INTERNET POLICY REVIEW

Five Year Anniversary Booklet

Internet Policy Review – 2013 - 2018 – Five year anniversary booklet

Electronic version of the booklet produced for the anniversary event held at HIIG Berlin on 4.9.2018.

This booklet was put together by the *Internet Policy Review* editorial team,
in collaboration with *Internet Policy Review* contributors.

Illustration: Kati Szilagyi
[http://katiszi.com/]

Design: Internet Policy Review Team
with visual elements from Olivier Guillard / The World We Live In
[https://www.theworldwelivein.co.uk/]

Photo p. 10: CC-BY 4.0, Branka Pavlovic

ISSN: 2197-6775

Alexander von Humboldt Institute for Internet and Society gGmbH
Französische Straße 9
10117 Berlin Germany

Represented by:
Prof. Dr. Jeanette Hofmann | Prof. Dr. Dr. Ingolf Pernice | Prof. Dr. Björn Scheuermann
Prof. Dr. Dr. Thomas Schildhauer | Prof. Dr. Wolfgang Schulz | Dr. Karina Preiss
Tel: +49 30 2007 6082 | Fax: +49 30 2060 8960 E-Mail: info@hiig.de

Responsible for content according to § 55 paragraph 2 RStV: Dr. Karina Preiss

---

published by:

Alexander von Humboldt
Institute for Internet
and Society

in cooperation with:

Institut des sciences de la communication
CNRS/PARIS SORBONNE/UPMC

CREATe

R&I IN3 Internet interdisciplinary Institute
Universitat Oberta de Catalunya

Contents

Foreword

Jeanette Hofmann
Member of the Managing board, *Internet Policy Review*
Director, *Humboldt Institute for Internet and Society*
@achdujeh

European Internet policy and regulation deserves an interdisciplinary journal. That much we knew already in the early days of planning the Humboldt Institute for Internet and Society (HIIG, Berlin). I remember a meeting at the HIIG's opening conference in 2011 where we tossed around ideas about what a new type of journal could look like. As all of those who have been involved from the beginning can testify, there's been a lot of water under the bridge since.

The innovator's dream is, of course, to do away with many of the restrictions that constitute a well-established object such as the academic journal. Open access was among the most obvious features we had in mind. We also hoped to be able to position *Internet Policy Review* as a discursive space between academia, practitioners and regulators, i.e., as a building block towards a European perspective on the internet. Alas, as all innovators figure out sooner or later, change requires careful dosing. Hence, today *Internet Policy Review* may look more academic than in its infancy but all the adjustments we made have been rewarded with a loyal and growing readership.

Today's personality of *Internet Policy Review* came about with its second generation website, which offers, along with the research papers, curated op-eds and news articles. Factoring in also the Twitter activities, the journal has established itself as a respected node in the conversation on internet policy in, but also beyond Europe.

The managing board and editorial team in their current forms, have existed since 2016. Its membership reflects the network of research centres in Barcelona, Berlin, Glasgow and Paris who have joined in as publishing partners over the last five years. All of these researchers, plus a devoted team of information law scholars in Amsterdam have helped developing the journal both in terms of substance and strategy. I am very grateful but also proud of this collaboration across disciplines, organisational cultures and countries. Independent of commercial publishers, we managed to establish a steady flow of high quality submissions and peer review.

More fundamentally, I would like to particularly salute the HIIG for its steadfast support of the journal. I would also like to extend a resounding thank you to the two major conferences, who have joined forces with Internet Policy Review for the publication of annual special issues.

However, nothing of this would have been possible without our managing editor Frédéric Dubois and his team, who run *Internet Policy Review* with unwavering passion and devotion. Probably without noticing it until it was too late, Frédéric has turned over the years into a somewhat reluctant academic himself.

There is still work ahead before *Internet Policy Review* can call itself fully durable, and we hope you will feel compelled to participate in that effort. But today, I am looking back at an impactful startup, with a well-crafted profile and a strong resonance in terms of citations, readers, and following. *Internet Policy Review* is there to stay.

Editorial

Frédéric Dubois
Managing Editor, *Internet Policy Review*
@fredericdubois

Five.

Five years.

Five years of publishing.

Five years of open access publishing.

Five years of open access publishing on internet research…

To me, starting up *Internet Policy Review* felt like writing a poem, collectively with a team of spirited editors. Then again, unlike the poet, and luckily I shall add, the editorial team was never free of conventions. Striking the right balance between *Gestaltung* (designing and crafting with room for manoeuvre) on the one hand, and academic and editorial traditions and conventions on the other, was and is for me the key for positioning the journal in the high standards / high quality category.

A journal in founding mode needs a spark. And that spark was Uta Meier-Hahn, my accomplice in the early days. Without her dedication, curious mind and her eye for details that matter, the generalist editor that I am, would have never been able to lay the sound editorial foundation of IPR - as we refer to the journal internally. From there on, we were able to draw in editors of excellence, starting with Francesca Musiani, Kristofer Erickson, Balázs Bodó, Joris van Hoboken and more recently, Montserrat Batet. They are the real story behind *Internet Policy Review*. They are the guardians of quality who year after year, have kept our lean and transparent peer reviews constructive, integrous, and precise.

I am also particularly indebted towards Christian Katzenbach, Paul Gebelein, but also Patrick Urs Riechert and Helene von Schwichow, who have injected fresh ideas, organisational talent and technical skill in decisive moments.

Crafting a journal with personality today, not only means publishing quality re-

search, but also the ability to find and listen to internet-related discussions. We have tried to do that by reaching out to audiences in online social networks, at conferences, but more importantly, allowing emerging scholars, senior researchers and practitioners alike, to participate in our journal. Our live-tweeting at events, the open abstract feature, and cooperation with international conferences AoIR and IAMCR on special issues were all meant to foster engagement in our journal.

I feel thankful to the publishing institute HIIG and its European partners for entrusting the editors with the freedom to innovate, and for allowing the journal to meet its diverse audience of internet scholars and policy practitioners.

Merci to all Managing and Editorial board members!

And yes, thanks to you dear **authors**, reviewers, readers and other allies.

Internet Policy Review's coming of age leaves us today with a journal who's authorship is diverse both regionally and in terms of academic disciplines. For this booklet, we only selected three of the most outstanding contributions: 1) an empirical article on filter bubbles by University of Amsterdam information law researchers Zuiderveen Borgesius et al.; 2) a paper looking at early internet design (1969-1979) and its implications for policy, by Sandra Braman and; a 2018 scholarly essay that interrogates discourses associated with encryption, by Sarah Myers West.

Enjoy the read!

Yours sincerely,

Frédéric Dubois

Internet policy politics

Q&A

Marianne Franklin

Professor of Global Media & Politics,
Goldsmiths, University of London
@GloComm

Marianne, you have been following the work of *Internet Policy Review* since the very beginning. Back in 2012, internet governance was a key notion. Does *internet governance* still mean anything today?

MF

The short answer is yes, more than ever.

The longer one is; depends what we mean by this term. Over the last decade, at least, the issues that fall under the rubric *internet governance* have multiplied with all kinds of analytical and practical implications - legal, technical, ethical, sociocultural, economic and political. The internet's design as a "network of [computer] networks" has also become increasingly complex technologically, which implies that the complexity of the legal, sociocultural, economic and political dimensions of internet design, access, use, and content management need to be embraced, rather than explained away. *Internet governance* used to be a descriptor, stemming from a stricter, engineering understanding of technical standards and network architectures that appear far removed from 'normative' issues such as rights, freedom, democracy and the like. In 2018, maintaining that this sort of narrow techno-centric definition is the only one possible would be avoiding the many issues we all face – as users, designers, policy-makers, academics, or activists for whom the internet is both an object and a means to achieve certain goals.

This is not to deny, or belittle the role that technical experts have played in shaping the way that the internet works. But as technologies are never neutral, nor immutable, the need to address the sociocultural and political

implications of transformative technologies such as the internet, given how many people take being online for granted, is even more pressing today. In the last few years the stakes have also been raised geopolitically and within national polities. This means that technical experts, scholars, political representatives, and activists need to both sharpen their focus whilst bearing in mind the broader context of any emerging design, terms of access, and use, and how content – databases – are being managed, and for whom. These are exciting and challenging times in that regard because finding a focus, and keeping focused, whilst not being blind to the rest is not an easy task. But as demanding as this may be, it needs to be a core premise for theory and research, public policy advocacy, and activism that are currently addressing the spectrum of internet governance topics; for established and emerging scholars and for journals that focus on the internet like *Internet Policy Review*.

Your specialty in internet governance is human rights. What are we looking at exactly?

MF

Simply put, human rights with regards to internet communications and architecture are more than social and economic rights. They are more than the narrowly defined set of rights stemming from the US civil liberties and the American constitution (that enshrine free speech for instance). I think we need to be more, not less ambitious in this regard and consider the ways in which internet design, terms of access and use implicate international human rights law and norms as a whole, not only those that have been currently 'cherry-picked' so to speak. In addition, human rights law and norms, as western liberal institutions, are not beyond criticism either. I do not see human rights as religious tenets for they are also products of human history, quite recent history as it happens. Nonetheless the term encompasses three, if not four 'generations' of rights anchored in the UN system, which span from the Universal Declaration of Human Rights and those treaties and covenants that are derived directly from the UDHR such as the ICCPR, the ICESCR, or the ECHR to those on the rights of women, of indigenous peoples, persons with disabilities, and those of children.

In Western countries and Europe in particular, we've been dealing with the right to privacy online, particularly since the Snowden revelations in 2013 and subsequent events. This discussion is far from over, as jurisprudence has only really started to emerge in recent years. But privacy is but one right among many others and, moreover, it is one of the more controversial ones from a sociocultural perspective. Whilst Privacy, along with Freedom of Expression, and Freedom of the Press are well-developed areas for debate and action, they are the tip of the human rights-internet iceberg, a beginning not an end to the matter. Take for example, the work being done on raising awareness of the gendered dimensions to even these fundamental rights and freedoms and their impact on internet policy-making, how these overlap advocacy platforms that address the way in which women's rights online (in terms of access, and freedom of association, and of information) are yet to be fully realised in many parts of the world. Existing and emerging rights (some argue that internet-access should be a new right) are already being reshaped in the face of how emerging technologies (the Internet of Things, artificial intelligence etc.), internet-dependent government services, and commercial mobile phone apps are changing the way in which people interact with the world around them. Looking ahead, moreover, to think about the connections between human rights and the internet across the spectrum and how much work there is still to do, we need to consider the role that education can play. By this I mean critical thinking, daring to ask questions and query the norm, not learning by rote.

Education, as a dialogue, in this regard is crucial because online and offline, internet-based practices and infrastructures based on data-tracking (viz. surveillance), not privacy or other rights and freedoms, have become normalised across Europe and around the world. The extrajudicial programmes of mass online surveillance about which Snowden called the world to attention have now become enshrined in law, from the UK to Germany, the Netherlands, France, and in the Global South as well. I'm deeply concerned about the continued assumption that accessing and using internet media and communications services have to be based on large-scale forms of data-retention, and the automated 24/7 tracking of our digital imaginations, and footprints, by both state agencies and companies (from tech giants to start-ups). These practices are political and commercial decisions, not a technical imperative. In Germany, France, the UK, we may now have privacy acts of some sort or another but all these regulations can be mitigated, if

not circumvented by intelligence services, and law enforcement agencies. Just because something is technically possible, even commercially attractive, that does not necessarily mean that it is either justifiable or desirable.

It is only along with, and through education (e.g., through teaching people how to use crypto-tools, or getting them to question their habits) that we can combat this incipient passivity towards this emergence of surveillance as the norm, rather than an exception.

What role can researchers play in addressing the challenges in internet governance?

MF

I would like to see internet policy and governance research open up to other disciplinary approaches, e.g., digital cultures, feminist studies, philosophy, anthropology (being online is, after all, a cultural practice). Many scholars, of digital cultures for instance, would not consider their work as internet governance, strictly speaking. Yet these research agendas and theoretical approaches, along with those from philosophers and historians of technology, have been looking at human-machine interactions long before internet governance became a recognisable, arguably trendy domain. Besides, to speak of 'governance' often elides questions about the exercising of deep power – I have written quite extensively on the need to more thoroughly theorise, rather than describe how power is exercised, and pushed back against through digital, networked domains. We need to beware of fetishising the technical in this domain; the web continues to be a space in which enormous amounts of content – meaning-makings – circulate, including relationships, art and culture such as music, communities in which ideas and identities are forged. For these reasons, internet governance as a scholarly but also policy-making rubric needs to be anchored in multidisciplinary forms of inquiry and action. It is too important to be left to the experts, or become 'parked' in one corner of academe in other words.

So I guess my answer to your question is: let's not get entangled in a

standoff between disciplines or one between academic cultures (e.g., Anglo-American and European traditions as, *ipso facto*, superior to those from other, non-Western traditions). Whilst it is too important to leave it up to experts – technical or legal – this does not mean we should ignore such experts; quite the contrary. If the internet, broadly defined, is a technology of interconnections then so too should the way we study, write, and mobilise around internet governance be interconnected, cross-disciplinary. As these very terms of reference are transforming in the wake of R&D, and now policy agendas are looking to promote artificial intelligence, biotechnologies, nano-technologies, and design innovations such as blockchain technologies, we may also well along the way in a shift in the very experience of what it means to function as community, act and feel as a human being at the online-offline nexus. In that regard, philosophers, including feminist scholars, have been considering these intimacies between humans and machines for some time, and not always in simplistic, pessimistic terms. Which leaves me with one thought: is there the possibility that some consideration might be needed to whether there should be a 'right' not to *have* to go online?

Quality control on a high level is the key

Q&A

Christina Riesenweber

Open Access Officer, *Freie Universität Berlin*
@c_riesen

Christina, you've been an editor at an open access journal yourself and are now spearheading open access at Freie Universität Berlin. We have a candid and naive question for you: what does open access mean in 2018?

CR

I think that in 2018 it is pretty obvious that we're not discussing whether open access is the way to go, but rather how we can ensure that easy, affordable, large scale open access publication happens. When I say easy, I mean easy for authors to submit, read and share open access research and for administrations to manage it. Open access today means making sure that services of high quality publication are well priced and paid for, and still remain realistic when compared to actual budgets of research institutions. In 2018, the main question regarding open access is: how and by whom is it being paid for?

The other remaining challenge is knowledge dissemination about open access. But we've already come a long way.

How would you qualify the open access model of *Internet Policy Review*?

CR

When we discuss the financial aspect of open access, we usually talk a lot about article processing charges (APCs). But three quarters of all

open access journals operate *without* APCs. Many of these are independent journals without a big publisher backing them. APCs are only suitable for certain disciplines and for researchers who have access to resources to cover APCs.

Internet Policy Review makes a true contribution to open access, in terms of experimentation, as in the larger picture, we need a bibliodiversity of publications. It is therefore not simply a drop in the open access ocean. As there are no well defined categories, it's hard to qualify *Internet Policy Review*. But, in the no-APC segment, the journal would probably end up in a category I would call precarious.

That sounds about right. But what exactly do you mean?

CR

It seems that *Internet Policy Review* is dependent on the goodwill of research institutions. There is no steady flow of income outside the publishing institutions. One could argue, there is insecurity *vis-à-vis* the future. But I see an advantage over other journals of the same make: the backbone of the journal is ensured by a paid position, that of the Managing editor. This lends the journal some level of stability.

Also, the fact that you use the Creative Commons license CC-BY puts you into the category of "very open" journals - because openness is not binary, but comes on a scale. In the early 2000s, with the Budapest open access initiative and the Berlin declaration, the open access movement advocated not only to enable researchers to write and read, but also to reuse research publications. That was a major stepping stone in the history of open access publications. Researchers, educators, and practitioners don't have to think twice about how to reuse papers in *Internet Policy Review*.

