discussed less often – investment in a public open access infrastructure.

SCENARIO 1: THE BIG FLIP

OA2020, announced in 2016, seeks to mobilise scholarly organisations (universities, research institutions, funders, libraries and publishers) to convert resources currently spent on journal subscriptions into funds to support open access. The big flip certainly has its advantages. It is probably the most promising approach for open access in the short run. It means that in the medium term, a substantial proportion of paywalled articles would be available under open access licenses. The initiative's playbook is being adopted by the DEAL consortium in Germany in negotiations between a large group of scientific institutions and a few major scientific publishers. Although similar negotiations undertaken by consortia in the UK, Austria, Finland and the Netherlands ended with each agreeing to far less than they wanted, DEAL's strong negotiating style could yield better outcomes (Vogel, 2017). It is hence being watched intently by science funders and science policymakers worldwide. If DEAL has success in pushing the big academic publishers towards flipping, and other countries follow suit such that the OA2020 vision is realised, what sort of open access would we inherit?

While journal flipping would mark a shift in the traditional business model for academic publishing and ultimately lead to many more articles being available under open licenses in the short run, there would be severe adverse effects in the long run.

Large-scale offsetting agreements exclude researchers from institutions and countries that cannot afford to buy in; this will be to the detriment and competitive disadvantage of researchers from poorer institutions. **Journal flipping will likely widen the gap between the rich and the poor in the global academic landscape.**

continue reading on page 80 ▸▸

THIS IS AN ARTICLE BY **BENEDIKT FECHER AND TONY ROSS-HELLAUER**

This essay was first published on 26 October 2017 on the LSE Impact Blog of the London School of Economics and Political Science. Benedikt Fecher and Tony Ross-Hellauer wrote this article in preparation for a panel at FORCE11, a conference for innovation in scholarly communication.

In his research activities, Benedikt Fecher is especially interested in open science, knowledge transfer, and scientific impact. The question that keeps him busy is: "What is scientific impact?". Benedikt Fecher is heading the research programme The Knowledge Dimension at Alexander von Humboldt Institute for Internet and Society. He wrote his PhD on data sharing in academia. In 2016, Benedikt was the scientific advisor to the Leibniz Association on the subjects of open access and research data. Benedikt Fecher is also co-editor of the blog journal Elephant in the Lab, which critically engages with the science system.

Tony Ross-Hellauer is a senior postdoctoral researcher in the Social Computing Research Group at Know-Center. He received his PhD in Information Studies in 2012 from the University of Glasgow. His main research interests are open science models and infrastructures, science policy, alternative models for peer review, and philosophy of technology. Tony Ross-Hellauer is actively involved in open science advocacy and community-building and has worked in a number of EU-funded open science projects. Tony Ross-Hellauer has published widely on open science, open access, peer review and library science and acts as programme committee member and co-organises and co-chairs a number of workshops and conferences on topics related to open science.

Given that many peer-reviewed articles remain uncited and do not even have a disciplinary impact, researchers would contribute more by publishing alternative scientific products, such as open data and code (Larivière, Gingras & Archambault, 2009). Yet, journal flipping would cement the role of the article and make it difficult for new, more digital-savvy products to emerge. **Journal flipping would cement an analogue academic mindset.**

Moreover, journal flipping would reproduce the dependence on a small number of commercial publishers that will likely continue to wield oligopolistic market power. The disproportionate market power of a few players like Elsevier has long been discussed in the open access community and far beyond. **Journal flipping would unnecessarily translate this market power to the digital world.**

Finally, the hurried push to flip journals within costs widely believed to be bloated could mean that **average levels of article processing charges would become inflated**, reflecting current publisher profit margins rather than the true cost of academic publishing.

The clear advantage of journal-flipping open access is its short-term effect. There is hardly a solution that would make more journals and articles open access in a short time. Plus, this approach will likely cost academia less than having libraries and research institutions negotiating individual licensing agreements with publishers—which is the situation now.

SCENARIO 2: A PUBLIC OPEN ACCESS INFRASTRUCTURE

An alternative future would be one in which a concerted and coordinated attempt is made to implement an open, public infrastructure. There are many pieces of such an infrastructure already in place, although at the moment they are scattered. For instance, the FairOA initiative calls for models where publication is not dependent on payments from authors or institutions and costs are "low, transparent, and in proportion to the work carried out". How this might be achieved sustainably is shown by the Open Library of Humanities (OLH), an academic-led gold open access publisher that circumvents Article Processing Charges (so-called APCs, fees that authors or their institutions pay to a journal for an article to be published open access) by collecting membership fees directly from (currently over 200) research libraries. OLH has been actively involved in "flipping" subscription journals over to its model (Greenberg, 2015).

At the same time, the green open access infrastructure of institutional repositories and preprint servers has been growing in interesting ways. Will preprint servers like arXiv, bioRxiv and the host of newly-created servers hosted by the Open Science Framework integrate review and editing technologies to enable them to become

functional publishing platforms? Could infrastructures like OpenAIRE and visions like COAR Next Generation Repositories provide a way forward for public infrastructures of repositories and overlay journals to create a researcher-centric, public publishing ecosystem (Confederation of Open Access Repositories, 2017)? Meanwhile, science funders like the European Commission, Bill & Melinda Gates Foundation and Wellcome Trust have already announced the establishment of their own open access megajournals. Although currently based on proprietary technologies, it is possible that, in future, these funds would be diverted to support public infrastructures. Overarching all of these developments, the EC's European Open Science Cloud, currently being piloted can be expected to become a central resource for new scholarly communication tools and methodologies that better support data generation and data processing. Most recently, the open-source Collaborative Knowledge Foundation has begun working with publishers like eLife and Hindawi to develop open-source publishing tools, including the PubSweet framework, an open-source platform for scholarly journals. According to Hindawi's Paul Peters (2017), the involvement of commercial actors in such an open enterprise requires four basic principles of openness: open source, open data, open integrations, and open contracts.

The authors believe the way ahead here lies in linking up all such efforts in order to coordinate them into an interoperable public infrastructure, sustainably funded directly by public institutions like research libraries or funders that are able to offer a researcher-centric, low-cost, innovative platform for the dissemination of research. A possible model for coordination of such activities is SCOSS, the Global Sustainability Coalition for Open Science Services, a community-led effort to help maintain, and ultimately secure, vital infrastructure. David Lewis's recent proposal that research libraries set aside 2.5 % of their total budget to support the common infrastructure needed to create the open scholarly commons, if it were to be realised, would ensure money was in place on a sustainable basis to fund these activities (Lewis, 2017).

A future in which coordinated public open access infrastructures play a much stronger role would bring the following advantages.

First and foremost, investing in a public infrastructure for open access could mean overcoming the dependence on a few commercial publishers. Instead of subsidising the big players in the business (e.g. Reed-Elsevier, Springer, Wiley-Blackwell, Taylor & Francis and SAGE) with licensing deals – and thereby perpetuating the same, oligopolistic publishing system – a bold step towards public infrastructures could mean that new players and services emerge.

With overlay models built upon a network of public repositories, the classic publishing model with an editorial board and a peer-review system would remain intact. Though this model itself can be criticised – in light of the replication crisis, for example – it

would not confront risk-averse authors with a completely new system. **It could be a starting point to push the necessary change required in academic publishing in small doses (e.g. with regards to a data and code policy)**.

A public infrastructure could widen the scope of activities of research libraries, redefining their role in an increasingly digital world. Instead of managing subscriptions for journals, they could provide the technical infrastructure for publishing and offer related services.

A truly public open access infrastructure would be open to access and to publish for researchers from everywhere . Whereas big deals (as in scenario 1) mainly benefit researchers affiliated with (relatively well-resourced) institutions that are included in the negotiations, public infrastructures would be better able to offer services regardless of ability to pay, thus not excluding researchers from the Global South.

THE RIGHT WAY FORWARD?

These two scenarios, although presented as a dichotomy, are not mutually exclusive. The open access future that will eventually come true will probably include a mix of flipped journals and public infrastructures. Nevertheless, the decisions made now will determine the degree to which either is favoured. Hopefully this article has shown that the chance to create a coordinated public open access infrastructure is at hand. ◆

REFERENCES

Cold Spring Harbor Laboratory (2017). bioRxiv. Retrieved from https://www.biorxiv.org

Collaborative Knowledge Foundation (2017). Coko Technology. Retrieved from https://coko.foundation/technology

Confederation of Open Access Repositories (2017). Next Generation Repositories. Behaviours and Technical Recommendations of the COAR Next Generation Repositories Working Group. COAR.

Cornell University Library (2017). arXiv.org. Retrieved from https://arxiv.org

Enserink, M. (2016, May 27). In dramatic statement, European leaders call for 'immediate' open access to all scientific papers by 2020. *Science*. Retrieved from https://doi.org/10.1126/science.aag0577

Fair Open Access (2017). Retrieved from https://fairoa.org

Fecher, B., Friesike, S., Hebing, M., & Linek, S. (2017). A reputation economy: how individual reward considerations trump systemic arguments for open access to data. *Palgrave Communications, 3,* 17051.

Fecher, B., Friesike, S., Peters, I., & Wagner, G. (2017, April 10). Rather than simply moving from 'paying to read' to 'paying to publish', it's time for a European Open Access Platform. *LSE Impact Blog.* Retrieved from http://blogs.lse.ac.uk/impactofsocialsciences/2017/04/10/rather-than-simply-moving-from-paying-to-read-to-paying-to-publish-its-time-for-a-european-open-access-platform

Greenberg, J. (2015, May 11). Editors of the Journal Lingua Protest-Quit in battle for Open Science. *Wired*. Retrieved from https://www.wired.com/2015/11/editors-of-the-journal-lingua-protest-quit-in-battle-for-open-access

Larivière, V., Gingras, Y., & Archambault, É. (2009). The decline in the concentration of citations, 1900-2007. *Journal of the American Society for Information Science and Technology, 60*(4), 858–862.

Lewis, David W. (2017). *The 2.5% Commitment*. Indianapolis: Indiana University-Purdue University Indianapolis.

Open Access 2020 (2017). Retrieved from https://oa2020.org

OpenAire (2017). Retrieved from https://www.openaire.eu

OSF Reprints (2017). Retrieved from https://osf.io/preprints

Peters, P. (2017, October 23). A radically open approach to developing infrastructure for Open Science. *Hindawi*. Retrieved from https://about.hindawi.com/opinion/a-radically-open-approach-to-developing-infrastructure-for-open-science

Projekt DEAL (2017). Retrieved from https://www.projekt-deal.de

Ross-Hellauer, T. (2017, June 8). OpenAIRE can form the basis for a truly public European Open Access Platform. *LSE Impact Blog*. Retrieved from http://blogs.lse.ac.uk/impactofsocialsciences/2017/06/08/openaire-can-form-the-basis-for-a-truly-public-european-open-access-platform

Schimmer, R., Geschuhn, K. K., & Vogler, A. (2015). Disrupting the subscription journals' business model for the necessary large-scale transformation to open access.