Zooming out, where are we at in terms of open access publishing in Europe right now?

Three things are happening: one is that Germany is negotiating publication deals with three major publishers. This will be decisive for the rest of Europe. Germany is an important research and publication location. So what will come out of these negotiations has the power to influence other European academic hubs.

CR

If a large-scale agreement is possible, that would be a precedent.

Secondly, we clearly see something that wasn't there five years ago: open access is now framed as part of the open science idea. Publication is opening up, but so are other elements of the research life-cycle. You can see this in other European countries and at the European Commission level, for example with the advent of the Open Science Monitor. Thus, open access is not a stand-alone feature anymore, but ties in with other elements of openness, like open research data or open research software.

Third, very recently something important happened. The European Commission decided that is was not going to fund hybrid open access anymore. This is a big step! In some closed subscription journals, authors can pay a fee to make their published article freely available online. The German research council DFG never supported this, but in the UK for example, this was supported. The European Commission realised that this model does not contribute to a large scale transformation to open access and therefore decided to stop funding hybrid open access.

In the larger picture, Europe does have a say when it comes to the publishing landscape. With Elsevier in the Netherlands, Springer in Germany, and many established research centres, Europe's embrace of open access will most certainly influence other jurisdictions. In the US, the Gates Foundation and the National Institutes of Health (NIH), just to mention two important research players, are supporting open access.

With the advent and multiplication of research platforms such as ResearchGate & co, do you continue believing in the chances of small journals to survive?

Every publishing service that can perform academic quality control on a high level, contributes towards making research better. Every service that does that stands a chance to survive. ResearchGate and Academia.edu have no quality control of their own, but are social networks. I wouldn't have predicted the downfall of MySpace either, so I don't want to speculate about the future of ResearchGate & co.

CR

In terms of where there is potential for growth, all kinds of meta services will play a very important role in the future. You see major publishers engaging in science monitoring, research information, science metrics, etc. This trend to making research more visible and quantifiable emerged lately, and there is money to be made. So we will likely see some companies' portfolios change in the future. Whether this affects small publishers and independent publications adversely or not is hard to guess. In any case, the future of academic publishing will be exciting and hold a lot of surprises, I'm sure.

So what about new open access journals?

Teams behind independent journals often overestimate the need for a new journal. Often also, there is not enough technological and librarian knowledge to actually establish a journal successfully and make it visible enough on the gigantic internet. It seems that this does not apply to *Internet Policy Review* though - you picked a very good spot and found your audience. In my view, however, the pioneer phase is over. We don't so much need new journals as rather the existing ones to transform to open access.

CR

> Just done first ever completely open review for @PolicyR. Great process - everyone knows who everyone is (authors, all reviewers). Google docs used to comment in line and provide overall comment as well.
> Thought-provoking on how there are different ways to do things.

– Nick Anstead
(Associate Professor, *London School of Economics and Political Science*)

> Believe me, I have never had to stand such an obnoxious group of reviewers in my entire academic life ;-P (this is a thanks—in convoluted form, but a thanks for the careful reading and the great suggestions for improvement…)

– Stefania Milan
(Professor, *University of Amsterdam*)

> Long live @PolicyR ! Happy and proud to have been there from the beginning to contribute making it what it is today :)

– Francesca Musiani
(Researcher, *French National Centre for Scientific Research*)

VOLUME **5**
ISSUE **1**
doi:**10.14763/2016.1.401**

RESEARCH ARTICLE

Should we worry about filter bubbles?

Frederik J. Zuiderveen Borgesius – *University of Amsterdam*
Damian Trilling – *University of Amsterdam*
Judith Möller – *University of Amsterdam*
Balázs Bodó – *University of Amsterdam*
Claes H. de Vreese – *University of Amsterdam*
Natali Helberger – *University of Amsterdam*

KEYWORDS: Filter bubble, Personalisation, Selective exposure.

ABSTRACT: Some fear that personalised communication can lead to information cocoons or filter bubbles. For instance, a personalised news website could give more prominence to conservative or liberal media items, based on the (assumed) political interests of the user. As a result, users may encounter only a limited range of political ideas. We synthesise empirical research on the extent and effects of self-selected personalisation, where people actively choose which content they receive, and pre-selected personalisation, where algorithms personalise content for users without any deliberate user choice. We conclude that at present there is little empirical evidence that warrants any worries about filter bubbles.

RECEIVED : 06 10 2015 ACCEPTED : 15 02 2016
PUBLISHED: 31 03 2016

1. INTRODUCTION

Media content is becoming increasingly personalised. Before the advent of digital media, news outlets generally featured exactly the same content for all users. Now, in theory, the same news website can show each visitor personalised content. Such personalisation has led to worries about filter bubbles and selective exposure: personalised content and services could limit the diversity of media content people are exposed to and thus have an adverse effect on the democratic discourse, open-mindedness and a healthy public sphere (e.g., Pariser, 2011; Sunstein, 2002). For instance, the High Level Expert Group on Media Diversity and Pluralism, an independent group advising the European Commission, warned for the impact of personalised communication on our democratic society:

> Increasing filtering mechanisms make it more likely for people to only get news on subjects they are interested in, and with the perspective they identify with. There are benefits in empowering individuals to choose what information they want to obtain, and by whom. But there are also risks. This new reality will decrease the role of media as editors and interpreters of information. It will also tend to create more insulated communities as isolated subsets within the overall public sphere. (…) Such developments undoubtedly have a potentially negative impact on democracy. (Vīķe-Freiberga, Däubler-Gmelin, Hammersley, & Pessoa Maduro, 2013, p. 27)

A dire warning, but is it true? How personalised are online news media today? What are the effects of personalised media on media exposure and the information choices people make? Even harder questions concern the long-term effects of personalisation. Does personalised content really influence consumers, newsreaders, citizens, and voters in a negative manner? Are concerns about filter bubbles supported by empirical evidence?

To address these questions, we provide an overview of concerns that have dominated the public information policy discourse, and review the main insights from empirical research. For this paper, personalisation is described as the phenomenon that media content is not the same for every user, but tailored to different groups or individuals.

In Section 2, we introduce the notion of personalisation, and distinguish self-selected personalisation from pre-selected personalisation. In Section 3, a brief overview is given of the main concerns about filter bubbles in current public policy discourse, based on a review of policy documents. Then, we review empirical evidence of the prevalence (Section 4) and effects (Section 5) of personalised communication.

2. SELF-SELECTED AND PRE-SELECTED PERSONALISED COMMUNICATION

In his book *Being Digital*, Negroponte (1995) discussed the idea of the 'daily me'. He suggested that people would soon be able to choose their own personalised media experiences:

> "Imagine a future in which your interface agent can read every newswire and newspaper and catch every TV and radio broadcast on the planet, and then construct a personalized summary. This kind of newspaper is printed in an edition of one." (Negroponte, 1995, p. 153)

Others worry that people can lock themselves in information cocoons or echo chambers. For instance, somebody might read only left-leaning blogs and websites, listen only to left-leaning radio, and watch only left-leaning television. Pariser coined the term 'filter bubble', "a unique universe of information for each of us" (Pariser, 2011, p. 9). For example, a personalised news website could give more prominence to conservative media items, based on the inferred political interests of the user. When they form their political ideas, users of such personalised services may encounter fewer opinions or political arguments.

We distinguish between two main types of personalisation: *self-selected personalisation* and *pre-selected personalisation*. Others have used different terms to describe similar phenomena: For instance, self-selected personalisation could also be called 'explicit personalisation', and pre-selected personalisation could be called 'implicit personalisation' (Thurman & Schifferes 2012; see also Treiblmaier, Madlberger, Knotzer, & Pollach, 2004).

Self-selected personalisation concerns situations in which people *choose* to encounter like-minded opinions exclusively. For example, a person who opposes immigration might want to avoid information that specifies how much a country has gained due to immigration, while paying a lot of attention to news stories about problems related to immigration. People tend to avoid information that challenges their point of view, for example by avoiding news outlets that often feature editorials that favour an opposing political camp. In communication science, this phenomenon is conceptualised as *selective exposure* (e.g. Stroud, 2011).

Pre-selected personalisation concerns personalisation driven by websites, advertisers, or other actors, often *without* the user's deliberate choice, input, knowledge or consent. Concerns about pre-selected personalisation are often summarised with the term 'filter bubble' (Pariser, 2011).

Pre-selected personalisation may be chosen by the user, or not. For instance, some people may realise that Facebook personalises the content in its newsfeed. If these people explicitly use Facebook to see the curated, pre-selected collection of news about 'friends', the newsfeed is an example of chosen pre-selected personalisation. Other people, however, may not realise that the newsfeed on Facebook is personalised; those people do not explicitly choose pre-selected personalisation.

3. CONCERNS AROUND PERSONALISED COMMUNICATION

Below, we summarise the main concerns regarding personalisation that have been brought forward in policy and scholarly circles. We discuss the effects of personalisation on democracy, the role of new gatekeepers and influencers of public opinion, autonomy-related concerns, the lack of transparency around personalisation, and the possibilities for social sorting. Examining the privacy implications of the massive collection of user data that is often involved in personalisation lies beyond the scope of this paper (for privacy implications of personalised services, see Zuiderveen Borgesius, 2015).

EFFECTS ON DEMOCRACY

Many worry about the effects that personalised communication could have on democracy. When the High Level Expert Group on Media Diversity and Pluralism commented on personalisation strategies in the media, one of its main concerns was that people would encounter fewer opinions, which could have a negative effect on the public sphere and the democratic opinion forming process (Vīķe-Freiberga et al., 2013). In a similar vein, the Council of Europe (2012, Appendix, Section I, paragraph 2) warned that the ordering and ranking of information in the context of search engines can affect information access and the diversity of information people are exposed to.

The concerns of the Expert Group echo arguments made in the scholarly debate, including those by Sunstein (to whom the group refers) (Vīķe-Freiberga et al., 2013). Sunstein discusses risks of too much personalisation. He mainly addresses self-selected personalisation: people locking themselves in 'information cocoons', which he describes as "communication universes in which we hear only what we choose and only what comforts us and pleases us" (Sunstein 2006, p. 9). To give a current example: somebody might self-select personalisation by following people on Twitter who hold like-minded opinions.

Sunstein discusses two risks of personalisation. First, in a democratic society people need to come across opinions that differ from their own opinions, to develop themselves fully. Otherwise, people might enter a spiral of attitudinal reinforce-

ment and drift towards more extreme viewpoints (Sunstein 2002, p. 9). This is a point also shared by the Expert Group: "The concern is people forgetting that alternatives do exist and hence becoming encapsulated in rigid positions that may hinder consensus-building in society" (Vīķe-Freiberga et al., 2013, pp. 27-28). Sunstein warns that "unplanned, unanticipated encounters are central to democracy itself" (2002, p. 9).

Second, if people locked themselves in their own information cocoons, they might have fewer common experiences. Sunstein says a diverse democratic society needs shared experiences as 'social glue' (2002, p. 9). The Habermasian understanding of the public sphere, in which societally relevant ideas are formulated, negotiated and distributed, and in the process the ruling authorities' actions are kept under control and guided (Habermas, 1989), still serves as an important point of reference, despite the extensive critique this idea rightly received.

NEW GATEKEEPERS AND INFLUENCERS OF PUBLIC OPINION

In the public policy discourse, much attention is given to search engines, app stores, and social network sites as new gatekeepers and influencers of public opinion (see e.g., European Commission, 2013, p. 13; Vīķe-Freiberga et al., 2013). There is a long tradition in media law and policy of regulating gatekeeper control, because such control can threaten the realisation of important public policy goals, such as media diversity, public debate and competition on the marketplace of ideas.

However, the new information intermediaries, such as providers of search engines, social network sites, and app stores, differ in many respects from the more traditional gatekeeper categories, like the old press barons and controllers of content and infrastructure. One of the most important differences is the set of mechanisms used to exercise gatekeeping control which, in the case of the new intermediaries, are often related to interaction with users, the amount of knowledge and control they have over the user base, and exposure to diverse information (Helberger, Kleinen-von Königslöw, & Van der Noll, 2015).

An experiment in which Facebook persuaded its users to vote in the US election demonstrates the power of new opinion influencers well. The "results suggest that the Facebook social message increased turnout directly by about 60,000 voters and indirectly through social contagion by another 280,000 voters, for a total of 340,000 additional votes. That represents about 0.14% of the voting age population of about 236 million in 2010" (Bond, Fariss, Jones, Kramer, Marlow, Settle, & Fowler, 2012, p. 1). Because of the potential power of gatekeepers, various scholars call for meaningful transparency regarding their algorithms and their profiling

practices (Hildebrandt & Gutwirth, 2008; Pasquale, 2015; Bozdag, 2015).

AUTONOMY-RELATED CONCERNS

Personalised communication may also restrict people's autonomy, according to some authors (e.g. Zarsky 2002, p. 42). In brief, people's opinions might be steered by personalised media, while they are not aware of being influenced.

However, personalisation, at least self-selected personalisation, could also enhance people's autonomy, because people can express which content they wish to receive. In contrast, in the traditional mass media situation, the editor determines which content is presented in which form. In other words, personalisation strategies can also have an empowering effect on users. In fact, pre-selected personalisation can also be used to help users make more diverse choices (Helberger, 2011).

LACK OF TRANSPARENCY

Another prominent item on the media policy agenda is the lack of transparency regarding pre-selected personalisation. The lack of transparency could affect the way people respond to personalised messages (Vīķe-Freiberga et al., 2013), and could make it harder for regulators to monitor the media sector. If people do not realise they see pre-selected content, they might think they see the same content as everybody else.

The Council of Europe seems to suggest that transparency about the search algorithm can help to promote media diversity and information access, and help to mitigate the filter bubble risk (Council of Europe, 2012, paragraph 7 and Appendix, Section 1, paragraph 4). Transparency in itself may not promote diversity of supply and exposure, but transparency is a necessary, albeit insufficient condition to detect problems with diversity. It is also unclear whether information about the way search engines work can cause people to choose more diverse content or can help people to avoid being trapped in a filter bubble. However, transparency about personalisation is at least essential to inform the policy discussions.

SOCIAL SORTING

Topics that received little attention in the public policy discourse on personalised communication are social sorting and discriminatory practices. Scholars have paid more attention to these topics. Social sorting involves, in Lyon's words, "obtain[ing] personal and group data in order to classify people and populations according to varying criteria, to determine who should be targeted for special treatment, suspicion, eligibility, inclusion, access, and so on" (Lyon, 2003, p. 20). In particular,

profiling and classification in one domain (for example in advertising) may outgrow its original context and define other domains of our life (Turow, 2011). Social sorting, thus, "may further erode the tolerance and mutual dependence between diverse groups that enable a society to work" (Turow, 2011, p. 196).

CONCLUSION

In public policy and academic discourse, personalised communication is regarded with much concern. Much of the existing public policy discourse makes little reference to empirical evidence, leaving unclear to what extent concerns are justified, exaggerated, or underestimated.

Empirical research into the extent of personalised communication, and its effects on access to diverse information, can serve as a reality check. Empirical research can help to adjust the priorities in public policy, and to identify areas in which we simply do not know enough to make any conclusive policy statements. Below, we focus on empirical evidence of the spread of personalised news services and its likely effects on political polarisation and political information.

4. HOW COMMON IS PERSONALISATION?

PREVALENCE OF SELF-SELECTED PERSONALISATION

Selectively using information that matches pre-existing beliefs is human. People tend to avoid media content that conflicts with their beliefs (Festinger, 1957). The first data on this were collected during a US election campaign in 1940: Democrats were more likely to be exposed to the Democratic Campaign, and Republicans to the Republican campaign (Lazarsfeld, Berelson, & Gaudet, 1944). Many European countries have known a strong party press until the first half of the 20th century, with people being exposed to mainly like-minded information (Hallin & Mancini, 2004). A prime example is the period of pillarisation (*verzuiling*) in the Netherlands, where Catholics were commonly assumed to read a Catholic newspaper, to join a Catholic sports club, and to listen to Catholic radio. Left-voting labour workers had their own pillar, as did protestants (Lijphart, 1968; Wijfjes, 2004). Although the premise that the cleavages were that rigid has been challenged somewhat (Bax, 1988; Blom & Talsma, 2000), being exposed to like-minded content was pretty likely.

Nevertheless, in a literature review from as early as 1967, Sears and Freedman (1967) contest the idea that selective exposure occurs because of cognitive dissonance. In the decades that followed, interest in the topic was lost, in part because media choice was limited to few TV channels and newspapers, rendering the

mechanism somewhat irrelevant. Once the choice grew with the advent of cable TV and the internet, the topic gained renewed scholarly interest.

Whereas it is trivial to show that the audience of partisan media outlets in general is partisan as well, this does not have to be problematic from a normative point of view. It is insufficient to look at usage of isolated media outlets, because those who use a lot of partisan information *also* use an above-average amount of mainstream news (e.g., Bimber & Davis, 2003; Trilling & Schoenbach, 2015; Zaller, 1992). Furthermore, at least in Europe, most people by far still get their news via traditional sources, most notably public-service television (Blekesaune, Elvestad, & Aalberg, 2012; Trilling & Schoenbach 2013a, 2013b, 2015). The fact that fewer people watch mainstream TV news and read newspapers does not mean that people massively turn to alternative specialist outlets; most online outlets with a substantial reach are spin-offs of traditional media. Thus, those who use extremely partisan outlets are mostly exposed to moderate ideas as well. If there are echo chambers, the walls are pretty porous. Therefore, Garret distinguishes between *selective exposure* and *selective avoidance*: while there is some evidence that people *select* information they agree with, it is much less certain whether people actually *avoid* possibly conflicting information (Garret, 2009a, 2009b; Garret, Carnahan, & Lynch, 2011).

In summary, people self-select information they agree with, but the importance of this might not be as dramatic as often suggested, because even if people self-select consonant content, they may well be confronted with conflicting content as well.

PREVALENCE OF PRE-SELECTED PERSONALISATION

In contrast to self-selected personalisation, pre-selected personalisation is not a result of a user's direct choice - but of a choice that is determined by algorithms. This is commonly known from recommendations on online shopping sites or on YouTube (O'Callaghan, Greene, Conway, Carthy, & Cunningham, 2013) and in the context of online search results (Van Hoboken, 2012; Dillahunt, Brooks, & Gulati, 2015). It is debatable how common and far-reaching pre-selected personalisation is. For example, there is some evidence that 11% of Google searches differ due to personalisation (Hannak, Sapiezynski, Molavi Kakhki, Krishnamurthy, Lazer, Mislove, & Wilson, 2013). Whether this 11% is a high percentage or not is impossible to tell as we lack the adequate benchmarks.

On news sites, algorithmic personalisation is still less prevalent. People generally have the choice whether they want their online news to be personalised or not. Additionally, people who choose pre-selected personalisation are more likely to

use an above-average amount of general-interest news as well (Beam & Kosicki, 2014), and to encounter messages that are not in line with their own ideas (Beam, 2013). However, as personalisation on news websites is still in its infancy, in the future the effects may be different (Thurman & Schifferes, 2012; Turow, 2011).

While personalisation features on news sites themselves are not common yet, de facto algorithmic personalisation can arise on two other layers: news aggregators and social networks. Purely algorithmic news aggregators like Google News have mostly failed to become a major news source for a large audience, but more and more traffic to news sites goes via social media sites, which use a blend of algorithmic and human recommendations to define the supply of news items for the individual.

Social media sites can lead to two sources of personalisation. First, although people connect with different types of contacts (friends, family, colleagues etc.) on such sites, many people might mostly connect to people who resemble them. If someone's network is rather homogeneous, this means that the content shared by someone's contacts may be in line with the person's preferences as well. This argument is based on the assumption that people only share content they agree with – an assumption that has been challenged by some (Barbera, Jost, Nagler, Tucker, & Bonneau, 2015; Morgan, Shafiq, & Lampe, 2013).

Second, on some sites, most prominently on Facebook, an opaque algorithm determines what content is shown in a user's newsfeed. A recent study suggests that the influence of this algorithm is lower than the influence of the user's choices (Bakshy, Messing, & Adamic, 2015). However, the validity of this study is debated among social science scholars and beyond (Lumb, 2015).

In sum, it looks as if either personalisation is still in its infancy on news sites, or we have too little empirical evidence on what is actually happening in this domain. More independent research is necessary.

5. WHAT ARE THE EFFECTS OF PERSONALISATION?

An even harder question concerns the long-term effects of personalisation. Does personalised content really influence people? Does, or could, personalisation really harm democracy? While the effects of self-selected personalisation on democracy have been studied in a number of experiments and surveys, the effects of preselected personalisation have not been investigated in a comprehensive academic study so far.

In general, we can expect effects of selective exposure or selective avoidance on two different variables that are relevant in democratic societies: political polarisation and political knowledge.

POLARISATION AS A CONSEQUENCE OF SELF-SELECTED PERSONALISATION

Numerous scholars of political communication have studied the effects of a selective media diet on democratic societies. Most of these studies are concerned with one potential consequence of selective exposure that might be harmful to democratic societies: partisan polarisation.

According to this line of research, people who are repeatedly exposed to biased information that favours a particular political standpoint that is close to their own will eventually develop more extreme positions and be less tolerant with regard to opposite points of view. Empirical evidence from the US supports this argument. For example, Stroud (2010) used representative American election survey data to show that Americans who adopt a homogenous partisan news diet become more extreme in their views during the campaign. Similar effects of self-selective exposure to partisan news on polarisation were also found in experimental settings (e.g. Knobloch-Westerwick & Meng, 2011).

To understand the importance of cross-cutting information in a democracy, Price, Cappella, and Nir (2002) investigated the effects of being exposed to information in the mass media that contradicts existing attitudes and beliefs. They found that people who regularly encounter diverse opinions in the media are not only better able to provide reasons for their own political choices; they also have a better understanding of what motivates the perspective of others.

The effect of personalised news on polarisation is conditional on the political system. Most of the research on the effect of polarisation stems from the US, which is characterised by a bipolar political system, in which the issue of polarisation is substantially different than, for example, in the Dutch political system where more than ten parties compete with each other (e.g., Trilling, Van Klingeren, & Tsfati, 2016). This difference between political systems must be kept in mind when discussing the effects of personalisation.

POLITICAL LEARNING, AS IMPACTED BY SELF-SELECTED PERSONALISATION

While there is a growing body of studies providing evidence that selective exposure is related to polarisation, evidence on the effect of selective exposure or selective avoidance on knowledge gains is scarce. Yet, there is a strong theoretical link between political knowledge and self-selected personalised communication.

First, many media users take advantage of the abundance of media outlets to avoid political information altogether. Hence, these users lose an important information source to form political opinions (Prior, 2007). Second, if media users select political information that is attractive to them, they will be better motivated to process the information they encounter.

Hence, personalisation might lead to knowledge gaps in society: News avoiders know little. Those who self-select political news learn more from the news. This holds in particular for online news sources where users can choose news they are interested in (Kenski & Stroud, 2006). However, the effects of self-selection of news on polarisation and political knowledge are – like most media effects – small. Additionally, the effect of a personalised and selective news menu is different for each individual, and many people are not affected (Valkenburg & Peter, 2013). The fact that the relationships introduced above are statistically significant means that there is convincing empirical proof that selective exposure to news and polarisation and differential knowledge gains are related. Yet, the fact that the effect is small means that selective exposure to news explains only a small fraction of the variance in political attitudes and political knowledge we find in democratic societies.

One of the reasons for the small effect is that hardly anyone lives in an absolute information cocoon, as mentioned previously. In the current fragmented media landscape, people can access an abundance of news sources. In addition, we often get information about current events through conversations with colleagues, friends, or family members. In such conversations people may be introduced to news items, or to different perspectives. Cross-cutting conversations about politics also can occur online, mostly in an environment that does not usually deal with political information, like an online hobby group (Wojcieszak & Mutz, 2009).

EFFECTS OF PRE-SELECTED PERSONALISATION

Empirical research into the long-term effects of pre-selected personalisation is scarce (see Van Hoboken, 2012). The lack of empirical evidence can be partly explained by the fact that algorithms which automatically pre-select news items for individual users have only been developed in the past few years.

It is, however, possible that potential effects of pre-selected personalisation are in line with effects of self-selected personalisation. Being repeatedly exposed to the same news frame, for example, may lead to reinforcing framing effects (Lecheler & De Vreese, 2011). Potentially, algorithms that favour news items framing events in a perspective close to the reader's point of view will lead to a more polarised society. One of the first studies of news personalisation using search behaviour

and social media as point of departure indeed found polarising effects, while also demonstrating an increase in cross-cutting exposure through social media (Flaxman, Goel, & Rao, 2014)

With regard to systematic gaps of knowledge about current events, pre-selected personalisation might contribute to social sorting, as explained above. If algorithms are programmed to favour news items that cover only a small set of topics that users are assumed to be interested in, users will not be exposed to information on many other topics that are important for society at large. As interest in news and politics correlates with higher education and higher social economic status, this could lead to a divided citizenry.

Moreover, commercial news providers gain power because they can control the algorithm. For example, a recent experiment carried out by Facebook shows that they were able to influence people's emotions by manipulating content. The experiment involved manipulating the selection of user messages ('posts') that 689,003 users saw in their newsfeeds. "When positive expressions were reduced, people produced fewer positive posts and more negative posts; when negative expressions were reduced, the opposite pattern occurred" (Kramer, Guillory & Hancock, 2014, p. 1). Hence, Facebook succeeded in influencing the emotions of users. However, the effects were rather small. In another study, the effects appeared to be stronger: Epstein and Robertson (2015) claim that differences in Google search results can shift voting preferences of undecided voters by 20%.

As outlined in a previous section, news users have always limited their exposure to specific news items themselves: a process of self-selected personalisation. Perhaps pre-selected personalisation by algorithms merely anticipates choices that news users would have made themselves?

Even if it were true that personalisation could influence people deeply, would the many possibilities to broaden one's horizon outweigh the effects of personalisation? For example, the web offers many ways to encounter unexpected content.

The effects of personalisation may be counteracted by other forces. For example, people who self-select content on some blogs and encounter a lot of pre-selected content on their Facebook newsfeed may still be avid users of non-personalised news sites as well.

Another reason to doubt whether there is a big risk that personalised content will steer people's worldview is that current personalisation technologies may be insufficient. For instance, with targeted online advertising (behavioural targeting)

the click-through rate on ads is around 0.1% to 0.5% (e.g. Chaffey, 2015). This suggests that algorithms of companies do not predict people's interests very accurately. After all, around 999 out of 1,000 people do not click on ads – perhaps the ads do not appeal to the interests of most people. On the other hand, the low click-through rate on ads could perhaps be explained by scepticism towards advertising rather than by bad personalisation.

In sum, there is no reason to worry about pre-selected personalisation leading to filter bubble problems, briefly put, because the technology is still insufficient. With technological developments, however, problems may arise. As Hildebrandt notes, pre-selected personalisation could be seen as an early example of ambient intelligence: technology that senses and anticipates people's behaviour in order to adapt the environment to their inferred needs (Hildebrandt, 2010). Consequently, algorithmic accountability through transparency becomes more and more important as the technology develops (Diakopoulos, 2014).

6. CONCLUSION

Some fear that personalised communication can lead to information cocoons or filter bubbles. In brief, the idea is that democratic society is at risk because personalised content and services limit the diversity of media content people are exposed to. In this way, personalisation could steer people's ideas and behaviour surreptitiously.

We discussed whether we should worry about filter bubbles. We distinguish between self-selected personalisation, where people actively choose which content they see, and pre-selected personalisation, where algorithms personalise content for users without any deliberate user choice. We summarised empirical research on the extent of personalisation in practice and on the effects of personalisation.

We conclude that – in spite of the serious concerns voiced – at present, there is no empirical evidence that warrants any strong worries about filter bubbles. Nevertheless, the debate about filter bubbles is important. Personalisation on news sites is still at an infant stage, and personalised content does not constitute a substantial information source for most citizens, as our review of literature on media use has shown. However, if personalisation technology improves, and personalised news content becomes people's main information source, problems for our democracy could indeed arise, as our review of empirical studies of media *effects* has shown.

In the light of the rapidly changing media landscape, many studies become out-

dated rapidly. In addition, existing studies mainly cover the US situation with its two-party political system, which means that the studies are only partly relevant for countries with multiparty systems.

One lesson we should have learned from the past is that panic does not lead to sane policies. More evidence is needed on the process and effects of personalisation, so we can shift the basis of policy discussions from fear to insight.

REFERENCES

Bakshy, E., Messing, S., & Adamic, L. (2015). Exposure to ideologically diverse news and opinion on Facebook. *Science, 58*(4), 707–731.

Barbera, P., Jost, J. T., Nagler, J., Tucker, J. A., & Bonneau, R. (2015). Tweeting from left to right: Is online political communication more than an echo chamber? *Psychological Science*, Advance online publication.

Bax, E.H. (1988). *Modernization and cleavage in Dutch society. A study of long term economic and social change*. PhD Dissertation, Rijksuniversteit Groningen, Netherlands.

Beam, M. A. (2013). Automating the news: How personalized news recommender system design choices impact news reception. *Communication Research, 14*, 1019-1041

Beam, M. A., & Kosicki, G. M. (2014). Personalized news portals: Filtering systems and increased news exposure. *Journalism & Mass Communication Quarterly, 91*(1), 59–77.

Bimber, B., & Davis, R. (2003). *Campaigning online: The Internet in U.S. elections*. New York: Oxford University Press.

Blekesaune, A., Elvestad, E., & Aalberg, T. (2012). Tuning out the world of news and current affairs: An empirical study of Europe's disconnected citizens. *European Sociological Review, 28*(1), 110–126.

Blom, C.H., & Talsma, J. (ed.) (2000). *De verzuiling voorbij. Godsdienst, stand en natie in de lange negentiende eeuw*. Amsterdam, Netherlands: Het Spinhuis.

Bond, R. M., Fariss, C. J., Jones, J. J., Kramer, A. D., Marlow, C., Settle, J. E., & Fowler, J. H. (2012). A 61-million-person experiment in social influence and political mobilization. *Nature, 489*(7415), 295-298.

Bozdag, E. (2015), *Bursting the Filter Bubble: Democracy, Design, and Ethics*. Delft University of Technology, PhD thesis.

Chaffey Chaffey, D. (2015, April). Display advertising clickthrough rates. *Smart Insights*. Retrieved from http://www.smartinsights.com/internet-advertising/internet-advertising-analytics/display-advertising-clickthrough-rates/

Cohen, S. (1973). *Folk devils and moral panics the creation of the Mods and Rockers*. St Albans: Paladin.

Council of Europe, Recommendation CM/Rec(2012)3 of the Committee of Ministers to member States on the protection of human rights with regard to search engines, adopted by the Committee of Ministers on 4 April 2012.