The Global Sustainability Coalition for Open Science Services (2017). Facilitating funding to ensure the long-term sustainability of Europe's Open Science infrastructure. *SCOSS*. Retrieved from http://scoss.org

University of Leipzig (2017). Open Libraries of Humanities. Retrieved from https://www.openlibhums.org

Vogel, G. & Kupferschmidt, K. (2017, August 23). A bold open-access push in Germany could change the future of academic publishing. *Science*. Retrieved from https://doi.org/10.1126/science.aap7562

"Of course, newspapers and television channels still exist and are important, but the distributing agency has now seriously gravitated towards one specific node: Facebook."

IS POLITICAL MICRO-TARGETING HIJACKING EUROPEAN DEMOCRACY?

INTERVIEW WITH NATALI HELBERGER AND TOM DOBBER

Tom Dobber, PhD candidate, and Natali Helberger, Professor of Information Law, both at the University of Amsterdam, are studying the individual, societal and legal implications of personalised communication. One of the phenomena that they have put under the magnifying glass is political micro-targeting, a technique employed by politicians to address individual voters with tailor-made messages, attuned to their individual background, attitudes, beliefs, concerns, etc. During campaigns, political micro-targeting can be used to personalise political advertising. Between elections, it is often used to grow the voter base, mobilise voters and keep existing voters engaged.

The interview was published on 18 December 2017 in Internet Policy Review, an open access and peer-reviewed journal on internet regulation, published by Alexander von Humboldt Institute for Internet and Society in cooperation with CREATe (Glasgow), ISCC-CNRS (Paris) and IN3 (Barcelona). The following key questions served as an appetiser to a special issue on political micro-targeting published in that journal in late 2017.

Who are the main actors involved in political micro-targeting? Google, Facebook, Palantir or rather political parties, communication/advertising agencies?

Political micro-targeting involves a network of interdependent actors. Political parties and their campaigns are important, of course, as they are the ones that decide to use political micro-targeting. However, political parties usually do not have the in-house expertise, infrastructure or sufficient data to model who to target with what kind of message, and to subsequently send their tailored messages. That is where third parties come in: communication/advertising agencies and consultancies sell or lease their expertise and infrastructure to political parties. Having said so, hiring third parties can be expensive, and not every party can afford their services.

All parties can use Facebook to specifically, easily and relatively cheaply reach certain groups of people with tailored messages. Kreiss and McGregor (2017) have nicely documented how technology companies such as Facebook offer embedded teams to closely work with campaigns. We see similar developments in Europe as well. During the recent Dutch election campaign, for example, Facebook actively approached political parties and offered them advice on how to best use Facebook for their specific purposes. At the moment, Facebook is a particularly prominent actor as it holds not only detailed data on a large number of people/voters worldwide, but also has the infrastructure and the expertise to use that data. This may rapidly lead to a situation in which Facebook is very powerful because political parties can no longer campaign without Facebook (but Facebook certainly doesn't need every single political party in order to turn a profit).

What's the potential impact of political micro-targeting for democracy in the coming years?

Much will depend on whether and how broadly political micro-targeting techniques will be taken up. In Europe, we observe that parties are at an experimental stage. Many parties are still struggling with the question of the extent to which they should get involved with micro-targeting techniques, if at all. The speed of adoption will depend on whether and how satisfactorily parties can negotiate this question. But institutional dynamics play a role as well. During our research we found, for example, a rather small Dutch party (GroenLinks) was quite advanced and transparent in their data-driven targeting techniques (Dobber, Trilling, Helberger, & De Vreese; not yet published). For instance, they developed their own canvassing app, and worked together with Blue State Digital. As the party ran a successful campaign, they are likely to set an example.

If political micro-targeting practices will indeed become more widespread, they could have positive as well as negative effects for democracy. Political micro-targeting has a positive potential for activating and engaging people. Tailored messages can have some appeal with voters, since they might be understood as more personally relevant, so politics may be perceived less as some abstract process that focuses on issues that are not, or only remotely, related to individual interests. Political micro-targeting could hence result in engaging formerly uninterested citizens and better informing them. Micro-targeting could also have an empowering effect, particularly for smaller parties, provided they are able to innovate and use smart technologies to optimise their campaign. Such smaller parties could potentially

run a more efficient campaign and maximise the effect of their resources (provided they are not in the game of competing with large parties for advertisement space on Facebook).

On the downside, there is a risk of fragmentation of the public sphere and the creation of political bubbles. These developments all have potential negative consequences, such as redlining, polarising and creating new digital divides. How serious these risks are, or how likely it is that they will materialise is difficult to predict. So far, we see that parties typically still use different media outlets in parallel, instead of relying solely on political micro-targeting. This means that at the moment, voters have a more than fair chance of receiving non-micro-targeted messages. Still, there is the undeniable potential for manipulation in micro-targeting. And to make things worse: manipulation is difficult to detect, exactly because of the hyper-personal nature of political micro-targeting.

Another worrisome development that flows from the increasing popularity of micro-targeting is the commercialisation of political advertising. New, commercial, players, such as Facebook and commercial advertising agencies are stepping forward, using essentially commercial strategies for commercial goals. Considerations about democracy, a level playing field or informed citizens make way for profit-maximisation, selling eyeballs and optimising for profitable engagement. As a result, voters increasingly become another target group that one can buy. In such a scenario, it would become possible to essentially buy elections, thereby turning politics into just another commercial business.

Did political micro-targeting play a relevant/marginal role in recent elections (i.e. the Dutch, French or German elections) and referenda in the EU (i.e. Catalonia, Brexit, Scotland)?

There are large differences between the countries. In the past Dutch elections in March 2017, many campaigns tried to micro-target for the first time. All parties used Facebook, but some parties went further and developed their own micro-targeting tools. Of course, micro-targeting was only part of a more comprehensive strategy that also involved broadcast media and traditional campaigning efforts. Interestingly enough, in neighbour-country Germany, there was hardly any micro-targeting efforts during the 2017 elections, as research from Kruschinski and Haller (forthcoming, 2018) shows, despite the fact that the budgets of the German parties can be up to ten times larger than those of their Dutch counterparts. However, the party that won the largest support, Christian Democratic Union (CDU), did

use a canvassing app that helped its campaigners to map the electorate and manage its resources more efficiently. During the Brexit referendum, micro-targeting appeared to play a role as well. The extent of that role is under investigation: the UK's independent Information Commissioner's Office (ICO) launched a probe into the use of personal data and data-analytics by political parties. The ICO investigation especially focuses on the role of commercial third parties, such as Cambridge Analytica and Aggregate IQ.

What are the three aspects of political micro-targeting that need to be fixed asap?

First: One aspect that needs fixing, and rather sooner than later, are the differences in the protection of consumers vis-à-vis commercial targeting and political micro-targeting. Right now we have a somewhat peculiar situation, in that consumers, as the intended audience of commercial micro-targeting, enjoy rather far-reaching rights to information, fairness in advertising and protection from misleading claims and unfair practices, but these rules are not applicable to political micro-targeting. Evidently, there are (significant) differences in commercial and political micro-targeting, but it is difficult to comprehend why the subjects of political micro-targeting are less entitled to protection from misleading or manipulative claims or from the lack of clear labelling of political micro-targeting practices. Campaigns typically fall under election laws that, in many cases, don't offer voters a comparable level of protection. The resulting discrepancy between voter and consumer rights needs our attention.

Second: Related to the former point is the fact that, from the perspective of citizens, transparency about being micro-targeted would help voters. A common feature of micro-targeting is that it is difficult to recognise that a tailored message is ... tailored. A voter is likely to think that a certain message is not tailored to her specifically, but to the entire electorate. When micro-targeted messages are recognisable as such, it may become more difficult to manipulate voters.

Third: Another point of immediate concern is the boundless commercialisation of politics and the accompanying "winner-takes-it-all" scenario that follows from it. There are indications that in Europe, Silicon Valley platforms are slowly rising to become pivotal platforms for campaigning. To the extent that these platforms approach political micro-targeting as "just another form of advertising revenue", this can be highly problematic for the political process, as the recent discussions about foreign influences and voter manipulation suggest.

If you could research the phenomenon with an unlimited budget at your disposal, what research objectives would you aim at and what methodology would you use to achieve these objectives?

We would aim at a large field experiment in which we would micro-target different groups using different techniques (personalised canvassing, personalised social media advertising, personalised post and email messages, etc.). We would then look for intended and unintended effects in general and for the democratic process, short and long-term effects on, and any changes in voter behaviour, political literacy, attitudes, creepiness factor, etc. Such a study would ideally be comparative because cultural differences, differences in election systems, regulations and other contextual factors are likely to influence the effects of micro-targeting. Europe would be a great location to conduct such research, because of the diversity of its cultures and electoral systems in a relatively small area. At the moment, the effects of micro-targeting are understudied empirically, and a comparative study would yield important knowledge. ◆

REFERENCES

Kreiss, D., & McGregor, S. C. (2017). Technology firms shape political communication: the work of Microsoft, Facebook, Twitter, and Google with campaigns during the 2016 U.S. presidential cycle. *Political Communication, 0*(0), 1–23.

Kruschinski, S., & Haller, A. (2017). "What is predictive modelling?" Restrictions for data-driven political micro-targeting in Germany using the example of door-to-door campaigning. *Internet Policy Review, 6*(4).


81.50
45.25
0.04
5.15
40.75
4
4.02
0.02
0.02
1.26
1.27
1.88
1.91
2.86
2.90
1.80
1.81
5.20
5.15
1.62
1.64
3.02
3.06
2.44
2.32
8.45
8.45
11.10
11.20
28.50
28.50
1.89
1.89
1.90
15.30
15.30
15.50
1.32
1.30
1.32
8.70
8.70
8.80
8.65
3.80
3.80
3.80
5.75
5.80
6.45
6.25
6.30
0.29
0
340
320
300
280
NW
W

WAHLKOMPASS DIGITALES
THE DIGITAL IN GERMAN POLITICS

How parties envision the process of digitisation is becoming an increasingly important factor in the fight for political power. How do parties view AI, what are the prospects for eGovernment and in what way is digitisation changing how scientific research is funded? Alexander von Humboldt Institute for Internet and Society (HIIG) set out to build a helpful online tool. The election programmes of six German parties were analysed regarding digital policy in different areas: health, government, security, infrastructure, media, economy and education. As a result, the Wahlkompass Digitales, or Digital Election Compass, was created – an interactive website to compare party programmes on digital politics. It generated about 50,000 views. HIIG researchers referred to the tool to reflect on the German parties' positions during the 2017 federal elections which will likely shape the agenda of digital politics in the upcoming years. Five articles, published within a dossier on the institute's Science Blog, are introduced here:

Christian Djeffal and Stefan Baack

CUSTOMER, READER OR ACTIVIST? CITIZENS IN THE PROCESS OF DIGITISING GOVERNMENT

The party platforms for the German general election 2017 agree on one point: public administration ought to be digitised. Yet, German parties have three different types of citizen in mind. Clients, who seek to find fast and reliable government services online. Newspaper readers, who wants to have a range of diverse digital information to form their political views, and digital activists, who are looking for new forms of digital engagement.

Florian Lüdtke

ABOUT TESTED CAMPAIGN PROMISES AND BURST BUBBLES

Before the elections in Germany, different types of voting advice applications appeared. Many of them, like the Digital Election Compass or the chatbot Wahltraud are purely informative and help voters to get a better overview of the parties' positions. Others, like the Wahl-o-mat, show the user's political proximity to the various parties. A new kind of online tool sets out to burst so called filter bubbles.

Benedikt Fecher and Nataliia Sokolovska

DIGITAL RESEARCH POLITICS

Digitisation is changing science and research. The following German parties are paying attention to digitisation in research: the SPD, FDP and Greens, although to different extents. The burning issues included open access, online learning, free software, and technical facilities. The shocking news: the CDU, Greens and AfD aren't paying any or enough attention to changes in science. Several very relevant topics for science in the digital age were not mentioned once: citizen science, a public infrastructure for publications, and the internationalisation of higher education.

Christian Djeffal

ALGORITHMS, ROBOTS AND SMART MACHINES: HOW GERMAN PARTIES DEAL WITH AI

In the future it might be necessary to have the algorithms of your digital assistants checked by state authorities. The German political debate on a possible test certificate (Algorithmen-TÜV) showed the relevance of that idea – all parties but the AfD mentioned this issue. One point for clarification: author Christian Djeffal asserts that none of the parties has a detailed plan when it comes to AI-based systems such as algorithms, robots and smart machines.

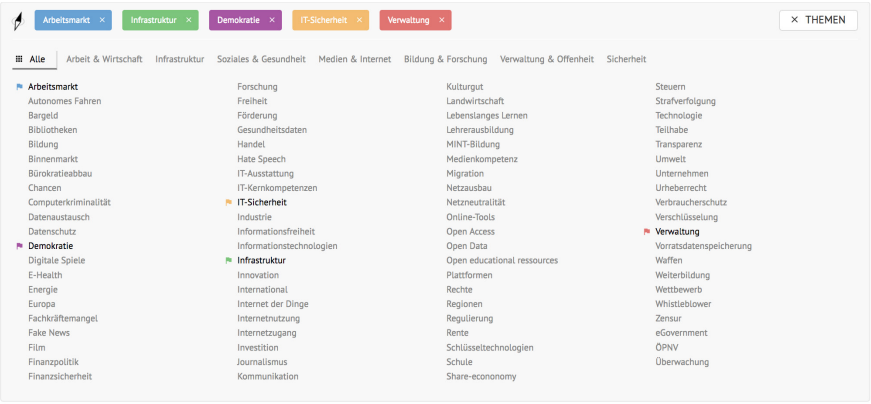
Jörg Pohle

STATE HACKING AND IT SECURITY

Despite the common belief that freedom and security are antagonists, there are some issues where they're on the same side. For example, in areas such as IT security, especially with respect to state hacking and the retention of information about security vulnerabilities in ICT systems by the state. The CDU and SPD regard IT security as part of the state's responsibility. Only the Greens, the Left and to some extent the FDP think that IT security is a fundamental citizens' right and warn that the state should keep this in mind and guarantee it in light of mass surveillance, for example.

wahlkompass-digitales.de

hiig.de/dossier/btw17



Issues addressed by digital policy are manifold. The topics that related to the parties' digital policies were clustered into seven areas. The user could select up to five topics of interest.

CDU/CSU 19 13 2 6 15

- Viele Ideen, die im Bereich der Globalisierung die Welt verändert haben, sind in jungen Unternehmen, den sogenannten Start-ups, entstanden. Deutschland hat in diesem Bereich Boden gut gemacht. Aus der ganzen Welt kommen Menschen mit Ideen nach Deutschland, gründen Unternehmen und schaffen Arbeitsplätze. Wir werden sie ermutigen und unterstützen. Durch die steuerliche Forschungsförderung und ein Fachkräfte-Zuwanderungsgesetz ebenso wie durch bessere Gründungs- und Wachstumsfinanzierung sowie weniger Bürokratie. Wir werden die Einführung einer zentralen Anlaufstelle (one-stop-shop) speziell für diese Unternehmen prüfen.
- Gerade in einer zunehmend digitalisierten Gesellschaft hat die Grundversorgung der Bevölkerung mit postalischen Dienstleistungen weiterhin einen wichtigen Stellenwert. Eine flächendeckende, schnelle und erschwingliche Zustellung von Briefen und Paketen bleibt ein wichtiges Standortkriterium. Bestehende Regulierungen werden wir deshalb überprüfen und gegebenenfalls anpassen.
- Wir wollen leistungsfähige und sichere digitale Bezahldienste. Auch im Zeitalter der Digitalisierung bleibt aber das Bargeld ein wichtiges Zahlungsmittel.
- Alle diese Anwendungen werden nur dann Erfolg haben, wenn die Menschen auf einen sicheren Betrieb von Anfang an vertrauen dürfen. Kluge, umfassende und fortschrittliche IT-Sicherheit ist die Grundlage für ein erfolgreiches digitales Deutschland. Dafür werden wir sorgen.

9.5. Chancen für Bildung und Wissen

Die großen Chancen, die für Deutschland mit der Digitalisierung verbunden sind, können wir nur dann wirklich nutzen, wenn wir in allen Bereichen über genügend gut und hervorragend ausgebildete Arbeitskräfte verfügen. Deshalb brauchen wir eine „Digitale Bildungsoffensive": Für Schüler, Auszubildende, Studenten und Lehrkräfte gleichermaßen. Aber ebenso auch für Arbeitnehmerinnen und Arbeitnehmer, die sich qualifizieren und weiterbilden wollen und müssen, weil lebenslanges Lernen schon heute eine Selbstverständlichkeit ist.

- Wir werden mit einem Digitalpakt dafür sorgen, dass unsere allgemeinbildenden und beruflichen Schulen über die erforderliche Ausstattung verfügen, um ausreichend junge Menschen auf ihr Berufsleben im digitalen Zeitalter vorzubereiten.
- Wir stellen sicher, dass bundesweit alle Schulen an das schnelle Internet angebunden sind. Das Gleiche gilt für Hochschulen.
- Wir unterstützen die Schaffung einer innovativen neuen Bildungs-Cloud, mit der wir über Deutschland hinaus neue Maßstäbe setzen werden.
- Wir werden die Länder dabei unterstützen, durch Weiterbildung von ausreichend Lehrerinnen und Lehrer die digitalen Kompetenzen der Schülerinnen und Schüler möglichst umfassend zu fördern.
- Wir legen eine „Nationale Weiterbildungsstrategie" auf, die wir gemeinsam mit Arbeitgebern, Gewerkschaften und zuständigen Stellen erarbeiten.

Die Grünen 18 12 8 14 3

Wir wollen die Potenziale des digitalen Wandels für Bildung und Forschung, gleichberechtigte Teilhabe, sozialen Fortschritt und eine nachhaltige Wirtschaft nutzen. Für Innovationen im digitalen Zeitalter, bessere (digitale) Infrastruktur und für mehr IT-Sicherheit für alle Menschen und Unternehmen ist Regulierung erforderlich. Demokratie IT-Sicherheit Verwaltung Gemeinsam mit einer engagierten Zivilgesellschaft streiten wir für schnelles, neutrales Internet und starke Verbraucher*innenrechte, mehr E-Government und offene Daten, freie und offene Software sowie Vertrauen durch Sicherheit in der digitalen Welt und gegen Massenüberwachung und uferloses Aufrüsten der Geheimdienste.

4.6.1. Schnelles und offenes Internet für alle

4.6.2. Gemeinsam gegen Hass im Netz

Mit Sorge beobachten wir die Verbreitung von Hass und Hetze im Netz. Die Strafverfolgung hingegen hinkt diesen Auswüchsen weit hinterher. Wir GRÜNE wollen dafür sorgen, dass Menschen, die sich volksverhetzend äußern oder andere mit Mord- und Vergewaltigungsfantasien bedrohen, konsequent zur Rechenschaft gezogen werden. Große Anbieter sozialer Netzwerke gehören hier in die Pflicht genommen, dürfen aber nicht in eine Richter*innenrolle gedrängt werden. Sie müssen offensichtlich strafrechtswidrige Inhalte umgehend löschen. Gerichte und Strafverfolgungsbehörden müssen sie bei der Dokumentation und Verfolgung solcher Fälle unterstützen. Dafür ist rund um die Uhr eine inländische Kontaktstelle für Anfragen von Strafverfolgungsbehörden vorzuhalten und sind entsprechende Reaktionsfristen einzuhalten, ansonsten drohen Bußgelder.

Einer Aushebelung der anonymen und pseudonymen Nutzung von Online-Diensten und damit der Meinungsfreiheit und -vielfalt stellen wir uns klar entgegen. Auskunft über Bestandsdaten von Nutzer*innen an private Dritte auf Entscheidung der Anbieter lehnen wir ab. Strafverfolgungsbehörden und Gerichte müssen technisch und personell so ausgestattet werden, dass sie Rechtsverstöße im Netz in angemessener Zeit bearbeiten können. Hasspostings und Falschmeldungen sind oft auch ein Fall für die medienrechtliche Aufsicht, die wir entsprechend ausstatten wollen. Im Netz muss erkennbar sein, ob Mensch oder Maschine kommunizieren. Wir fordern deshalb eine Kennzeichnungsp icht für Computerprogramme (Social Bots), die eine menschliche Identität vortäuschen und zu Zwecken der Manipulation und Desinformation eingesetzt werden können.