Diakopoulos, N. (2014). Algorithmic accountability. Journalistic investigation of computa-

tional power structures. Digital Journalism, 3, 398–415. http://doi.org/10.1080/21670811.2014.976411

Epstein, R., & Robertson, R. E. (2015). The search engine manipulation effect (SEME) and its possible impact on the outcomes of elections. *Proceedings of the National Academy of Sciences, 112*(33), E4512–E4521.

European Commission (2013). 'Preparing for a Fully Converged Audiovisual World: Growth, Creation and Values (Green Paper) Brussels, COM(2013) 231 final' (24 March 2013) <https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/convergence_green_paper_en_0.pdf> accessed on 29 July 2015, p. 14.

Festinger, L. (1957). *A theory of cognitive dissonance*. Stanford, CA: Stanford University Press.

Flaxman, S. R., Goel, S., & Rao, J. M. (2014). Filter bubbles, echo chambers, and online news consumption. Retrieved from https://5harad.com/papers/bubbles.pdf

Gitlin, T. (1998). Public spheres or public sphericules. In T. Liebes & J. Curran (Eds.), Media, ritual and identity (pp. 168–174). London: Routledge.

Garrett, R. K. (2009). Echo chambers online?: Politically motivated selective exposure among Internet news users. *Journal of Computer-Mediated Communication, 14*(2), 265–285.

Garrett, R. K. (2009). Politically motivated reinforcement seeking: Reframing the selective exposure debate. *Journal of Communication, 59*(4), 676–699.

Garrett, R. K., Carnahan, D., & Lynch, E. K. (2011). A turn toward avoidance? Selective exposure to online political information, 2004–2008. *Political Behavior, 35*(1), 113–134.

Gutwirth, S. & Hildebrandt, M. eds. (2008). *Profiling the European Citizen*. Dordrecht: Springer 2008.

Habermas, J (1989). *The structural transformation of the public sphere: An inquiry into a category of bourgeois society*. Cambridge, MA: MIT Press.

Hallin, D. C., & Mancini, P. (2004). *Comparing Media Systems*. Cambridge, UK: Cambridge University Press.

Hannak, A., Sapiezynski, P., Molavi Kakhki, A., Krishnamurthy, B., Lazer, D., Mislove, A., & Wilson, C. (2013). Measuring personalization of web search. In *Proceedings of the 22Nd International Conference on World Wide Web* (pp. 527–538). Geneva, Switzerland: International World Wide Web Conferences Steering Committee.

Helberger, N. (2011). Diversity by design. *Journal of Information Policy, 1*, 441–469.

Helberger, N., Kleinen-Von Königslöw, K. and Van der Noll, R. (2015). Regulating the new information intermediaries as gatekeepers of information diversity, *info 17*(6), p. 50-71.

Hildebrandt, M. (2010). Privacy en identiteit in slimme omgevingen. *Computerrecht*, 6, 172-182.

Kenski, K., & Stroud, N. J. (2006). Connections between Internet use and political efficacy, knowledge, and participation. *Journal of Broadcasting & Electronic Media, 50*(2), 173–192.

Kim, J., Kim, J., & Seo, M. (2014). Toward a person × situation model of selective exposure: Repressors, sensitizers, and choice of online news on financial crisis. *Journal Of Media Psychology: Theories, Methods, And Applications, 26*(2), 59-69.

Knobloch-Westerwick, S., & Meng, J. (2011). Reinforcement of the Political Self Through

Selective Exposure to Political Messages. *Journal of Communication, 61*(2), 349–368.

Kramer, A. D., Guillory, J. E., & Hancock, J. T. (2014). Experimental evidence of massive-scale emotional contagion through social networks. *Proceedings of the National Academy of Sciences, 111*(24), 8788-8790.

Lazarsfeld, P. F., Berelson, B., & Gaudet, H. (1944). *The people's choice: How the voter makes up his mind in a presidential campaign*. New York: Columbia University Press.

Lecheler, S., & de Vreese, C. H. (2011). Getting real: The duration of framing effects. *Journal of Communication, 61*(5), 959-983.

Lijphart, A. (1968). *Verzuiling, pacificatie en kentering in de Nederlandse politiek*. Amsterdam: De Bussy.

Lumb, D. (2015). Why scientists are upset about the Facebook Filter Bubble story. Retrieved from: http://www.fastcompany.com/3046111/fast-feed/why-scientists-are-upset-over-the-facebook-filter-bubble-study

Lyon, D. (2003). Surveillance as social sorting: Computer codes and mobile bodies. In D. Lyon (ed.) *Surveillance as social sorting: Privacy, risk and automated discrimination* (pp. 13–30). New York, NY: Routledge.

Morgan, J. S., Shafiq, M. Z., & Lampe, C. (2013). Is news sharing on Twitter ideologically biased ? In *Proceedings of the 2013 conference on Computer supported cooperative work* (pp. 887–897). ACM.

Negroponte, N. (1995). *Being digital*. New York, NY: Knopf.

O'Callaghan, D., Greene, D., Conway, M., Carthy, J., & Cunningham, P. (2013). The extreme right filter bubble. *arXiv preprint arXiv:1308.6149*.

Pariser, E. (2011). *The filter bubble: What the Internet is hiding from you*. New York, NY: Penguin.

Pasquale F (2015). *The black box society: The secret algorithms that control money and information*. Cambridge: Harvard University Press.

Price, V., Cappella, J. N., & Nir, L. (2002). Does disagreement contribute to more deliberative opinion? *Political Communication, 19*(1), 95-112.

Prior, M. (2007). *Post-broadcast democracy: How media choice increases inequality in political involvement and polarizes elections*. Cambridge, UK: Cambridge University Press.

Sears, D. O., & Freedman, J. L. (1967). Selective exposure to information: A critical review. *Public Opinion Quarterly, 31*(2), 194–213.

Stroud, N. J. (2010). Polarization and partisan selective exposure. *Journal of Communication, 60*(3), 556–576.

Stroud, N. J. (2011). Niche news: The politics of news choice. Oxford University Press.

Sunstein, C. R. (2002). *Republic.com*. Princeton, NJ: Princeton University Press.

Sunstein C. R. (2006). *Infotopia: How many minds produce knowledge*. New York, NY: Oxford University Press

Dillahunt, T. R., Brooks, C. A., & Gulati, S. (2015, April). Detecting and Visualizing Filter Bubbles in Google and Bing. In *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems* (pp. 1851-1856). ACM.

Thurman, N., & Schifferes, S. (2012). The future of personalization at news websites: Lessons from a longitudinal study. *Journalism Studies, 13*(5-6), 775-790.

Treiblmaier, H., Madlberger, M., Knotzer, N., & Pollach, I. (2004, January). Evaluating personalization and customization from an ethical point of view: an empirical study. In *System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on System Sciences* (pp. 10-pp). IEEE.

Trilling, D., & Schoenbach, K. (2013a). Patterns of news consumption in Austria: How fragmented are they? *International Journal of Communication, 7*, 929–953.

Trilling, D., & Schoenbach, K. (2013b). Skipping current affairs: The non-users of online and offline news. *European Journal of Communication, 28*(1), 35–51.

Trilling, D., & Schoenbach, K. (2015). Investigating people's news diets: How online news users use offline news. Communications: *The European Journal of Communication Research, 40*(1), 67–91.

Trilling, D., Van Klingeren, M., & Tsfati, Y. (2016). Selective exposure, political polarization, and possible mediators: Evidence from the Netherlands. *International Journal of Public Opinion Research*, online first. doi:10.1093/ijpor/edw003

Turow, J. (2011). The daily you: How the new advertising industry is defining your identity and your worth. New Haven, CT: Yale University Press.

Van Hoboken, J. V. J. (2012). *Search engine freedom: on the implications of the right to freedom of expression for the legal governance of search engines*. Alphen aan den Rijn, Netherlands: Kluwer Law International.

Valkenburg, P. & Peter, J.(2013). The differential susceptibility to media effects model. *Journal of Communication 63*(2), 221–243.

Vīķe-Freiberga, V., Däubler-Gmelin, H., Hammersley, B., Pessoa Maduro, L.M.P. (2013). *A free and pluralistic media to sustain European democracy*. Retrieved from http://ec.europa.eu/digital-agenda/sites/digital-agenda/files/HLG%20Final%20Report.pdf

Wojcieszak, M. E., & Mutz, D. C. (2009). Online groups and political discourse: Do online discussion spaces facilitate exposure to political disagreement? Journal of Communication, 59(1), 40–56.

Wijfjes, H. (ed.) (2004). *Journalistiek in Nederland. Beroep, cultuur en organisatie 1850-2000*. Amsterdam, Netherlands: Boom.

Zaller, J. R. (1992). *The nature and origins of mass opinion*. Cambridge, UK: Cambridge University Press.

Zarsky, T. Z. (2002). Mine your own business: making the case for the implications of the data mining of personal information in the forum of public opinion. *Yale Journal of Law and Technology* 5, 1–56.

Zuiderveen Borgesius, F.J. (2015). *Improving privacy protection in the area of behavioural targeting*, Alphen aan den Rijn, Netherlands: Kluwer Law International.

VOLUME **5**
ISSUE **3**
doi:**10.14763/2016.3.429**

This paper is part of the special issue **Doing internet governance: practices, controversies, infrastructures, and institutions** (doi:10.14763/2016.3.435)

RESEARCH ARTICLE

Instability and internet design

Sandra Braman – *Texas A&M University*

KEYWORDS: Internet design, Sociotechnical decision-making, Resilience.

ABSTRACT: Instability - unpredictable but constant change in one's environment and the means with which one deals with it - has replaced convergence as the focal problem for telecommunications policy in general and internet policy in particular. Those who designed what we now call the internet during the first decade of the effort (1969-1979), who in essence served simultaneously as its policy-makers, developed techniques for coping with instability of value for network designers today and for those involved with any kind of large-scale sociotechnical infrastructure. Analysis of the technical document series that was medium for and record of that design process reveals coping techniques that began with defining the problem and went on to include conceptual labour, social practices, and technical approaches.

RECEIVED : 25 04 2016 ACCEPTED : 17 06 2016
PUBLISHED: 30 09 2016

FUNDING: This material is based upon work supported by the US National Science Foundation under Grant No. 0823265. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author.

Where convergence was the orienting issue for communication policy-makers in the second half of the 20th century, in the 21st it is resilience in the face of instability, whether from human or natural causes, that has come to the fore (see, e.g., Manzano, et al., 2013; Smith, 2014; Sterbenz et al., 2014; Tipper, 2014). Defining instability here as unpredictable but constant change in one's environment and in the means with which one interacts with it, instability-based problems underlie many of today's internet policy issues.

Among those who must be considered policy-makers for the internet are the computer scientists and electrical engineers responsible for the technical decision-making that brings the network into being and sustains it through constant transformations, expansions, and ever-increasing complexity. The instabilities faced by early internet designers - those who worked on the problem from when it was first funded by DARPA in 1969 through the close of 1979 - were myriad in number and form. They arose on both sides of this sociotechnical infrastructure, appearing technically in software and hardware, and socially in interpersonal and institutional relations. This was a difficult working situation not only because instabilities were pervasive and unpredictable, but also because the sources of instability and their manifestations were themselves constantly refreshed, unrelenting.

It is these policy-makers who are the focus of this article, which asks: *how did technical decision-makers for what we now call the internet carry on their work in the face of unpredictable but pervasive and ongoing instability in what they were building and what they had to build it with?* It addresses this question by inductively mining the technical document series that served as both medium for internet design and a record of that history (Abbate, 1999).

The analysis is based on a reading of the almost 750 documents in the Internet Requests for Comments (RFCs, www.ietf.org/rfc.html) series that were published during the first decade of the design process (1969-1979). Coping techniques developed during this early period remain important after almost 50 years at the time of writing because such a wide range of types and sources of instability appeared during that period, and because the decisions, practices, and norms of that decade were path determinative for internet decision-making going forward. The document series records a conversation among those responsible for the technical side of the sociotechnical network, but during the first 20 years of the process in particular the discussion included a great deal of attention to social, economic, cultural, legal, and governance issues. Thinking about the design process through the lens of what it took to conceptualise the network and bring it into being under conditions of such instability increases yet again one's appreciation of what was accomplished.

The focus here is on those types of instability that are particularly important for large-scale sociotechnical infrastructure rather than those that appear with any type of endeavour. In bridge-building, for example, it is not likely that the technologies and materials being used will change constantly over the course of the project, but this is a common problem for those working with large-scale sociotechnical infrastructure. Such instability remains a central problem for internet designers today; a draft book on possible future network architectures by David Clark (2016), who has been involved with internet design since the mid-1970s, devotes significant attention to problems of this kind. Other ubiquitous and inevitable decision-making problems, such as value differences among those involved and frustration over time lags between steps of development and implementation processes, were also experienced by internet designers but are beyond the scope of this piece.

Mechanisms developed to cope with instabilities are rarely discussed in scholarly literature. The closest work, although it addresses a qualitatively different type of problem, comes from those in science, technology, and society studies (STS) who examine ways in which scientists transform various types of messiness in the laboratory into the clean details reported as scientific findings (importantly, in the work by Latour & Woolgar [1986], and Star [1989]), and into public representation of those efforts (Bowker, 1994). The research agenda going forward should look in addition at what can be learned from psychology and anthropology.

Internet designer efforts to cope with instabilities began with determining just what constituted stability - in essence, designing the problem itself in the sense of learning to perceive it and frame it in ways that helped solve it. They went on to include figuring out the details (conceptual labour), getting along (social practices), and making it work (technical approaches).

DEFINING THE PROBLEM AS A TECHNIQUE FOR ITS CURE

Discerning the parameters of instability is an epistemological problem requiring those involved in addressing it to figure out just how to know when the system is stable enough for normal operations to proceed. Internet designers have, from the beginning, required a consensus on the concepts fundamental to such problems. [1] The techniques used to achieve a consensus regarding just what distinguished stability from instability of particular importance included drawing the line be-

1. Of course the extent to which this was true shouldn't be overstated. Jon Postel famously simply announced himself as the "naming czar " when he was still a graduate student.

tween stability and instability, distinguishing among different types of change for differential treatment within protocol (standard) setting processes, and resolving tensions between the global and the local, the universal and the specific.

Although the subject of what internet designers knew empirically about how the network was actually functioning is beyond the scope of this article, it is worth noting that comprehending and responding to the sources of instability was made even more problematic by a lack of information:

> **(RFC 550, 1973, p. 2)**
>
> [E]ven those of us presumably engaged in 'computer science' have not found it necessary to confirm our hypotheses about network operation by experiment an [sic] to improve our theories on the basis of evidence.

Indeed, design force was explicitly preferred over empirical knowledge:

> **(RFC 209, 1971, p. 1)**
>
> If there are problems using this approach, please don't 'code around' the problem or treat your [network interconnection node] as a 'black box' and exxtrapolate its characteristics from a series of experiments. Instead, send your comments and problems to . . . BBN, and we will fix the . . . system."

STABILITY VS INSTABILITY

For analytical and pragmatic purposes, instability as understood here - unpredictable but constant change in one's environment, including the ways in which one interacts with and is affected by it whether directly or indirectly - can usefully be distinguished from other concepts commonly used in discussions of the internet. Instability is *not* the same thing as ignorance (lack of knowledge about something specific), uncertainty (lack of knowledge about the outcome of processes subject to contingency or opacity, or otherwise unknowable), or ambiguity (lack of clarity regarding either empirical realities or intentions). Indeed, instability differs from all of these other terms in an important way: ignorance, uncertainty, and ambiguity are about what is known by those doing the design work, *the maker*. Instability, on the other hand, is about unpredictable mutability in *that which is being made and the tools and materials available to make it*.