Nicht alles, was hetzerisch im Netz geäußert wird, ist rechtswidrig. Meinungsfreiheit gilt auch für abseitige, oftmals schwer erträgliche Positionen. Wir fordern Internet-Unternehmen auf, intensiv mit Organisationen zusammenzuarbeiten, die sich für Opfer von Hass und Hetze, Rassismus und Diskriminierung im Internet einsetzen, und diesen auch direkte Meldewege zur Verfügung zu stellen. Ein demokratisches Netz braucht Nutzer*innen, die Hass und Hetze eine klare, ethisch begründete Haltung entgegensetzen, die Inhalte kritisch hinterfragen, um Falschmeldungen keine Chance zu geben, und die sich aktiv in Diskussionen mit Gegenrede einbringen, um Betroffene von Rassismus und Mobbing zu unterstützen. Ein freies, offenes und inklusives Netz lebt von der Einbindung und dem Engagement der Zivilgesellschaft.

Digitale Kompetenz ist heute eine Grundvoraussetzung für gleichberechtigtes und selbstbestimmtes Leben. Wir wollen daher mehr Programme für digitale Bildung und

The user then chose two party programmes for comparison. Paragraphs regarding digitital policies were highlighted according to the above selected topics.

HENRIKE MAIER

Increased liability for linking and streaming

Two judgements of the Court of Justice of the European Union (CJEU) in 2017 dealt with the (il)legality of linking and streaming in terms of copyright. The decisions could also become important for the current copyright reform and for hosting platforms.

The first CJEU ruling (Case C-527/15 – *Stichting Brein*) concerns a media device distributed in the Netherlands: *filmspeler*. This enabled users to access movies from external streaming sites on their TV screens via an easy-to-use graphical interface. Some of the linked streaming pages contained illegally uploaded content. Based on this, the seller of filmspeler advertised aggressively. From a technical point of view, however, the device only offered hyperlinks to the streaming pages. The CJEU has now in essence ruled that the sale of such devices is nevertheless not permitted. It found that the seller thereby communicates copyright-protected works to the public without permission and thus infringes copyright (para. 52).

The second decision (Case C-610/15 – *Ziggo BV*) concerns a blocking injunction against the platform *The Pirate Bay*. This site is notorious for facilitating illegal downloads by providing an index of copyrighted works in peer-to-peer networks for downloading. So, although The Pirate Bay does not itself host the works, the court ruled that the platform communicates works to the public and therefore directly infringes copyright. This will make it easier to block this site in individual member states. The court's more precise justification for both judgements is interesting, as it could have far-reaching implications for the grey area of streaming and the liability of other platforms, such as hosting platforms.

IMPLICATIONS FOR THE GREY AREA OF STREAMING

The implications for streaming can be explained quickly: streaming from illegal sources is highly likely to be illegal and is no longer a grey area for users. The CJEU commented on this question because filmspeler merely simplified streaming. If this had already been covered by a copyright exception and had thus been legal, facilitating access to it would also have been unproblematic. With respect to streaming, only the exception for temporary copying comes into consideration (in Germany, this is transposed into law in § 44a of the Act on Copyright – UrhG). During streaming, the data is only stored temporarily. Yet there are further conditions for the exception to be applicable – in particular, the reproduction would have to be necessary in order to permit the lawful use of the work. However, the CJEU made it clear that users of the device cannot claim that they are merely watching the content and are thus not doing anything illegal. It stated that, due to the advertising alone, they were aware that they would thus gain access to "a free and unauthorised offer of protected works" (para. 69). In the CJEU's view, if the exception were to be interpreted more

generously for temporary copies, this would "adversely affect the normal exploitation of such works and cause unreasonable prejudice to the legitimate interests of the right holder" (para. 70). The judgement thus strengthens the position of copyright holders, because when using most streaming sites it should be clear to users that they are watching content that has made its way onto the internet by illegal means. The prosecution of individual users may still be difficult for technical reasons. Anyone who uses streaming services, however, is very likely to be infringing copyright from a legal point of view and has little claim to have been acting in a legal grey area.

POSSIBLE IMPLICATIONS FOR HOSTING PLATFORMS

Another interesting aspect of both rulings is that the CJEU has adopted a very broad understanding of the right of communication to the public and its direct infringement. It should be noted that the seller of filmspeler did not upload the copyrighted content, but only facilitated access to the streaming pages with the device. Similarly, The Pirate Bay provides an index and not the works themselves.

This broad understanding of an intermediary company as a direct infringer could have implications for hosting platforms. As the (currently settled) dispute between GEMA and YouTube shows, the parties disagree on whether YouTube as the hosting platform itself is undertaking copyright-relevant activities when users upload videos. German jurisprudence (e.g.: OLG Munich decision from 28 January 2016, 29 U 2798/15) has so far (with good reason) refused to consider the hosting platforms themselves directly liable for their users' copyright infringements. However, distributor liability (in German law this is known as the concept of *Störerhaftung*) was considered, because platforms wilfully make an adequate causal contribution to the infringements. They therefore had to meet certain duties of care to prevent illegal uploads. The CJEU judgements may have changed the legal situation such that platforms will increasingly come to occupy a grey area and find it more difficult to ensure that they themselves are not direct infringers through user uploads. This will also be important in the context of the current copyright reform. This is because a draft directive on copyright in the digital single market (COM (2016) 593 final) proposed by the European commission aims to impose far-reaching filtering obligations on hosting platforms such as YouTube or Vimeo. The relevant provisions in the draft directive have rightfully been criticised for being poorly drafted, imposing far-reaching monitoring obligations and not taking the fundamental rights of the users into account, see e.g. Angelopolous, 2017. The commission also seems to implicitly assume that platforms themselves infringe copyright and can therefore be obligated to introduce filtering mechanisms. This (implied) understanding of what constitutes communication to the public in the draft directive has so far been criticised (see e.g. Angelopolous, 2017). The fact that the CJEU now also assumes a broader reading of this exclusive right – at least to some

continue reading on page 100 ▸▸

THIS IS AN ARTICLE BY **HENRIKE MAIER**

This is an updated version of an article first published on 27 April 2017 on the Science Blog of Alexander von Humboldt Institute for Internet and Society (HIIG). The updated version also considers the implications of the CJEU decision in Ziggo BV, Case C-610/15 from 14 June 2017.

Henrike Maier studied law at the Humboldt University Berlin and the University of Paris 1 (Panthéon-Sorbonne). Her research focuses on copyright and media law as well as European law. She submitted her doctoral thesis on remix videos and hosting platforms in 2017. At Alexander von Humboldt Institute for Internet and Society she works on issues related to orphan works, platform liability, copyright for transnational creative uses, and organises a workshop series on music and copyright in cooperation with the Haus der Kulturen der Welt. From 2017 to 2019 she is undertaking her graduate legal traineeship (Rechtsreferendariat).

degree – seems to confirm the commission's interpretation of the right. However, to fully understand the possible implications of the new ruling for hosting platforms, it is necessary to engage more closely with the complex case law of the CJEU on the right of communicating to the public.

When considering the question of whether a copyright-relevant act has occurred, the CJEU has used a number of criteria that are "not autonomous and are interdependent" (CJEU Case C-527/15 Stichting Brein [2017] para. 30). To prove that the seller of filmspeler communicated works to the public, the CJEU made several arguments. The court stated that the device makes it possible to establish "a direct link [...] between websites broadcasting counterfeit works and purchasers of the multimedia player" and also facilitates access to sites "without which the purchasers would find it difficult to benefit from those protected works" (para. 41). In addition, the court found that the seller was acting with a view to making a profit (para. 51). This argument could – in part – indeed also be applied to hosting platforms. As with filmspeler, the platform operators do not upload content themselves, but the platform's infrastructure increases the retrievability of content and facilitates access. Of course, hosting platforms also benefit financially (mostly via advertising revenue). However, the seller of filmspeler actively promoted the illegal content, so there was no doubt that he acted "in full knowledge of the consequences of his conduct" (para. 41). This may be different for platforms that do not control what their users upload in advance. However, in Ziggo BV, the CJEU – unlike the Advocate General in his opinion – not only relies on knowledge of specific infringements, but also refers to the general knowledge of the operator when it states: "the operators of the online sharing platform TPB could not be unaware that this platform provides access to works published without the consent of the rightholders" (para. 45).

Of course, users also upload some infringing content on hosting platforms. However, the problem occurs on a very different scale on such platforms, and their business models – unlike that of The Pirate Bay – are not primarily designed to promote infringement.

WHY THE JUDGEMENTS ARE PROBLEMATIC

These judgements considerably broaden the scope of direct liability in comparison to how they were previously understood in German law. They are problematic for several reasons. For one thing, despite this broadening, the CJEU does not address how direct liability and contributory liability are to be distinguished. The latter is not yet harmonised by European law. According to current understandings in Germany and other member states, subjective elements – knowledge or some form of red flag knowledge – do not play a role for direct liability, but do play a role for contributory

liability (Ohly, 2017, p. 797). This distinction is increasingly being blurred by the recent CJEU case law.

In addition, both cases were based on situations in which the copyright infringement was evident and even advertised. However, the CJEU has not commented on whether the standards would continue to apply to legitimate business models in unaltered form. In this case, there would be a risk of extensive liability for damages (instead of the mere requirement to take the content down). If, for example, hosting platforms were held liable as direct infringers for the copyright-infringing posts of their users, they would have considerable incentives to block content in doubtful cases. This would not be good news for remixers, as this would encourage comprehensive filtering for copyright-protected content, which could also result in legal content such as parodies being taken down. These questions have not yet been finally decided. How the German courts will deal with the new criteria from Luxembourg is awaited with bated breath. ◆

REFERENCES

Angelopoulos, C. (2017). On Online Platforms and the Commission's New Proposal for a Directive on Copyright in the Digital Single Market.

Ohly, A. (2017). Der weite Täterbegriff des EuGH in den Urteilen »GS Media«, »Filmspeler« und »The Pirate Bay«: Abenddämmerung für die Störerhaftung. *ZUM*, 793 – 802

"[Blockchain technology] will prove to be more disruptive
than most can imagine at this stage."

BEYOND THE BLOCKCHAIN BOOM
INTERVIEW WITH SHERMIN VOSHMGIR

As an open, decentral public ledger and the technical innovation behind Bitcoin, blockchain technology is revolutionising the financial sector. Shermin Voshmgir, founder of BlockchainHub, sees blockchain technology as the driving technology of the next generation internet. Even so, it is still in the early stages of development and has many technological and legal challenges to face. BlockchainHub is an international network of autonomous hubs that promote the idea of blockchain, crypto-economics and the decentralised web. Shermin Voshmgir regularly speaks at conferences and consults on blockchains and the social impact of future technologies. She was interviewed by Farzaneh Badiei, a former fellow and associate researcher at Alexander von Humboldt Institute for Internet and Society.

Why did you become interested in blockchain in the first place?