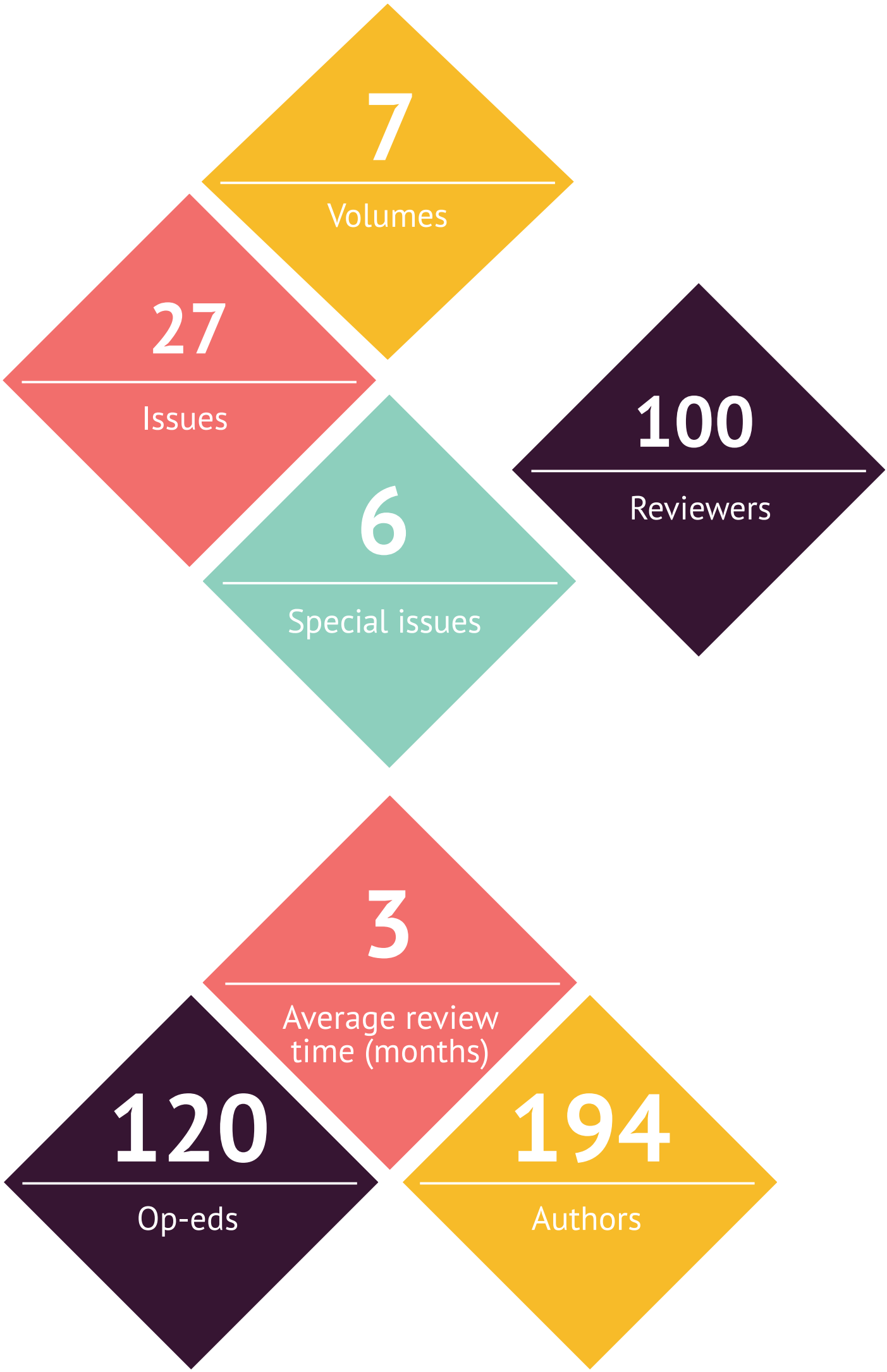
For designers of what we now call the internet, goals during the first decade of the design process *re* network stability were humble. They sought protocols that could last for at least a couple of years, fearing that if this level of stability could not be achieved it would be hard to convince others to join in the work (RFC 164, 1971). It was considered a real improvement when the network crashed only every day or two (RFC 153, 1971), a rate neither widely nor commonly experienced. According to RFC 369 (1972), no one who responded to a survey had reported a mean-time-between-failure of more than two hours and the average percentage of time with trouble free operation was 35%.

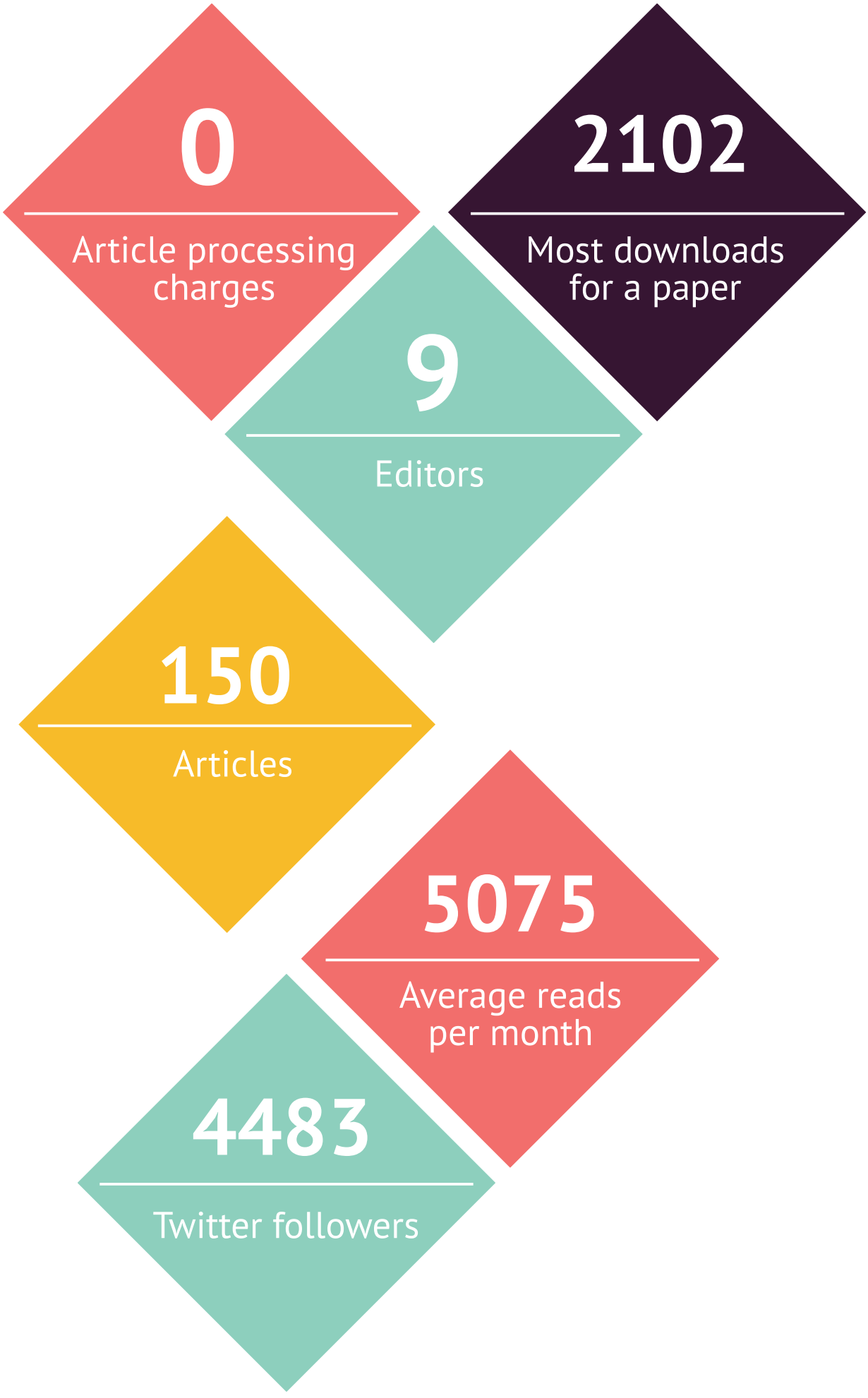
Network designers defined stability operationally, not theoretically. The network is unstable when it isn't functional or when one can't count on it to be functional in future barring extraordinary events. Concepts long used in the security domain to think about those forces that can make a system unstable can be helpful in thinking about instabilities and the internet design process. Those involved with national security distinguish between system *sensitivity* and *vulnerability*. Sensitivity involves system perturbations that may be annoying and perhaps costly but are survivable; hacking into the Democratic National Committee information systems (Sanger & Schmitt, 2016) was a perturbation, but hasn't brought the country down (as of the time of writing). Vulnerability entails those disturbances to a system that undermine its survival altogether; if malware such as Conficker (Kirk, 2015) were used to shut down the entire electrical network of the United States, it would generate a serious crisis for the country. Vulnerability has long been important to the history of telecommunications networks, being key to stimulating the growth of a non-British international telecommunications network early in the 20th century (Blanchard, 1986; Headrick, 1990); the push for greater European computational capacity and intelligent networks in the 1980s (Nora Minc, 1980; Tengelin, 1981); and in discussions of arms control (Braman, 1991) and cybersecurity (Braman, 2014). Factors that cause network instability are those that present possible vulnerabilities.

TECHNICAL CHANGE

The phenomenon of fundamental and persistent change was explicitly discussed by those involved in the early years of designing what we refer to today as the internet. The distinction between incremental and radical change was of particular importance because of the standard-setting context.

It can be difficult for those of us who have been online for decades and/or who were born "digital natives" to appreciate the extent of the intellectual and group decision-making efforts required to achieve agreement upon the most fundamen-


7
Volumes
27
Issues
6
Special issues
100
Reviewers
3
Average review time (months)
120
Op-eds
194
Authors


0
Article processing charges
2102
Most downloads for a paper
9
Editors
150
Articles
5075
Average reads per month
4483
Twitter followers

tal building blocks of the internet. Even the definition of a byte was once the subject of an RFC and there was concern that noncompliance with the definition by one user would threaten the stability of the entire network (RFC 176, 1971).

For the early internet, *everything* was subject to change, all the time: operating systems, distinctions among network layers, programming languages, software, hardware, network capacity, users, user practices, and on. Everyone was urged to take into account the possibility that even command codes and distinctions among network layers could be redefined (RFC 292, 1972). Those who were wise and/or experienced expected operational failures when ideas were first tried under actual network conditions (RFC 72, 1970). Operating by consensus was highly valued, but it was also recognised that a consensus once achieved might still have to be thrown out in response to experience or the introduction of new ideas or protocols. Instituting agreed-upon changes was itself a source of difficulty because use of the network was constant and maintenance breaks would therefore be experienced as instability (RFC 381, 1972), a condition ultimately mitigated but not solved by regular scheduling of shutdowns.

Looking back from 2016, early perceptions of the relative complexity and scale of the problem are poignant:

> **(RFC 525, 1973, p. 5)**
>
> Software changes at either site can cause difficulties since the programs are written assuming that things won't change. Anyone who has ever had a program that works knows what system changes or intermittent glitches can do to foul things up. With two systems and a Network things are at least four times as difficult.

RFC 525 (1973) also repeats the point that changes by a user at a local site can cause difficulties for the network as a whole. RFC 528 (1973) makes the opposite point: changes in the network could impede or make it impossible for processes at local user sites to continue operating as they had (RFC 559, 1973; RFC 647, 1974); one author complained about the possibility of a situation in which servers behave erratically when they suddenly find their partner speaking a new language (RFC 722, 1976). Interdependencies among the technologies and systems involved in internet design were complex, often requiring delay in implementation of seemingly minor changes because each would require so many concomitant alterations of the protocols with which they interact that all are better left until they can be a part of a major overhaul package (RFC 103, 1971).

INCREMENTAL VS RADICAL

A particularly difficult problem during the early years of the internet design process was determining when what was being proposed should be considered something new (a radical change) or a modification (incremental change) (RFC 435, 1973). The difference matters because systems respond differently to the two. Both types of change were rife during the internet design process, manifested in explicit discussions about whether something being discussed in an RFC should be treated as an official change or a modification if ultimately agreed upon and put into practice. As the question was put in RFC 72 (1970), what constitutes official change to a protocol, given that ideas about protocols go through many modifications before reaching solutions acceptable to all?

Translation of value differences into an objective framework was one means used to try to avoid tensions over whether something involved an incremental or radical change. Describing the design of algorithms as a "touchy" subject, a “Gordian knot”, for example, one author proposing a graphics protocol notes, “There are five or ten different criteria for a ‘best’ algorithm, each criterion different in emphasis” (RFC 292, 1972, p. 4). The coping technique used in response to this problem in RFC 292 was to simply order the commands by level and number them. If several commands at the same level came into conflict, some attempt would be made to encode variations of meanings in terms of bit configurations.

MACRO VS MICRO

There are two dimensions along which distinctions between macro-level and micro-level approaches were important in network design: the global vs the local, and general function vs specific function. These two can be aligned with each other, as with the local and specific treatment of a screen pixel trigger in an early graphics protocol that was determined to be so particular to a given configuration of technologies that it should not be included in internet protocols (RFC 553, 1973). The two dimensions of globality and generality, however, need not operate in tandem. In one example, sufficient universality on the network side was ensured by insisting that it could deal with all local variations encountered (e.g., RFC 184, 1971; RFC 529, 1973).

GLOBAL VS LOCAL

The tension between the universal and the local is fundamental to the nature of infrastructural systems. Indeed, as Star and Ruhleder (1996, p. 114) put it, infrastructure - however global - only comes into being in its local instances. The relationship between the two has long been important to telecommunications networks. In the 1880s, long-time AT&T president Theodore Vail and chief engineer

J. J. Carty, who designed the company's monopoly-like and, for the era, ubiquitous network, encountered it:

> 'No one knows all the details now,' said Theodore Vail. 'Several days ago I was walking through a telephone exchange and I saw something new. I asked Mr. Carty to explain it. He is our chief engineer; but he did not understand it. We called the manager. He didn't know, and called his assistant. He didn't know, and called the local engineer, who was able to tell us what it was. (Casson, 1910, p. 167)

Early internet designers phrased the problem this way: "Should a PROTOCOL such as TELNET provide the basis for extending a system to perform functions that go beyond the normal capacity of the local system" (RFC 139, 1971, p. 11). Discussion of ways in which a single entity might provide functions for everyone on the network that most other hosts would be unable to provide for themselves reads much like ruminations on a political system characterised by federalism (in the US) or subsidiarity (in Europe): ". . . to what extent should such extensions be thought of as Network-wide standards as opposed to purely local implementations" (*Ibid.*). The comparison with political thinking is not facile; a tension between geopolitical citizenship and what can be called "network citizenship" runs throughout the RFCs (Braman, 2013).

Drawing, or finding, the line between the universal and the local could be problematic. Decisions that incorporated that line included ensuring that special-purpose technology- or user-specific details could be sent over the network (RFC 184, 1971), treating transfer of incoming mail to a user's alternate mailbox as a feature rather than a protocol (RFC 539, 1973), and setting defaults in the universal position so that they serve as many users as possible (RFC 596, 1973). Interestingly, there was a consensus that users needed to be able to reconnect, but none on just where the reconnection capacity should be located (RFC 426, 1973).

GENERAL PURPOSE VS SPECIFIC PURPOSE

The industrial machines for which legal and policies were historically crafted were either single-purpose or general-purpose. As this affected network policy a century ago, antitrust (competition) law was applied to the all-private US telecommunications network because, it was argued, being general purpose - serving more than one function, carrying both data and voice - was legally problematic as unfair competition. The resulting Kingsbury Commitment separated the two functions into two separate companies and networks that could interconnect but not be the same (Horwitz, 1989).

The internet, though, was experienced as a fresh start in network design. When the

distinction between general and special purpose machines came up in the RFCs, it was with pride about having transformed what had previously been the function of a special purpose process into one available for general purpose use:

> **(RFC 435, 1973, p. 5)**
>
> With such a backbone, many of the higher level protocols could be designed and implemented more quickly and less painfully -- conditions which would undoubtedly hasten their universal acceptance and availability".

It was a basic design criterion - what can be considered, in essence, a constitutional principle for network design - that the network should serve not only all kinds of uses and all kinds of users, but also be technologically democratic. The network, that is, needed to be designed in such a way that it served not only those with the most sophisticated equipment and the fastest networks, but also those with the most simple equipment and the slowest networks (Braman, 2011). [2]

With experience, internet designers came to appreciate that the more general purpose the technologies at one layer, the faster and easier it is to design and build higher level protocols upon them. Thus it was emphasised, for example, that TELNET needed to find all commands "interesting" and worthy of attention, whether or not they were of kinds or from sources previously known (RFC 529, 1973, p. 9). In turn, as higher level and more specialised protocols are built upon general purpose protocols, acceptance of (and commitment to) those protocols and to design of the network as general purpose are reinforced (RFC 435, 1973).

Standardisation was key. It was understood that a unified approach would be needed for data and file transfer protocols in order to meet existing and anticipated network needs (RFC 309, 1972). Designing for general purpose also introduced new criteria into decision-making. Programming languages and character sets were to be maximised for flexibility (RFC 435, 1973), for example, even though that meant including characters in ASCII set that were not needed by the English language users who then dominated the design process (RFC 318, 1972).

---

2. In contrast to technological democracy, network neutrality involves regulatory treatment of vendor efforts to differentiate service provision speed to and access by users through pricing mechanisms sometimes, though not always, driven by relations between service and content providers that are also subject to competition (antitrust) law.

FIGURING OUT THE DETAILS

The importance of the conceptual labour involved in the internet design process cannot be overstated, beginning with the need to define a byte discussed above through the most ambitious visions of globally distributed complex systems of diverse types serving a multitude of users and uses. Coping techniques in this category include the art of drawing distinctions itself as well as techniques for ambiguity reduction.

CONCEPTUAL DISTINCTIONS

Early recognition that not all information received was meant to be a message spurred efforts to distinguish between bit flows intended to as communications or information transfer, and those that were, instead, errors, spurious information, manifestations of hardware or software idiosyncrasies, or failures (RFC 46, 1970; RFC 48, 1970). Other distinctions had to be drawn between data and control information and among data pollution, synchronicity, and network "race" problems (when a process races, it won't stop) (RFC 82, 1970).

The need for distinctions could get very specific. A lack of buffer space, for example, presented a very different type of problem from malfunctioning user software (e.g., RFC 54, 1970; RFC 57, 1970). Distinctions were drawn in ways perhaps more diverse than expected: people experienced what we might call ghost communications when BBN, the consulting firm developing the technology used to link computers to the network during the early years, would test equipment before delivery by sending messages received by others as from or about nodes they didn't think existed (RFC 305, 1972). And there were programmes that were perceived as having gone "berserk" (RFC 553, 1973).

Identifying commonalities that can then become the subject of standardisation is a critically important type of conceptual labour. The use of numerous *ad hoc* techniques for transmitting data and files across ARPANET was considered unworkable for the most common situations and designers knew it would become more so (RFC 310, 1972). Thus it was considered important to identify common elements across processes for standardisation. One very basic example of this was discussion of command and response as something that should be treated with a standard discipline across protocols despite a history of having previously been discussed only within each specific use or process context (RFC 707, 1975). The use of a single access point is another example of the effort to identify common functions across processes that could be standardised for all purposes (RFC 552, 1973).

Drawing conceptual distinctions is a necessary first step for many of the other cop-

ing techniques. It is required before the technical labour of unbundling processes or functions into separate functions for differential treatment, one of the technical tools discussed below, for example, and is evident in other techniques as well.

AMBIGUITY REDUCTION

Reducing ambiguity was highly valued as a means of coping with instability. One author even asserted this as a principle: "words which are so imprecise as to require quotation marks should never appear in protocol specifications" (RFC 513, 1973, p. 1). Quotation marks, of course, are used to identify a word as a neologism or a term being used with an idiosyncratic and/or novel meaning. This position resonates with the principle in US constitutional law that a law so vague two or more reasonable adults cannot agree on its meaning is unconstitutional and void.

Concerns about ambiguity often arose in the course of discussions about what human users need in contrast to what was needed for the non-human, or daemon users such as software, operating systems, and levels of the network, for which the network was also being designed (Braman, 2011). It was pointed out, for example, that the only time mail and file transfer protocols came into conflict was in naming conventions that needed to serve human as well as daemon users (RFC 221, 1971).

GETTING ALONG

The history of the internet design process as depicted in the internet RFCs provides evidence of the value of social capital, interpersonal relationships, and community in the face of instability. Valuing friendliness, communication, living with ambiguity, humour, and reflexivity about the design process were all social tools for coping with instability visible in the RFCs from the first decade. Collectively, we can refer to such tools as "getting along".

FRIENDLINESS

In addition to the normative as well as discursive emphasis on community consensus-building discussed elsewhere (Braman, 2011), the concept of friendliness was used explicitly. Naming sites in ways that made mnemonic sense to humans was deemed usefully user-friendly, allowing humans to identify the sources of incoming messages (RFC 237, 1971). Friendliness was a criterion used to evaluate host sites, both by network administrators concerned also about reliability and response time (RFC 369, 1972) and by potential users who might have been discouraged by a network environment that seemed alien (RFC 707, 1975). Interpersonal relations - rapport among members of the community (RFC 33, 1970) - were appreciated as a coping technique. The effects of one's actions on others were to be

considered: "A system should not try to simulate a facility if the simulation has side effects" (RFC 520, 1973, p. 3).

The sociotechnical nature of the effort, interestingly, shines through even when discussing interpersonal relations:

> **(RFC 33, 1970, p. 3)**
>
> The resulting mixture of ideas, discussions, disagreements, and resolutions has been highly refreshing and beneficial to all involved, and we regard the human interaction as a valuable by-product of the main effect.

At the interface between the network and local sites, internet designers learned through experience about the fundamental importance of the social side of a sociotechnical system. After discussing how network outsiders inevitably become insiders in the course of getting their systems online, one author noted,

> **(RFC 675, 1974)**
>
> [I]f personnel from the several Host[s] [sic] are barred from active participation in attaching to the network there will be natural (and understandable) grounds for resentment of the intrusion the network will appear to be; systems programmers also have territorial emotions, it may safely be assumed.

The quality of relations between network designers and those at local sites mattered because if the network were perceived as an intruder, compliance with protocols was less likely (RFC 684, 1975).

COMMUNICATION

Constant communication was another technique used in the attempt to minimise sources of instability. Rules were set for documentation genres and schedules (RFC 231, 1971). Using genre categories provided a means of announcing to users how relatively fixed, or not, a particular design decision or proposal was and when actual changes to protocols might be expected - both useful as means of dealing with instability. Today, the Internet Engineering Task Force (IETF), which hosts the RFCs online, still uses genre distinctions among such categories as *Internet Standard*, *Draft Standard*, and *Proposed Standard*, as well as genres for *Best Practices* and

others that include those that are *Informational*, *Historic*, or *Experimental*. [3]

Users were admonished to keep the RFCs and other documentation together because the RFCs would come faster and more regularly than would user guides. Still, it was highlighted, it was impossible for users to keep up with changes in the technologies: "It is *almost* inevitable that the TUG [Tip user Guide] revisions follow actual system changes" (RFC 386, 1972, p. 1, emphasis added). Simplicity and clarity in communication were valued; one author's advice was to write as if explaining something both to a secretary and to a corporation president - that is, to both the naiver and to the sophisticated (RFC 569, 1973).

LIVING WITH AMBIGUITY

Although eager to reduce ambiguity wherever possible, early network designers also understood that some amount of ambiguity due to error and other factors was inevitable (RFC 203, 1971). In those instances, the goal was to learn to distinguish among causal factors, and to develop responses to each that at least satisficed even if that meant simply ignoring errors (RFC 746, 1973).

HUMOUR

Humour is a technique used to cope with instability, as well as with ignorance, uncertainty, and ambiguity, in many environments. Within the internet design process, it served these functions while simultaneously supporting the development of a real sense of community. In RFC 468 (1973), for example, there is an amusing description of just how long it took to define something during the course of internet design. There was an ongoing tradition of humorous RFCs (beware of any published on 1 April, April Fool's Day) (Limoncelli & Salus, 2007).

REFLEXIVITY ABOUT THE DESIGN PROCESS

The final social technique for adapting to instability evident early on was sustaining communal reflexivity about the nature of the design process itself. RFC 451 (1973) highlighted the importance of regularly questioning whether or not things should continue being done as they were being done. It was hoped that practices developed within the network design community would diffuse into those of programmers at the various sites linking into the network (RFC 684, 1975).

3. Other genre distinctions have been found useful by those conducting research on the RFCs. Below (2012), for example, analysed all of the documents identifiable as "guides" by those in the field of technical communication for the ways in which they were used for community-building in a valuable case study for that community of scholars and practitioners.

MAKING IT WORK

Many of the coping techniques described above are social. Some are technical, coming into play as the design principles that are, in essence, policy for the internet design process (Braman, 2011). A final set of techniques is also technical, coming into use as specific design decisions intended to increase adaptive capacity by working with characteristics of the technologies themselves. Approaches to solving specific technical problems in the face of instability included designing in adaptive capacity, tight links between genre and machinic specifications, delay, and the reverse of delay, making something happen.

ADAPTIVE CAPACITY

General purpose machines begin by being inherently flexible enough to adapt to many situations, but it is possible to go further in enhancing adaptive capacity. The general goal of such features was captured in RFC 524 (1973):

> **(RFC 524, 1973, p. 3)**
>
> The picture being painted for the reader is one in which processes cooperate in various ways to flexibly move and manage Network mail. The author claims . . . that the picture will in future get yet more complicated, but that the proposal specified here can be conveniently enlarged to handle that picture too

The problem of adaptation came up initially with the question of what to do with software that had been designed before its possible use in a network environment had been considered. RFC 80 (1970) argued that resolving this incompatibility should get as much attention as developing new hardware by those seeking to expand the research capacity of network users. Another such mechanism was the decision to require the network to adapt to variability in input/output mechanisms rather than requiring programmes to conform with the network (RFC 138, 1971). Taking this position did not preclude establishing standards for software programmes that interact with the network and making clear that using those standards is desirable (RFC 166, 1971).

Beginning with recuperation of lost messages, and irrespective of the source of error, redundancy has long been a technique for coping with network instability issues. When satellites became available for use in international communications, for example, the US Federal Communications Commission (FCC) required every network provider to continue to invest as much in underseas cables as it invested

in satellites (Horwitz, 1989). The early RFCs discuss redundancy in areas as disparate as message transmission (RFC 65, 1970) and the siting of the network directory (RFC 625, 1974). Redundancy in databases was understood as an access issue (RFC 677, 1975).

There are other ways adaptation was technically designed into the early network as a means of coping with instability. RFC 435 (1973) looks at how to determine whether or not a server has an echoing mode during a period in which many hosts could either echo or not echo, but did not have the option to go either way. Requiring fixed socket offsets until a suitable network-wide solution could be found to the problem of identity control at connection points between computers and the ARPANET (RFC 189, 1971) is another example.

There were situations for which reliance on *ad hoc* problem solving was the preferred approach (RFC 247, 1971). At their best, *ad hoc* environments could be used for experimentation, as was done with the mail facility (RFC 724, 1977). A "level 0" protocol was a more formal attempt to define an area in which experimentation could take place; successes there could ultimately be embedded in later protocols for the network itself (RFC 549, 1973). Maintaining a “wild west” zone for experimentation as a policy tool is familiar to those who know the history of radio regulation in the United States, where amateur (“ham”) radio operators have long been given spectrum space at the margins of what was usable. Regulators understood that these typically idiosyncratic individuals were persistent and imaginative inventors interested in pressing the limits of what they could do - and that their tinkering had yielded technical solutions that then made it possible to open up those wavelengths to commercial use over and over again.

Reliance on probabilities was another long familiar technique for situations involving instability as well as uncertainty. RFC 60 (1970) describes a technique apparently used by many larger facilities connected to the network to gain flexibility managing traffic and processing loads. They would falsely report their buffer space, relying on the probability that they would not get into logistical trouble doing so and assuming that statistics would keep them out of trouble should any difficulties occur. The use of fake errors was recommended as a means of freeing up buffer space, a measure considered a last resort but powerful enough to control any emergency.

GENRE SPECIFICATIONS

Working with the genre requirements described above offered another set of opportunities for coping with instability. The RFC process was begun as an intentionally informal conversation but, over time, became much more formal regard-

ing gatekeeping, genre classification, and genre requirements specific to stages of decision-making. Concomitantly, the tone and writing style of the documents became more formal as well. It is because of these two changes to the RFC publishing process that discussions of social issues within the design conversation declined so significantly after the first couple of decades.

For any RFC dealing with a protocol, what had not been articulated simply didn't exist (RFC 569, 1973). This put a lot of weight on the needs both to provide documentation - and to keep a technology operating in exactly the manner described in that documentation (RFC 209, 1971). This was not a naive position; in discussion of the interface between the network and host computers, it was admitted that specifications were neither complete nor correct, but the advice was to hold the vendor responsible for technical characteristics as described. In a related vein, RFC authors were advised not to describe something still under experimentation in such a manner that others will believe the technology is fixed (RFC 549, 1973)

This position does, however, create a possible golem problem, in reference to the medieval story about a human-type figure created out of clay to do work for humans, always resulting in disaster because instructions were never complete or specific enough. From this perspective, the expectation of an unambiguous, completely specified mapping between commands and responses may be a desirable ideal (RFC 722, 1976), but could not realistically be achieved.

PUTTING THINGS OFF

The network design process was, by definition, ongoing, but this fundamental fact itself created instabilities: "Thus each new suggestion for change could conceivably retard program development in terms of months" (RFC 72, 1970, p. 2).

Because interdependencies among protocols and the complexity of individual protocols made it difficult to accomplish what were otherwise incremental changes without also requiring so much perturbation of protocols that wholesale revision would be needed (RFC 167, 1971), it was often necessary to postpone improvements that solved current problems until an overhaul took place. This happened with accounting and access controls (*Ibid*.) and basic bit stream and byte stream decisions for a basic protocol (RFC 176, 1971). As the network matured, it became easier to deal with many of these issues (RFC 501, 1973).

There were a number of occasions when the approach to a problem was to start by distinguishing steps of a process that had previously been treated as a single step - unbundling types of information processing, that is, in the way that vendors or regulators sometimes choose or are required to do with service or prod-

uct bundles. It was realised, for example, that treating "hide your input" and “no echo” as two separate matters usefully permitted differential treatment of each (RFC 435, 1973). Similarly, the official FTP process was broken down into separate commands for data transfer and for file transfer, with the option of further distinguishing subsets within each (RFC 486, 1973). If we think of unbundling the steps of a single process as one way of making conceptual distinctions that provide support for continuing to work in the face of instability as a vertical matter, we might call it horizontal unbundling when distinctions among types of processing involved in a single step are drawn. By 1973 (RFC 520, 1973) it had already been found that having three digits for codes to distinguish among types of replies was insufficient, so a move to five digits was proposed as a short-term fix.