Blockchains dis-intermediate and disrupt governance by offering an incentive system for decentralised coordination of a disparate group of people who do not know and trust each other. Auto-enforceable smart contracts could disrupt traditional governance structures by reducing bureaucracy through lower transaction costs, solving principal–agent issues, and subsequent moral hazard. It enables a new set of organisations, so-called decentralised autonomous organizations (DAOs), where the bylaws of an organisation are encoded in the protocol or smart contract, and auto-enforced by a P2P network of computers. Instead of having centralised legal entities that coordinate in a more or less top down way and have legal agreements with their employees, contractors and clients, we now have a distributed network of autonomous actors that opt into a network ruled by pre defined code: no legal entities run these organisations, and there are no classic legal agreements (yet).

Now that the hype about the revolutionary power of blockchain has passed, what kind of realistic changes can you see blockchain bringing about in our lives?

I don't believe the hype has passed. In my opinion, we are in the middle of the hype cycle. But to answer your core question: blockchain and similar distributed technologies, are still in the very early stages of development. There are many technological and legal challenges to face, usability is still bad, and we are far from having the necessary network effects for

many use cases to be viable in the immediate future. If and once this technology reaches its inflection point, it is hard to foresee how things will evolve. I think it will prove to be more disruptive than most can imagine at this stage.

Do you think drawing an analogy between the early days of the internet and present status of blockchain is correct?

Yes, I do. But we have to understand that analogies can also be limiting if we think of them too rigidly. I would say that blockchain is the driving technology in the next generation internet. Some refer to it as the Web 3.0, others as the decentralised web, other to the internet of agreements. In that sense it is similar in its disruptiveness to the Web. While email and world wide web revolutionised information and communication, blockchain can revolutionise agreements, and has the potential to radically disintermediate our value interactions. However, this is a potential. Who knows what technology is lurking around the corner and might build on top of blockchain or substitute for it. Furthermore, I think we should start talking about crypto-economy or crypto-governance instead of blockchain, as we are already seeing the first technologies that are in fact not blockchain but use other crypto-economic mechanisms to reach machine consensus.

What do you think are the most important policy discussions regarding blockchain?

There are many policy issues. However, I would like to focus on the issue of governance beyond code. Many regard blockchain as an operating system for trustless trust: we don't have to trust people anymore, we only have to trust the code. So the theory goes. In reality, formalised and codified governance rulesets can only depict known knowns and known unknowns, but have very limited capabilities to properly deal with unknown unknowns – aka all those events that cannot be anticipated, or have not been considered at the time of writing or agreeing on the code. While machine consensus can radically reduce transaction costs and disrupt traditional governance structures, there is a gap between initial conceptualisations of blockchains and their first instantiations. First use cases show that as circumstances change, protocols can become inappropriate for the new environment and require modification. Modification of blockchain code happens through majority consensus, but reaching consensus in a distributed multi-stakeholder network with sometimes unaligned interests is complex, potentially introducing new agency issues. ◆

BARCAMP

"How do you feel about using # (pound) for groups. As in #barcamp [msg]?"

With this tweet in August 2007, social technology innovator @chrismessina introduced hashtags to bundle conversations around a subject. Ironically, Twitter founder Evan Williams supposedly told Messina that hashtags were too nerdy to go mainstream and that Twitter would rather use machine learning to group tweets together automatically by topic.

WILLIAM DUTTON

Fostering a cybersecurity mindset

Cybersecurity is a broad concept encompassing the "technologies, processes, and policies that help to prevent and/or reduce the negative impact of events in cyberspace that can happen as the result of deliberate actions against information technology by a hostile or malevolent actor" (Clark et al., 2014, p. 2). It involves physical security – such as protection from insider threats – as well as cyber security. It entails all levels of the internet and all the many actors involved in the provision and use of the network, from those governing and building this infrastructure to the diverse array of end users.

Given this broad definition, who then is responsible for cybersecurity? While responsibility is most often contingent on the specific activity and context, it is increasingly clear that the worldwide diffusion of the internet and its incorporation into everyday life has dissipated this responsibility far more than in early stages of computer-mediated media, information and communication systems to involve a wide array of actors across multiple layers of the internet – from internet use to its global governance.

More specifically, the worldwide adoption of the internet has enabled end users not only to access information from around the world, but also to create and otherwise source their own information for the world. In many respects, this has empowered users, as is illustrated by the many ways users are able to challenge those in positions of influence, such as the press, with countervailing information (Dutton, 2009). However, it has also meant that responsibility for the security of information resources on the internet has devolved to include users around the world and the institutions in which they are involved and not only the technical experts engaged in cybersecurity.

This does not mean that end users should be expected to be responsible for their own security online, but they are expected increasingly to have some shared responsibility with other actors. Creating systems that would centrally protect end-users would also undermine their role in creating and using the internet in powerful ways. Put another way, the protection of cybersecurity is no longer lodged solely with the computer experts in some centralised department of information technology within a user's place of work or with their internet service provider. It is distributed globally across over 3.6 billion internet users who share some responsibility in this process with a multitude of other actors.

Unfortunately, this realisation has not been accompanied by strong programmes of research aimed at understanding the attitudes, values and behaviour of users with respect to cybersecurity. However, there have been promising initiatives seeking to bring the social sciences into work on cybersecurity (Whitty et al., 2015). Also, there have been studies focused on particular communities of users exposed to security risks, such as digital rights activists, bloggers, whistle-blowers and journalists (e.g., Coleman,

2014), the victims of romance scams (Whitty & Buchanan, 2012) or consumers involved in online banking (Shillair et al., 2015). In the neighbouring area of privacy research, there has been much work done over decades on the beliefs, attitudes and values of computer and internet users, including on the motivations behind their actions relevant to protecting personal information from unauthorised disclosure (Acquisti & Grossklags, 2008; Bennett & Parsons, 2013). But arguably, a focus on the technical issues of cybersecurity, such as standards, has overshadowed work on the social and cultural issues.

Moreover, with some exceptions, most social and cultural research initiatives have focused on the development of awareness campaigns, information campaigns designed to alert users to security risks. Awareness campaigns have been prominent in a wide range of areas, particularly in research on health behaviour, where social psychologists and other social scientists have sought to convey threats and also change behaviour in ways that might mitigate risks in such areas as anti-smoking and safe sex campaigns. However, translating awareness into behavioural change has been the central difficulty for all such strategies, even with smoking and safe sex, where the behavioural response is relatively simple to convey (Rice & Atkin, 2013). In cybersecurity, the risks are more difficult to communicate, given the multiplicity of risks in particular circumstances, and the remedies, which are often difficult for end users to implement. Too often, the design of systems makes more secure practices less usable (Nurse et al., 2011).

In the cybersecurity area, awareness campaigns are too often focused on generating fear among users, fear that they will be harmed if they do not follow safe practices (Bada & Sasse, 2014). Yet seldom are these fear campaigns accompanied by clear instructions on best practice nor are they useable and acceptable, such as memorising dozens of more complex passwords and frequently changing them (Whitty et al., 2015). Simple practices in the eyes of security practitioners often fail as useful guides to end users. In fact, fear campaigns can have a chilling effect and otherwise be counterproductive if they are not tied to clear approaches to addressing the problem (Lawson, 2016).

Fear campaigns might work in some areas, such as health campaigns on smoking, where there is a clear response (stop smoking). But failure is common even in these areas, since behavioural change is dependent on messages being well produced and anchored in strong social psychological theories of behaviour change. In the area of cybersecurity, they have proven less effective, as the threats and solutions are ever changing and the problems seem to be mounting (Bada & Sasse, 2014). Rather than simply blame users for not following safe cybersecurity practices, more focus needs to be placed on designing systems for which security practices are more usable, as is reflected in moves toward the use of more biometric data. However, this is particularly difficult given the diversity of uses and contexts of use around the internet. It was in the context of these dilemmas that I stumbled upon the concept of a cybersecurity mindset.

THE IDEA OF A CYBERSECURITY MINDSET

In a conversation at a workshop on cybersecurity, Alastair Cook (2014), director of Critical Insight Security Ltd., argued that the challenges in this area required a security mindset among internet users, which I would define as a set of attitudes, beliefs and values that motivate individuals to continually act in ways to secure themselves and their network of users, for instance, by acquiring technical skills, new practices or changing their behaviour online. This is not necessarily the adoption of a particular set of practices or habits, like changing your password, since secure behaviour will change over time and across contexts. It could, however, involve keeping an open mind to changing cybersecurity threats and practices.

The idea is that users need to prioritise cybersecurity in all aspects of their online behaviour as a matter of course. Rather than following a learned set of practices or habits, individuals could internalise this goal in ways that motivate them to prioritise security in their online behaviour. As noted above, research has begun to explore attitudes toward cybersecurity, as well as the practices of users with respect to security. However, could the concept of a "security mindset" be a subtle but important shift away from more common notions of the priority given to security attitudes and practices, such as habits?

Is this indeed a significant shift in thinking about cybersecurity? Can the concept of a security mindset be conceptually defined and empirically operationalised? Perhaps it is also a more qualitative shift to a sensitising concept that captures a complex set of concrete habits, values and attitudes of internet users? In either case, would it be a positive direction for guiding policy and practice? If so, how could this be accomplished? What are the policy implications of efforts to foster a security mindset?

REASONING THROUGH ANALOGY – WITH A BICYCLE

An analogy might be useful before I try to develop the concept more precisely. Any analogy is inherently inaccurate of what it represents, and better analogies might be suggested, but the example of bike security came immediately to mind when faced with the idea of a cybersecurity mindset.

Since I had lived in Oxford for over a decade, where bikes are a major mode of transportation, and routinely biked to work, it was clear that nearly all bike riders in this city had a security mindset. For instance, they do not think about whether or not to buy a lock, or whether or not to lock their bike when they leave it. They just do these things as a matter of course. It is a habit, yes, but also a mindset in that those purchasing or riding a bike have incorporated a set of assumptions that eliminate

the need to move through a set of decisions on each particular occasion. They are not going through a threat assessment each time they purchase a bike or get on their bike. They simply follow a course dictated by their security mindset.

Security provides a context to other decisions about other things. A person might even buy an older or less attractive bike in order to reduce the risk of it being stolen. In such ways, bike riders in Oxford feel as if they know what to do in order to better secure their bikes. They have a sense of personal efficacy associated with bike security. Moreover, it is a framework arising from the bottom up, rather than from the top down. For example, a bike lock is not part of the bike, or a required purchase, but something most users would incorporate with the purchase of a bike. The lock is viewed as part and parcel of the bike. As it is bottom up, it is socially supported by fellow bike owners. All riders lock their bike, and would question anyone who did not. Everyone can advise others on ways to secure their bikes. Buying a lock is not viewed as odd, but as normal. Not buying a lock would be viewed as silly by other bike riders, but it is not required by law.

In contrast, bike safety – not security – might be less of a mindset in that you can see wide variation among bike riders. Some equip themselves with helmets, reflective clothing, and more, while others do not. Riders are more likely to go through a process of threat modeling, such as weighing the choices on whether or not to use a helmet, depending on where they are riding and what they are wearing, than on whether to secure their bike. Should I stay behind the bus, and have a 100 % chance of losing my momentum, or veer around the bus with a 1 % chance of being hit by a car? Safety might be a mindset for some, but it appears less universal and more flexible than a bike security mindset.

A BIKE IS NOT A COMPUTER NETWORK

Of course, protecting a bicycle is very different from protecting a computer device, or personal information in the cloud. I would argue that this makes the analogy all the more powerful, since it moves discussion away from specific practices or rules that vary across different technical systems. Instead, it highlights the personal and social factors behind a motivation for security practices, whatever they may be.

That said, some have raised problems with my bike analogy. The first concerns the visibility of the security issue. You know sooner or later when your bike has been damaged or stolen, but it is often far more difficult to detect whether your networked computing resources have been tampered with, copied, or disclosed without your authorisation. Increasingly, breaches of a computer can leave no physical evidence of being compromised, such as not changing its performance. Perhaps this difference in

continue reading on page 114 ▸▸

THIS IS AN ARTICLE BY **WILLIAM DUTTON**

This piece is a shortened version of an article published on 19 January 2017 on the Internet Policy Review, a peer-reviewed online journal on internet regulation in Europe.

William H. Dutton is the Quello Professor of Media and Information Policy in the Department of Media and Information, College of Communication Arts and Sciences at Michigan State University, where he is Director of the Quello Center. Prior to this appointment, William Dutton was Professor of Internet Studies at the Oxford Internet Institute, University of Oxford, where he was the Founding Director of the OII and a Fellow of Balliol College. William Dutton received a Lifetime Achievement Award for his role as Founding Director of the OII. He is also the recipient of the International Communication Association (ICA) first Fred Williams' award for contributions to the study of communication and technology, the William F. Ogburn Lifetime Achievement Award from the Communication and Information Technologies Section of the American Sociological Association in 2014. He was named an ICA Fellow in 2015 and received an Endowed Faculty Medallion from MSU in 2017.

transparency or visibility suggests a direction for supporting a cybersecurity mindset. The visibility of spam, for example, enabled spam filters to be widely accepted and used. The visibility of a stolen bike or a breach of your computer could help foster a security mindset.

Another concern raised was over the degree that individuals who have poor security practices in relation to computer networks are likely to have consequences for those with whom they communicate, while the consequences of a stolen bike are likely to rest more squarely with the individual who failed to secure it. In this case, I find the bike analogy valuable, despite this difference, because there is clear social pressure to adopt a bike security mindset even when the consequences are less networked. Again, the visibility of not following these practices could be a key difference. When friends realise a problem with another person's bike or computer security, such as when they receive spam from a friend, they do sanction their friends. Visibility or transparency might be key to building a cybersecurity mindset by also enhancing the likelihood of peer social influence.

DEFINING A MINDSET

The idea of a cybersecurity mindset arose from qualitative interviews, conversations with cybersecurity researchers and practitioners, and participant-observation around the social aspects of cybersecurity. Within a qualitative tradition, this concept, like many other qualitative concepts is what Herbert Blumer (1954) has called a "sensitizing concept". That is, the concept helps to sensitise the reader to a complex set or patterns of concrete empirical observations. It is not a quantitative concept that is operationally defined, such as by answers to questions or by specific behaviour. It is more flexible, and does not have a definitive set of empirical attributes since it could be manifested in different ways across time or contexts. It is in this tradition that I am employing the concept of cybersecurity mindset, as a sensitizing concept within a qualitative perspective of social research.

So – what is in a mindset? As noted above, I have defined a cybersecurity mindset as a pattern of attitudes, beliefs and values that motivate individuals to continually act in ways to secure themselves and their network of users. A mindset suggests a way of thinking about a matter of significance. It is a firm – not a fleeting or ephemeral – perspective or framework for thinking about other things. In other contexts, a mindset has been usefully defined as "how we receive information" (Naisbitt, 2006: xvii). For example, the same information, such as an email attachment, will be received in different ways if one has a cybersecurity mindset. And it shapes choices about other

matters. A security mindset might drive decisions about other aspects of internet use. It arises from the interaction of peers – bottom up – rather than from sanctions or directions from above. In line with this, it is supported socially, such as through the social influence of friends and fellow users, and sources of information chosen by users.

Different actors, such as cybersecurity experts versus end users, will manifest a cybersecurity mindset in very different ways. For example, the security experts with such a mindset would be constantly considering ways that a technical system could be breached, as these mental scenarios will lead them to design systems and train users to avoid the problems they anticipate. Users are unlikely to think about how malicious users might try to steal their information, but they are likely to consider ways to keep their equipment and network resources safe from others, if they have a cybersecurity mindset.

It is immediately apparent that a mindset is not a dichotomous state. It is not that you have it or you don't. For example, a security mindset might be so disproportionate to the risks, that it would be dysfunctional. Alternatively, there could be an absence of a security mindset by many internet users, who fail to take minimal precautions in their computing practices, such as protecting passwords, or changing the default password on the wireless router. These two extreme examples suggest that a security mindset can err on either being set too high or low, exaggerating or underestimating threats. In the bike analogy, there is also no guaranteed security with a lock that can be cut, but it would be a disproportionate response for people to stop riding their bikes on the grounds that they inevitably must leave them in public places.

The bike example also suggests that a disproportionately high cybersecurity mindset might be a functionally rational response to the perceived lack of a security mindset by too many users. In this sense, adoption of a security mindset would be in the interest of all actors in the larger context of users.

More importantly, however, it is unclear that the experts in IT can continue to protect institutions and the public on their own, given the nature of the internet and web and social media, which will be exacerbated by the rise of the Internet of Things (IoT). Clearly, the larger public of internet users need to be enrolled in a security mindset. The IT security officers will be less significant, making a mindset more relevant to a larger public. "[A security mindset] should be more accessible as technical understanding and technical measures become less significant in the management of security" (Cook, 2014). Over time, as current security practices become outdated, such as reliance on passwords, technical know-how might well diminish in importance, relative to the motivations of users that are anchored in more social and psychological processes.

CONCLUSION

Social research on cybersecurity will need to move away from models based on pro-health and other awareness campaigns that have more obvious sets of safe practices. We need research anchored in cybersecurity challenges and behaviour, as well as on other related online issues, such as user perspectives on privacy and surveillance. There is a need to identify those with a cybersecurity mindset, to understand how to diffuse this mindset, and to gauge what impact its acquisition is likely to have on cybersecurity. At the same time, it is important to recognise that a cybersecurity mindset is but one possible aspect of the social and cultural dimensions of cybersecurity that need to be addressed alongside allied efforts to enhance educational, technical, organisational, business, policy and regulatory approaches to cybersecurity.

REFERENCES

Acquisti, A., & Grossklags, J. (2008). What can behavioral economics teach us about privacy? In Acquisti, A., Gritzalis, S., Lambrinoudakis, C., and De Capitani di Vimercati, S. (Eds.), *Digital privacy: Theory, technologies, and practices* (pp. 363 – 380). Boca Raton, FL: Auerbach Publishers.

Bada, M., & Sasse, A. (2014). Cyber security awareness campaigns: Why do they fail to change behaviour? *Global Cyber Security Capacity Centre, University of Oxford: Oxford, UK.* Retrieved from http://discovery.ucl.ac.uk/1468954

Bennett, C. J., & Parsons, C. (2013). Privacy and surveillance: The multidisciplinary literature on the capture, use, and disclosure of personal information in cyberspace. In Dutton, W. H. (ed.), *The Oxford handbook of internet studies* (pp. 486 – 508). Oxford: Oxford University Press.

Blumer H. (1954). What is wrong with social theory? *American Sociological Review, 19*(1), 3 – 10.

Clark, D., Berson, T., & Lin, H. S. (Eds.) (2014). *At the nexus of cybersecurity and public policy*. Computer Science and Telecommunications Board, National Research Council, Washington DC: The National Academies Press.

Coleman, G. (2014). *Hacker, hoaxer, whistleblower, spy: the many faces of Anonymous*. London: Verso.

Cook, A. (2014). Personal communication via email, 23 June 2014. Alastair Cook permitted me to paraphrase his comments at a workshop on 19 June 2014.

Dutton, W. H. (2009). The fifth estate emerging through the network of networks. *Prometheus, 27*(1), 1 – 15.

Lawson, S. T., et al. (2016). The cyber-doom effect: The impact of fear appeals in the US cyber security debate. *In Cyber Conflict (CyCon), 2016 8th International Conference on* (pp. 65 – 80). IEEE.

Naisbitt, J. (2006). *Mindset!* New York: Harper Collins.

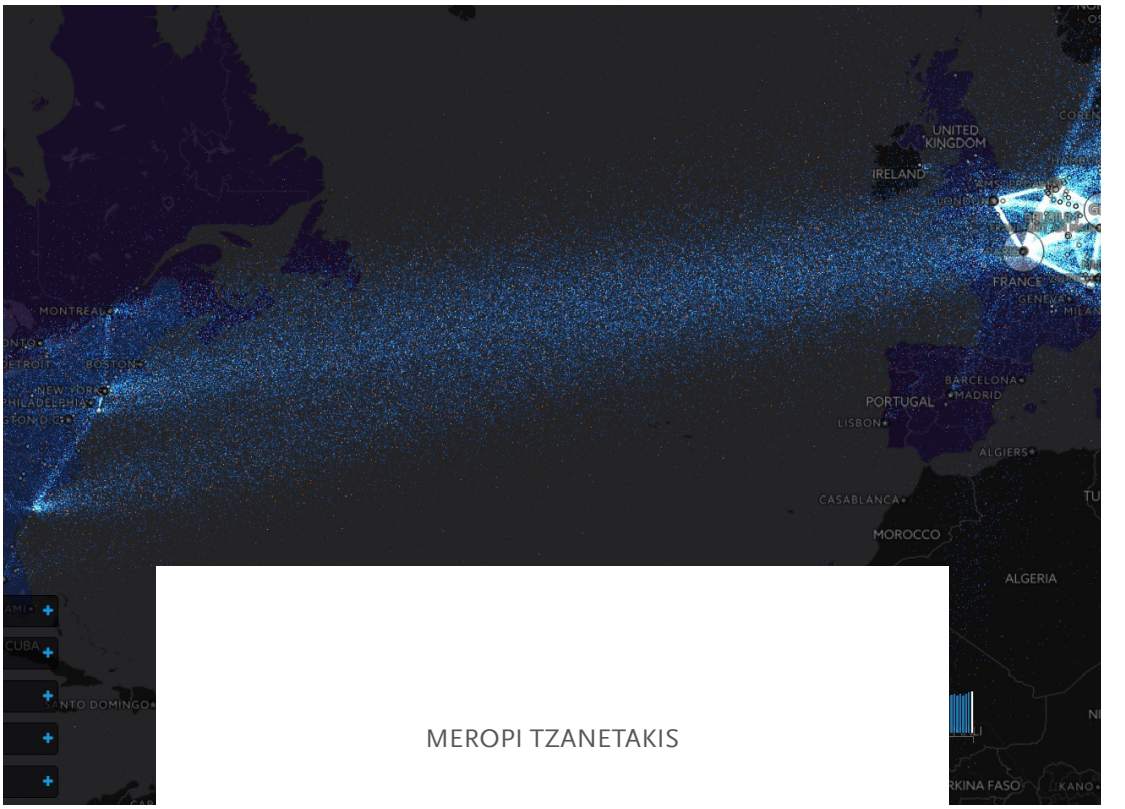
Nurse, J.R.C., Creese, S., Goldsmith, M., & Lamberts, K. (2011). 'Guidelines for usable cybersecurity: Past and present', in The 3rd International Workshop on Cyberspace Safety and Security (CSS 2011) at The 5th International Conference on Network and System Security (NSS 2011), Milan, Italy, 6 – 8 September.