DEMONSTRATION

There were some instances in which designers foresaw a potential problem but could not convince others in the community that it was likely and serious. One technique used in such instances was to make actualize the potential - to make it happen in order to demonstrate the problem in such a way that the community would so appreciate the nature and seriousness of the concern that they would turn to addressing the issue. In 1970, for example, one designer - acting on an insight he had had about a potential type of problem in 1967 - deliberately flooded the network in order to convince his colleagues of the lock-up that results when that happens because of errors in message flow (RFC 635, 1974). This technique is familiar to those who know the literature on the diffusion of innovations. In Rogers’ (2003) synthesis of what has been learned from thousands of studies of the diffusion of many different types of technologies in a wide range of cultural settings around the world, trialability and observability are among the five factors that significantly affect the willingness of individuals and groups to take up the use of new technologies and practices.

CONCLUSIONS

In today's digital, social, and natural worlds, instability is a concern of increasing importance to all of us as individuals and as communities. Those responsible for designing, building, and operating the infrastructures upon which all else depends - during times of instability just as during times of calm and slow change - confront particular difficulties of enormous importance that may be technical in nature but are of social, political, economic, and cultural importance as well. Insights drawn from discussions about the Internet design process in the Requests for Comments (RFCs) technical document series during the first decade of work on what we now call the internet (1969-1979) regarding how they coped with in-

stability provides insights into coping techniques of potential use in the design, building, and operation of any large-scale sociotechnical infrastructure. The toolkit developed by network designers engaged with all facets of what makes a particular system sociotechnical rather than "just" social or technical: negotiating the nature of the issue, undertaking the conceptual labour involved in figuring out the details, learning how to get along with all of those involved, and incorporating adaptive techniques into the infrastructure itself.

Many of those involved with "ethics in engineering," including the relatively recent subset of that community that refers to itself as studying “values in design,” often start from theory and try to induce new behaviours among computer scientists and engineers in the course of design practice with the hope of stimulating innovations in content, design, or architecture. Here, instead, the approach has been to learn from the participants in the design process themselves, learning from these highly successful technical decision-makers - *de facto* policy-makers for the internet - about how to cope with instabilities in a manner that allowed productive work to go forward.

REFERENCES

Abbate, J. (1999). *Inventing the Internet*. Cambridge, MA: MIT Press.

Below, A. (2012). The genre of guides as a means of structuring technology and community. Unpublished MA Thesis, University of Wisconsin-Milwaukee.

Blanchard, M. A. (1986). *Exporting the First Amendment*. New York: Longman.

Bowker, G. C. (1994). *Science on the run: Information management and industrial geophysics at Schlumberger, 1920-1940*. Cambridge, MA: MIT Press.

Braman, S. (2014). Cyber security ethics at the boundaries: System maintenance and the *Tallinn Manual*. In L. Glorioso & A.-M. Osula (Eds.), *Proceedings: 1st Workshop on Ethics of Cyber Conflict*, pp. 49-58. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence.

Braman, S. (2013). The geopolitical vs. the network political: Governance in early Internet design, *International Journal of Media & Cultural Politics*, *9*(3), 277-296.

Braman, S. (2011) The framing years: Policy fundamentals in the Internet design process, 1969-1979, *The Information Society*, *27*(5), 295-310.

Braman, S. (1990). Information policy and security. Presented to the 2nd Europe Speaks to Europe Conference, Moscow, USSR.

Casson, H. N. (1910). *The history of the telephone*. Chicago, IL: A. C. McClurg & Co.

Clark, D. D. (2016). *Designs for an internet*. Available at http://groups.csail.mit.edu/ana/People/DDC/archbook.

Headrick, D. R. (1990). *The invisible weapon: Telecommunications and international relations, 1851-1945*. New York/Oxford: Oxford University Press.

Horwitz, R. B. (1986). *The irony of regulatory reform: The deregulation of American telecommunications*. New York/Oxford: Oxford University Press.

Kirk, J. (2015, Aug. 3). Remember Conficker? It’s still around, *Computerworld*, http://www.computerworld.com/article/2956312/malware-vulnerabilities/remember-

conficker-its-still-around.html, accessed Sept. 6, 2016.

Latour, B. & Woolgar, S. (2013). *Laboratory life: The construction of scientific facts*, 2d ed. Princeton, NJ: Princeton University Press.

Limoncelli, T. A. & Salus, P. H. (Eds.) (2007). Book on humor in the RFCs. Peer-to-Peer Communications.

Manzano, M., Calle, E., Torres-Padrosa, V., Segovia, J., & Harle, D. (2013). Endurance: A new robustness measure for complex networks under multiple failure scenarios, *Computer Networks*, *57*, 3641-3653.

Nora, S. & Minc, A. (1980). *The computerization of society?* Cambridge, MA: MIT Press.

Rogers, E. M. (2003) *Diffusion of Innovations*, 5th ed. New York: Free Press.

Sanger, D. E. & Schmitt, E. (2016, July 26). Spy agency consensus grows that Russia hacked D.N.C., *The New York Times*, http://www.nytimes.com/2016/07/27/us/politics/spy-agency-consensus-grows-that-russia-hacked-dnc.html, accessed Sept. 6, 2016.

Smith, P. (2014). Redundancy, diversity, and connectivity to achieve multilevel network resilience, survivability, and disruption tolerance, *Telecommunications Systems*, *56*, 17-31.

Star, S. L. (1989). *Regions of the mind: Brain research and the quest for scientific certainty*. Stanford, CA: Stanford University Press.

Star, S. L. & Ruhleder, K. (1996). Steps toward an ecology of infrastructure: Design and access for large information spaces, *Information Systems Research*, *7*(1), 111-134.

Sterbenz, J.P. G., Hutchison, D., Çetinkaya, E.K., Jabhar, A., Rohrer, J.P., Schöller, M., & Tipper, D. (2014). Resilient network design: Challenges and future directions, *Telecommunications Systems*, *56*, 5-16.

Tengelin, V. (1981). The vulnerability of the computerised society. In H. P. Gassmann (Ed.), *Information, computer and communication policies for the 80s*, pp. 205-213. Amsterdam, The Netherlands: North-Holland Publishing Co.

RFCS CITED

RFC 33, New Host-Host Protocol, S. D. Crocker, February 1970.

RFC 46, ARPA Network Protocol Notes, E. Meyer, April 1970.

RFC 48, Possible Protocol Plateau, J. Postel, S. D. Crocker, April 1970.

RFC 54, Official Protocol Proffering, S.D. Crocker, J. Postel,l J. Newkirk, M. Kraley, June 1970.

RFC 57, Thoughts and Reflections on NWG/RFC 54, M. Kraley, J. Newkirk, June 1970.

RFC 60, Simplified NCP Protocol, R. B. Kalin, July 1970.

RFC 65, Comments on Host/Host Protocol Document #1, D.C. Walden, August 1970.

RFC 72, Proposed Moratorium on Changes to Network Protocol, R. D. Bressler, September 1970.

RFC 80, Protocols and Data Formats, E. Harslem, J.. Heafner, December 1970.

RFC 82, Network Meeting Notes, E. Meyer, December 1970.

RFC 103, Implementation of Interrupt Keys, R. B. Kalin, February 1971.

RFC 138, Status Report on Proposed Data Reconfiguration Service, R.H> Anderson, V.G. Cerf, E. Harslem, J.F. Heafner, J. Madden, R.M. Metcalfe, A. Shoshani, J.E. White, D.C.M. Wood, April 1971.

RFC 139, Discussion of Telnet Protocol, T. C. O'Sullivan, May 1971.

RFC 153, SRI ARC-NIC Status, J.T. Melvin, R.W. Watson, May 1971.

RFC 164, Minutes of Network Working Group Meeting, 5/16 through 5/19/71, J. F. Heafner, May 1971.

RFC 166, Data Reconfiguration Service: An Implementation Specification, R.H. Anderson, V.G. Cerf, E. Harslem, J.F. Heafner, J. Madden, R.M. Metcalfe, A. Shoshani, J.E. White, D.C.M. Wood, May 1971.

RFC 167, Socket Conventions Reconsidered, A.K. Bhushan, R. M. Metcalfe, J. M. Winett, May 1971.

RFC 176, Comments on 'Byte Size for Connections', A.K. Bhushan, R. Kanodia, R. M. Metcalfe, J. Postel, June 1971.

RFC 184, Proposed Graphic Display Modes, K.C. Kelley, July 1971.

RFC 189, Interim NETRJS Specifications, R.T. Braden, July 1971.

RFC 203, Achieving Reliable Communication, R.B. Kalin, August 1971.

RFC 209, Host/IMP Interface Documentation, B. Cosell, August 1971.

RFC 221, Mail Box Protocol: Version 2, R. W. Watson, 1971.

RFC 231, Service center standards for remote usage: A user's view, J.F. Heafner, E. Harslem, September 1971.

RFC 237, NIC View of Standard Host Names, R.W. Watson, October 1971.

RFC 247, Proffered Set of Standard Host Names, P.M. Karp, October 1971.

RFC 292, Graphics Protocol: Level 0 Only, J. C. Michener, I.W. Cotton, K.C. Kelley, D.E. Liddle, E. Meyer, January 1972.

RFC 305, Unknown Host Numbers, R. Alter, February 1972.

RFC 309, Data and File Transfer Workshop Announcement, A. K. Bhushan, March 1972.

RFC 310, Another Look at Data and File Transfer Protocols, A> K. Bhushan, April 1972.

RFC 318, Telnet Protocols, J. Postel, April 1972.

RFC 369, Evaluation of ARPANET Services January-March, 1972, J.R. Pickens, July 1972.

RFC 381, Three Aids to Improved Network Operation, J.M. McQuillan, July 1972.

RFC 386, Letter to TIP Users-2, B. Cosell, D.C. Walden, August 1972.

RFC 426, Reconnection Protocol, R. Thomas, January 1973.

RFC 435, Telnet Issues, B. Cosell, D.C. Walden, January 1973.

RFC 451, Tentative Proposal for a Unified User Level Protocol, M. A. Padlipsky, February 1973.

RFC 468, FTP Data Compression, R.T. Braden, March 1973.

RFC 486, Data Transfer Revisited, R.D. Bressler, March 1973.

RFC 501, Un-muddling 'Free File Transfer', K.T. Pogran, May 1973.

RFC 513, Comments on the New Telnet Specifications, W. Hathaway, May 1973.

RFC 520, Memo to FTP Group: Proposal for File Access Protocol, J.D. Day, June 1973.

RFC 524, Proposed mail protocol, J.E. White, June 1973.

RFC 525, MIT-MATHLAB meets UCSB-OLS -- an example of resource sharing. W. Parrish, J.R. Pickens, June 1973.

RFC 528, Software checksumming in the IMP and network reliability, J.M. McQuillan, June 1973.

RFC 529, Note on Protocol Synch Sequences, A.M. McKenzie, R. Thomas, R.S. Tomlinson, K.T. Pogran, June 1973.

RFC 539, Thoughts on the Mail Protocol Proposed in RFC 524, D. Crocker, J. Postel, July 1973.

RFC 549, Minutes of Network Graphics Group Meeting, 15-17 July 1973, J.C. Michener, July 1973.

RFC 552, Single Access to Standard Protocols, A.D. Owen, July 1973.

RFC 553, Draft Design for a Text/Graphics Protocol, C.H. Irby, K. Victor, July 1973.

RFC 559, Comments on the New Telnet Protocol and its Implementation, A.K. Bushan, August 1973.

RFC 569, NETED: A Common Editor for the ARPA Network, M.A. Padlipsky, October 1973.

RFC 596, Second thoughts on Telnet Go-Ahead, E.A. Taft, December 1973.

RFC 625, On-line hostnames service, M.D. Kudlick, E.J. Feinler, March 1974.

RFC 635, Assessment of ARPANET protocols, V. Cerf, April 1974.

RFC 647, Proposed protocol for connecting host computers to ARPA-like networks via front end processors, M.A. Padlipsky, November 1974.

RFC 675, _____. 1974.

RFC 677, Maintenance of duplicate databases, P.R. Johnson, R. Thomas, January 1975.

RFC 684, Commentary on procedure calling as a network protocol, R. Schantz, April 1975.

RFC 707, High-level framework for network-based resource sharing, J.E. White, December 1975.

RFC 722, Thoughts on Interactions in Distributed Services, J. Haverty, September 1976.

RFC 724, Proposed official standard for the format of ARPA Network messages, D. Crocker, K.T. Pogran, J. Vittal, D.A. Henderson, May 1977.

RFC 746, SUPDUP graphis extension, R. Stallman, March 1978.

VOLUME 7
ISSUE 2
doi:10.14763/2018.2.792

This paper is part of the special issue **Networked publics: multi-disciplinary perspectives on big policy issues**
(doi:10.14763/2018.2.795)

RESEARCH ARTICLE

Cryptographic imaginaries and the networked public

Sarah Myers West – *University of Southern California*

KEYWORDS: Encryption, Privacy, Security, History, Information control.

ABSTRACT: This paper interrogates discourses associated with encryption in contemporary policy debates. It traces through three distinct cryptographic imaginaries – the occult, the state, and democratic values – and how each conceptualises what encryption is, what it does, and what it should do. Situating each imaginary in time through historical research, I consider how they foreground distinct configurations of power and authority. It concludes by describing the development of a new cryptographic imaginary, one which sees encryption as a necessary precondition for the formation of networked publics.

RECEIVED: 19 12 2017 ACCEPTED: 26 03 2018
PUBLISHED: 15 05 2018

INTRODUCTION

Scholars in communication and STS have long been concerned with the implications of connective technologies for society, exploring ICTs through the frameworks of the "network society" (Castells, 1996), "culture of connectivity" (van Dijck, 2013), and "network public" (boyd, 2010), among others. In recent years, we have begun to grapple with the runaway effects of connectivity; how networked infrastructures can be used for control (Barzilai-Nahon, 2008; Benkler, 2016), enabling internet companies to accumulate vast amounts of digital data with little transparency (Zuboff, 2015; Pasquale, 2014; Angwin, 2014), and facilitating surveillance by state intelligence agencies (Schneier, 2015; Deibert, 2013) that can be used to manipulate elections (Kreiss & McGregor, 2017).

This article aims to contribute to this evolving body of work through the study of related policy debates over encryption technologies. In keeping with the theme of this special issue, 'networked publics', I explore the cultural value of cryptography as a potential counterbalance to connectivity. Cryptography enables the transformation of messages or data into code inscrutable to anyone save those with the key to unscramble it. It thus enables us to selectively reveal information to some and not to others; adding asymmetries to the process of communication that imbue messages with new kinds of power relations. Cryptographic systems exert control over access to information through the construction of their infrastructure and design: they push the limits of written communication, experiment with new forms of visual representation of an inscribed meaning, or transform it using mathematics.

But whether and to whom access to the hidden meaning in a text is selectively available is also a social and political question. Recent policy debates over encryption reflect a struggle over the information asymmetries that have arisen in an environment of surveillance capitalism (Zuboff, 2015). Over the last decade, we have undergone a process of deep mediatisation (Couldry & Hepp, 2016), recording the most intimate details of ourselves as we move through time and space. By incorporating technologies to our daily habits, the amount of metadata we produce has bloomed, leading to the production of an infinitesimal number of data traces.

As the Snowden revelations demonstrated, these data traces are not scattered to the wind, ephemeral and fleeting. Rather, they are commoditised, mined for their economic potential and harvested by intelligence agencies in the name of national security (Zuboff, 2015; West, 2017). The work of surveillance scholars situates these transitions in their political and economic context (Lauer, 2017; Schneier, 2014), observing how systems of surveillance lead to new forms of algorithmic

control (Pasquale, 2014) and are interwoven with historical patterns of discrimination (Browne, 2015).