Rice, R. E., & Atkin, C. K. (Eds.) (2013). *Public communication campaigns*, 4th edition. Los Angeles, CA: Sage.

Shillair, R., Cotten, S. R., Tsai, H. S., Alhabash, S., Larose, R., & Rifon, N. J. (2015). Online safety begins with you and me : Convincing internet users to protect themselves. *Computers in Human Behavior, 48,* 199 – 207.

Whitty, M. T., & Buchanan, T. (2012). The online dating romance scam: a serious crime. *CyberPsychology, Behavior, and Social Networking, 15*(3), 181 – 183.

Whitty, M., Doodson, J., Creese, S., & Hodges, D. (2015). Individual differences in cyber security behaviours: An examination of who's sharing passwords. *Cyberpsychology, Behavior, and Social Networking, 18*(1): 3 – 7.



MEROPI TZANETAKIS

The darknet's anonymity dilemma

The darknet is not just a place for criminalised activities; it facilitates anonymous communication between all those adopting marginalised positions, including human rights activists, dissidents and whistleblowers. They show that our society must face the dilemma between freedom and control.

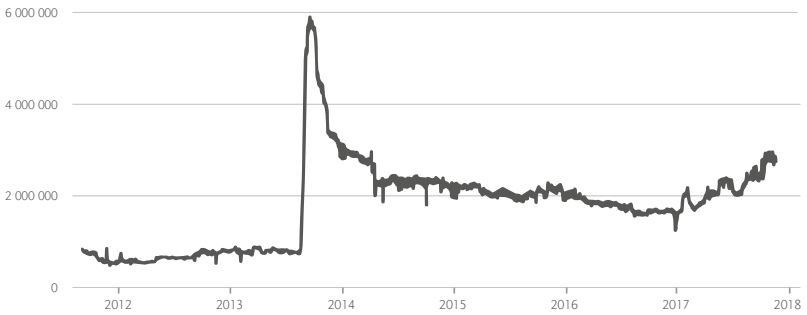
The darknet has a somewhat mystical, criminal and threatening aura about it. The prefix *dark* alone evokes these associations. These are only reinforced by reports on the weapons and drugs trade on the darknet. The public at large became aware of the existence of the darknet, when it became known that the Munich shooter had acquired his weapon in a darknet shop. The media coverage of drug shops on the darknet, principally *Silk Road* and the *AlphaBay* platform that closed in July 2017, also supported the thesis that the darknet was intrinsically a place of evil that should and must be surveilled and regulated.

In contrast, my article seeks to do two things. First, I would like to explain what lies behind the term darknet. By sharpening our understanding of the term, I would like to help demystify the darknet. Second, I would like to discuss a fundamental dilemma associated with the darknet as a place both for criminalised activities and freedom of expression. Finding a way to deal with this seemingly irresolvable contradiction between power and freedom should, in my opinion, be part of a broader societal process of negotiation. It is to this process that I wish to contribute with this article.

WHAT LURKS UNDER THE SURFACE OF THE INTERNET?

The internet consists of the *surface web* and the *deep web*; the darknet is a small part of the deep web (Bergman, 2001). In short, the darknet is a part of the internet where users can communicate almost completely anonymously. While content that can be captured by conventional search engines is referred to as the surface web, the deep web consists of websites that cannot be accessed and indexed by these same search engines. The deep web includes databases or content that is only accessible after a login or payment and that requires a password or a membership registration. Described in imagistic terms, the surface web is the visible tip of an iceberg, the underwater component of which, the deep web, is likely multiple times larger. Although its design makes its size almost impossible to quantify, the deep web is believed to be growing exponentially (Weimann, 2016). As part of the deep web, the darknet contains *hidden internet services*, i.e. hidden services that can only be accessed with special software such as TOR (The Onion Router) or I2P (Invisible Internet Project). TOR is based on a network of servers, in which requests are encrypted and routed over three randomly selected servers, so that communication within the network is almost impossible to

trace back to the source. The identities and locations of the approximately 2 million users worldwide (see Figure below) are thus concealed, unlike in the surface web. Hence, the term darknet does not say anything about its content's legal status, but only about how these services can be accessed.



Estimated number of users of TOR between 2012 and 2017, the rapid increase in TOR usage in 2013 is attributed to a botnet (The Tor Project, https://metrics.torproject.org)

WHAT CAN YOU FIND ON THE DARKNET?

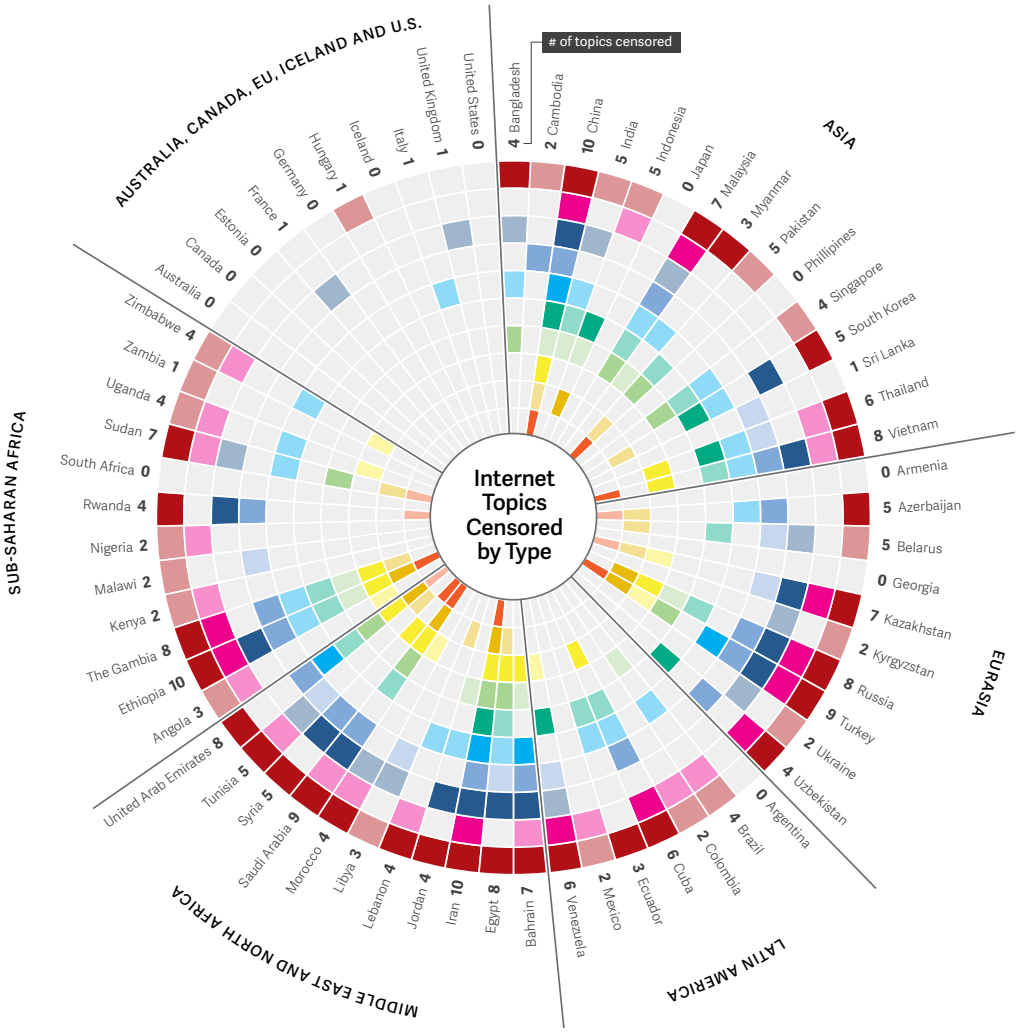
Contrary to the popular belief outlined at the outset of this article, two exploratory studies show that neither weapons nor drugs are of primary importance in the darknet. A British study of 13,600 pages on the TOR network calculated that 52 % of the contents could be classified as legal under UK or US law (Intelliag, 2016). Of all analysed sites, 29 % are file-sharing services, followed by 28 % consisting of leaked data and 12 % relating to financial fraud. Only 4 % of the websites surveyed sold drugs and only 0.3 % are related to weapons. A similar conclusion was reached by researchers from King's College, who evaluated 2,723 websites from the TOR network. 43 % of the contents of these pages were classified as legitimate (Moore & Rid, 2016). Of the remaining illegal offers, 15 % related to drugs, 12 % to finance, 7 % to other illegal content and 1.5 % to weapons. Unfortunately, the detailed results of the two studies are not directly comparable, since the former refers to all analysed TOR pages, while the latter only provides detailed listings for the contents classified as illegal. Despite their relatively small sample sizes, both studies illustrate the relationship between legal and illegal offerings on the darknet and the secondary importance of drugs and weapons. The visualisations on page 118 additionally illustrate the TOR network's data streams.

continue reading on page 123 ▸▸

THIS IS AN ARTICLE BY **MEROPI TZANETAKIS**

This article was first published on 10 March 2017 on the Science Blog of Alexander von Humboldt Institute for Internet and Society (HIIG).

Meropi Tzanetakis is a postdoctoral fellow at the University of Vienna. Meropi currently holds an Erwin Schrödinger Fellowship by the Austrian Science Fund (Marie Skłodowska-Curie Action). From 2016 to 2017 Meropi was a visiting researcher at HIIG. Meropi holds a PhD in Political Science from the University of Vienna. Her research interests are at the intersection of drug markets, digital technologies and public policy. Meropi is especially interested in approaching these areas from an interdisciplinary perspective, and in particular from the fields of political science, sociology and criminology. She is editor of Drugs, Darknet and Organised Crime (Nomos publishing house, forthcoming).



CENSORED TOPICS BY COUNTRY

Censorship was reflected if state authorities blocked or ordered the removal of content, or detained or fined users for posting content on the topics considered. The chart does not consider extralegal pressures such as violence, self-censorship, or cyberattacks, even where the state is believed to be responsible.

FREEDOM ON THE NET 2016 – REPORT BY FREEDOM HOUSE

	Widespread, ongoing, or repeated censorship	Sporadic or limited censorship
Criticism of Authorities		
Corruption		
Conflict		
Political Opposition		
Satire		
Social Commentary		
Blasphemy		
Mobilization for Public Causes		
LGBTI Issues		
Ethnic and Religious Minorities		

THE DILEMMA OF POWER AND DIGITAL FREEDOM

These empirical findings on the darknet lead me to this article's second concern. In addition to an anonymous bartering of legal and illegal goods and services, including drugs, weapons, counterfeit money, credit card data, counterfeit ID cards, malware and paedophilic content, the darknet's hidden services also offer communication that facilitates freedom of expression. The particular value of the darknet is that it guarantees a high level of security and privacy. And this is of special relevance after the Snowden revelations about cross-border mass surveillance practices and data protection violations. The darknet can also be used to circumvent state censorship by repressive governments. At the same time, the TOR network can be used by terrorists for communication. Yet the darknet is also used by human rights activists, journalists and dissidents to draw attention to corruption, oppression and other abuses. During the Arab Spring, for example, activists used the TOR network to exchange information, to commiserate about state persecution and, above all, to remain anonymous (Howard & Hussain, 2013). By using the darknet, people can express their opinions freely without revealing their identity and location.

The darknet can be understood as a virtual field that has thus far escaped total state and private control. This state of affairs is, incidentally, reminiscent of the early phase of the surface web in the 1990s. But it is precisely these limited options for monitoring and control that expose the darknet's dilemma. By guaranteeing anonymity, it provides the technological basis for safeguarding both civil liberties and the criminal activities that run counter to society's legal and moral norms as well as its broader values. On the darknet, power (Gehl, 2016), understood here as surveillance practices, traceability, algorithmic regulation and the limitation of the system's architecture go hand in hand with the right to freedom of expression, which is a fundamental right and an important component of democracy. The dilemma entailed by this co-occurrence is that an increase in surveillance power is associated with a decrease in freedom of expression and vice versa.

ON THE TRADE-OFF BETWEEN CONTROL AND FREEDOM OF EXPRESSION

More monitoring and control of criminalised activities and an associated increase in subjective security also means less freedom of expression and privacy. This is reflected, for instance, in the increasing restrictions on freedom of expression on the surface and deep web (Freedom House, 2016). As can be seen in the chart on the left, issues such as criticism of state authorities, corruption, ongoing conflicts and terrorism,

political opposition, but also satire are censored in 52 states all over the world. This can be explained by the fact that norms and values are not fixed social facts, but are anchored in a social context that varies based on the place, jurisdiction of a state and time (Henecka, 2015). The example of the drug markets on the darknet illustrates that this good-evil binary cannot be maintained in this case. Although legal and illegal drugs are globally available on anonymous markets, they provide consumers with the opportunity to find out in advance about the qualities and effects of the substances for the first time. In addition, customers report less violence than when buying from friends, acquaintances or on the street (Barratt, Ferris & Winstock, 2016). Thus, even if they do not do so legally, drug markets on the darknet nevertheless contribute to reducing the risks and health consequences of drug use (Tzanetakis & von Laufenberg, 2016). This complexity deserves particular consideration when calls for bans on anonymisation services are raised in light of recent events. The question thus has less to do with darknet technologies or the technical implementation possibilities, but rather of what values and standards we wish to apply when using them, as well as how and for what purposes.

Finally, it is also a question of negotiating how much freedom we are prepared to give up for more subjective security. Different people, groups and institutions evaluate these questions differently depending on their interests. But it is precisely here where the political challenge lies, in my opinion; it is the challenge of ensuring that diverse interest groups and associations can participate in the societal negotiation process and thus have a say in deciding where democratic societies are going. ◆

REFERENCES

Barratt, M.J., Ferris, J., & Winstock, A. (2016). Safer scoring? Cryptomarkets, social supply and drug market violence. *International Journal of Drug Policy, 35*, 24 – 31.

Bergman, M.K. (2001). White Paper: The Deep Web: Surfacing Hidden Value. *Journal of Electronic Publishing, 7*(1).

Freedom House (2016, November). *Freedom on the Net 2016.* Retrieved from https://freedomhouse.org/sites/default/files/FOTN_2016_BOOKLET_FINAL.pdf

Gehl, R.W. (2016). Power/Freedom on the Dark Web: A Digital Ethnography of the Dark Web Social Network. *New Media and Society, 18*(7),1219 – 1235.

Henecka, H.P. (2015). *Grundkurs Soziologie*, 10th ed., Konstanz: UVK.

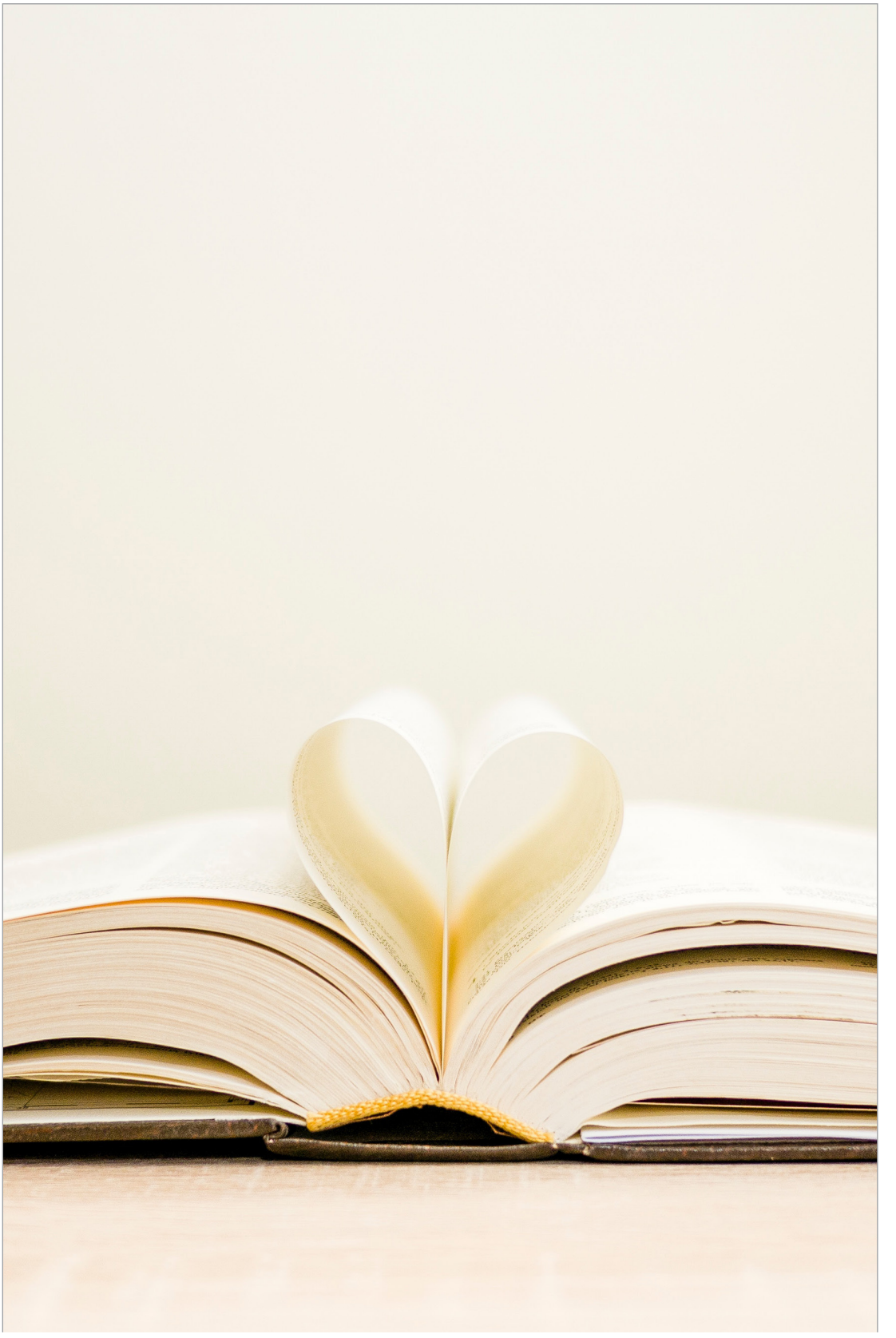
Howard, P.N., & Hussain, M.M. (2013). *Democracy's Fourth Wave? Digital Media and the Arab Spring.* New York: Oxford University Press.

Intelliag (2016). *Deeplight: shining a light on the Dark Web*. Retrieved from http://deeplight.intelliagg.com/deeplight.pdf

Moore, D., & Rid, T. (2016). Cryptopolitik and the Darknet. *Survival, 57*(1), 7 – 38.

Tzanetakis, M., & von Laufenberg, R. (2016). Harm Reduction durch anonyme Drogenmärkte und Diskussionsforen im Internet? In akzept e.V. Bundesverband (Ed.), *Alternativer Drogen- und Suchtbericht 2016, 3* (pp. 189 – 194). Lengerich: Pabst Science Publishers.

Weimann, G. (2016). Going Dark: Terrorism on the Dark Web. *Studies in Conflict & Terrorism, 39*(3), 195 – 206.



encore

Volume 2017
Published January 2018

PUBLISHER

Alexander von Humboldt Institute for Internet and Society
Französische Str. 9
10117 Berlin

EDITORIAL TEAM

Julia Ebert, Kirsten Gollatz, Jeanette Hofmann,
Rebecca Kahn, Florian Lüdtke, Christian Pentzold,
Jörg Pohle, Jessica Schmeiss, Larissa Wunderlich

DESIGN

Larissa Wunderlich

CREDITS

Photo on cover by complize / photocase.de
Photo p. 34 by Nikola Kuzmanic
Photo p. 70 by Axel Schmidt

Alexander von Humboldt
INSTITUTE FOR INTERNET
AND SOCIETY

Alexander von Humboldt
INSTITUTE FOR INTERNET
AND SOCIETY