The policy debate over encryption centres on questions about whether and under what conditions digital information should be allowed to be obscured by making it indecipherable to anyone who does not have the key to decode it. [1] For privacy advocates, encryption presents an important, if partial, solution to the harms posed by mass surveillance. In the face of growing incursions on our privacy by the state and market and insufficient accountability by regulators, encryption can serve to bolster the rights of individuals. By contrast, law enforcement agencies argue that encryption presents an existential challenge: investigators contend that they are reliant on the ability to collect and use this data in order to track down people engaged in violent extremism, using bulk collection and network analysis to map the communications networks of possible terrorists. They claim that the widespread adoption of encryption could lead to the data traces produced by suspects suddenly "going dark" (Homeland Security Committee, 2016).

These two contrasting perspectives illustrate two distinct conceptualisations of the cultural meaning of encryption. Authorities assert there must be ways of using encryption to protect secrets from adversary nations while granting law enforcement access. Advocates argue this is not mathematically possible without weakening encryption such that it could easily be broken by adversaries. This often resolves into a stalemate due to differing interpretations of what is both technically and mathematically possible and politically desirable.

At its furthest extremes, the encryption debate has displaced the underlying argument over how to synthesise differing incentives between and among state agencies seeking to protect national security and individuals' right to privacy. [2] These arguments verge on treating encryption as a teleological goal in itself; what Gürses, Kundnani and van Hoboken (2016) refer to as "crypto as a defense mechanism". By reducing the argument to technical solutions, this response fails to account for the political nature of the surveillance problem, undermining its social consequences and ignoring issues of race, gender, and class.

Really, these arguments over encryption are not about the technology itself, but

1. Though this is a global debate, taking place in the US, EU, Australia, Brazil, China and elsewhere, my analysis, admittedly, will be most representative of American policy discourses. Additional study of these issues in non-US, and particularly non-Western, contexts, is of great value.
2. The notion that there is a binary opposition between privacy and security is contested, see: Gill, 2018 (in press) and Abelson et al., 2015.

who has access to information and at what scale. The crypto debate centres on the question, what are the 'right' relationships between information and power, and how are these relationships defined? Understanding the politics of encryption requires teasing out these questions in a nuanced way, placing them in dialogue with the broader landscape of social and technological change.

This article contributes to our understanding by tracing several readings of the cultural value of encryption historically through archival research, illustrating how they have evolved over its centuries-long history and surface today in contemporary discourses. I see each of these readings as distinct *cryptographic imaginaries* - conceptualisations about what encryption *is*, what it *does*, and what it *should do*. Following Charles Taylor (2004), I see the cryptographic imaginary as something more than a set of ideas or discourses - it is embodied in both technological architecture and social practice, ways of thinking and ways of being in the world.

My analysis is grounded in a tradition in science and technology studies (STS) that sees technological infrastructures - "those systems without which contemporary societies cannot function" (Edwards, 2003) as both having hard technical materiality and being shaped through social processes. Because these infrastructures are embedded in social arrangements, they can inscribe ethical principles into a system - signaling what is important or of value, whose voice is seen as representative or marginal, or what is seen as non-controversial or mainstream.

Surfacing and making visible the imaginaries we develop around encryption provides an entrypoint to understanding the implications of encryption technologies in a networked society: how ciphers are designed to obscure information to some and not to others, how decisions are made about who can be privy to the secrets they obscure, and who can gain access to the technologies of encryption in the first place. As cryptographer Phil Rogaway writes, "That cryptographic work is deeply tied to politics is a claim so obvious that only a cryptographer could fail to see it" (Rogaway, 2015, p. 3). Understanding *how* it is tied to politics has important normative and legal implications; shaping not only the policy debate, but legal and judicial interpretations of cryptography and the architecture of encryption technologies themselves.

METHODS

The findings in this article are part of a larger multi-sited ethnographic study that traces evolutions in the cultural meaning of encryption in relation to the development of networked infrastructures between the 1960s and present day (Marcus, 1995). The analysis I outline here is largely historical and interpretive in nature,

drawing on two years of archival research across collections at Stanford Library, the Computer History Museum, the Smithsonian Museum of Natural History and IBM Research.

In order to make sense of shifts in the cultural meaning of encryption, I first sought to understand cryptography in the context of its broad, historical trajectory. I researched canonical histories of cryptography across a range of disciplines, drawing primarily on computer science, literature, and early modern history, as well as histories that were written for popular audiences. To select texts for analysis, I conducted general searches related to cryptography and encryption through my university's library, Google Scholar, and at each of the archives listed above. In addition, at each archive I conducted targeted keyword searches of the names of companies active in this space (such as RSA, Public Key Partners, and Netscape) as well as prominent individuals who were engaged in the study of cryptography (such as Martin Hellman, Whitfield Diffie, Ron Rivest, Adi Shamir, Leonard Adleman, and David Chaum), generating further sources of material to study. I coded the archival materials thematically using in vivo coding to identify dominant themes and historical trajectories, then worked within each theme to form a linear narrative that traced the evolution of the thematic material over time.

Though the findings I present largely draw from this historical research, they are also informed by two years of ethnographic field work conducted at conferences where members of the contemporary crypto community gather to discuss their work: these included the Chaos Communication Congress, the Internet Freedom Festival, RightsCon, and the Crypto Summit, among others. In addition to collecting participant observation data, I conducted dozens of interviews with privacy advocates, policy officials, and technologists working on encryption projects. This data was not included in my analysis for the purposes of this project, but was useful for providing context.

Despite this, my findings will inevitably be fragmentary and partial, the product of several limitations: first, there are aspects of cryptography that are notably absent from my analysis, such as its relationship to copyright regimes and incorporation into digital rights management technologies, which I determined to be out of scope for this project. Second, because encryption has historically been seen as a critical national security resource it is subject to the classification regimes of both government and corporate institutions; I was able to access some declassified materials but suspect that there are others that remain classified. Lastly, but importantly, there are gaps in whose voices were represented in the archives: those who spoke were primarily men with high levels of technical expertise and education, even though women and people of colour were actively involved in cryptologic

enterprises during World War II. [3] I hope to explore these gaps further in future work.

DEFINITIONS

Most texts on cryptography – its mathematical principles as well as its history – begin with a brief glossary in terms. They generally start with a statement somewhat like the following, from the Oxford English Dictionary: encryption is a "Noun. The process of converting information or data into a code, especially to prevent unauthorised access" (Oxford, 2017). This definition captures a number of different aspects of the concept: encryption as both an object (Noun.) and a process (of converting information or data into code). It is often used, as the definition suggests, "to prevent unauthorised access" – rendering its contents unintelligible to anyone without the key, or the capacity to break the code.

Encryption is also often inscribed into technical artifacts. Here, two new distinctions are drawn around what kind of inscription is involved: *ciphers*, which transpose individual letters in an alphabet, and *codes*, which replace entire plaintext words (Kahn, 1967). Similarly, to *encrypt* or *encipher* something refers to the process of translating a piece of plaintext into a ciphered text, while to *encode* means to translate the meaning of the plaintext into code. When it comes to the process of returning a code/cipher to its original plaintext, the actor's intent comes into play, as well as the environment in which they are acting: if the person has legitimate possession of the key or the system needed to convert the cryptogram back to its original plaintext, they are *deciphering* or *decoding* the text. If they are a third party adversary – someone without possession of the system or key – they are *cryptanalysing*, or *codebreaking*, the text.

Finally, encryption is increasingly implicated in infrastructure, and the term encryption is often used interchangeably with the systems it is built into. Encryption is a part of contemporary networked infrastructure, inscribed in the structures and technologies of the internet and working invisibly to support the things we do with it (Star & Ruhleder, 1996). Encryption technologies are behind every credit

3. See, for example: Mundy, L. (2017). *Code Girls: The Untold Story of the American Women Code Breakers of World War II*. New York: Hachette Books; Fagone, J. (2017). *The Woman Who Smashed Codes: A True Story of Love, Spies, and the Unlikely Heroine Who Outwitted America's Enemies*.New York: Dey Street Books; Williams, J. (2001). *The Invisible Cryptologists: African Americans, WWII to 1956*. Center for Cryptologic History, National Security Agency. Retrieved Mar. 31, 2018 from https://www.nsa.gov/about/cryptologic-heritage/historical-figures-publications/african-americans/.

card transaction, Bluetooth connection, and mobile phone call made by billions of people worldwide. They are used during the authentication of connections, protecting the connection between your computer browser and the servers of the websites we navigate to. They protect data at rest, ensuring that private information stored on servers is not easily accessed or changed by third parties. Each of these infrastructures are applications of encryption, constructed by technologists and deployed in particular ways. And thus, there are values and ethical principles inscribed in the depths of the systems that deploy encryption.

CRYPTOGRAPHIC IMAGINARIES

The remainder of this chapter is split into three sections, each describing and analysing a different cryptographic imaginary: the occult, the state, and democratic values. I define the cryptographic imaginary as a concept about what encryption *is*, what it *does*, and what it *should do* that is is embodied in both technological architecture and social practice, ways of thinking about cryptography and putting it to use.

The idea of a cryptographic imaginary owes much to the work of Charles Taylor and his elaboration of the social imaginary. Drawing on his work, I understand a social imaginary to be something broader and more all-encompassing than discourse; it is, as Taylor describes it, "not a set of ideas; rather it is what enables, through making sense of, the practices of a society" (2002, 91). Social imaginaries bridge ideas and practices, they encompass both ways of thinking and ways of being in the world. This is a particularly powerful concept for understanding the ideas that we elaborate around technologies, because it affords a mode of analysis that can include both technical practice and discursive arguments (Kelty, 2005).

In each section that follows, I trace the history of cryptography in association with each imaginary, interrogate the values implicit in them, and explain how these values surface in contemporary policy debates about cryptography.

ENCRYPTION AND THE OCCULT

The first and one of the oldest domains in which cryptography emerged associates the transformation of writing with secrecy, magic, and the occult. This is an association that lives on today as much in the writing of the thrillers of Dan Brown and his 'symbologist' Robert Langdon as in claims by Google CEO Eric Schmidt that "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place" (CNBC, 2009).

Some of the earliest versions of cryptography sought to use encryption as a way of

mystifying texts, using obfuscation not so much as a way of masking its meaning from adversaries but rather as a way to add a layer of symbolic meaning to written words. Early practices include the use of hieroglyphics in Egyptian funerary formulas and rune-writing in Scandinavia and Anglo-Saxon Britain, necromancers in the Roman empire, and the use of codes in religious texts such as the Hebrew substitution cipher Atbash, used throughout the Bible and other Jewish mystic writings to encode the names of important words. The use of codes and ciphers in mystic texts became a subject of fascination for the devoted, who developed a practice of decipherment and interpretation to unlock the deeper meanings embedded in religious texts.

The association of encryption with religious mysticism took on a darker tone by the 16th and 17th centuries, but not necessarily because cryptography was actually used as an occult practice – rather, these associations are more likely tied to the stigmatisation of secrecy by average individuals during this period. The early modern cryptography manual *Steganographia* is a good exemplar. *Steganographia* was published in 1606 by the German cryptographer Trithemius, and for years was held up as an example that tied the emerging discipline of cryptography to the practices of early modern magic (Ellison, 2017, Kahn, 1967). This historical interpretation is understandable – the text of the manuscript makes claims about instructing the reader in the use of spirits to send messages over great distances. But in the 1990s, cryptographers finally deciphered the text of its final volume, revealing these interpretations to be misguided. They found *Steganographia* to be a text that is centrally focused on cryptography, but was disguised to be a book purely focused on magic (Reeds, 1998).

Other early modern cryptographers attempted to disassociate encryption from the occult by aligning it with the emerging disciplines of the liberal arts, repositioning practices once considered to be magic, such as alchemy and astrology, into experimental and scientific practices like chemistry and astronomy (Ellison, 2017, p. 72). Their work would seem, at first, to contrast with the efforts of contemporaries like Robert Boyle, who worked to make the production of knowledge public in order to differentiate matters of fact from matters of belief. Shapin and Shaffer (1985) write of Boyle's efforts to cultivate practices of *experimental witnessing,* observing "Matters of fact were the outcome of the process of having an empirical experience, warranting it to oneself, and assuring others that grounds for their belief were adequate" (Shapin & Shaffer, 1985, p. 25).

But cultural, political, and economic factors during the time period may have indeed required some level of secret communication among participants in the scientific revolution: for example, many of these early scientists faced political dan-

gers from ecclesiastical and civil authorities (Hull, 1985), were incentivised to protect trade secrets (Macrackis, 2010), and retained paraphernalia of secret political and religious orders as a form of bonding within the budding scientific community, such as the adoption of secret names, emblems, and oaths to brotherhood (Eamon, 1985). As such, the popularity of secret communication in the emerging scientific discipline is not necessarily in contradiction with the effort to establish new standards of empiricism grounded in experimental witnessing.

Just as important, the circulation of published texts – encrypted or otherwise – in England during the 17th century was in itself subversive. Manuscripts were often spread by clandestine means in order to evade the eyes of government censors. Secret writing is thus intertwined with the practices of reading and writing, and made urgent by the widespread availability of printed matter through the invention of the printing press (Jagodzinski, 1999). As Ellison writes, cryptography "was as much a global communication system for knowledge sharing as it was also a system for hiding and concealing cultural secrets. It was as much an attempt to standardise communication across nations, ethnicities, and languages as it was a means of discriminating between audience members and preserving cultural difference" (2017, 17). It was only after the practice of reading and writing became widespread that the concepts of privacy and secrecy finally discarded their occult associations and developed a relatively neutral meaning (Jagodzinski, 1999, p. 24).

The idea that cryptography is an occult practice reflects the idea, as persistent at the time as it is today, that secrecy is a mark of poor moral character. The sociologist Georg Simmel rejected this notion, saying that "secrecy is a universal sociological form, which, as such, has nothing to do with the moral valuations of its contents" (1906, 462). But the notion never fully went away: Facebook CEO Mark Zuckerberg has made statements that suggest that hiding one's identity is a sign of a lack of integrity, reasoning that inhibiting Facebook users' capacity to obscure their identities will lead to more civil discourse.

These views are also reflected in how the use of encryption can become a trigger for surveillance: for example, the use of technologies like the Tor browser is one signal that leads to higher levels of targeting in US intelligence agencies' surveillance systems (Cox, 2014). Such an approach incorporates the common argument that "if you aren't doing anything wrong, you should have nothing to hide" in surveillance architecture, perpetuating the idea that individuals seeking privacy must be undeserving of its protections. However, it neglects to account for the real discrepancies in power between citizens and a surveillance state (Solove, 2007).

These ideas are almost never explicitly contextualised historically or tied to the

complex set of factors that related cryptography to occult practices in the early modern era. But the association between cryptography and the occult is powerful: despite the efforts of cryptographers over centuries to establish the practice as a science, it retains the residual mark of these dark associations.

CRYPTOGRAPHY AND THE STATE

Another dominant reading of cryptography centres the art of secret writing as a tool of the state. In this domain, cryptography is used as a strategic advantage over adversaries for states waging war in a geopolitical battlefield. As Lois Potter puts it in her book Secret Rites and Secret Writing: Royalist Literature 1641-1660, "Mystery is an advantage for any party in power, and, since knowledge is power, any party out of power will naturally demand further access to it. At the same time, any party which is denied access to the open expression of its views will express them covertly if it can" (Potter, 1989, p. 209).

The assertion that cryptography has historically been monopolised by state authorities requires some unpacking, however. The contemporary debates over the legal status of encryption reveal contradictions between two overlapping perspectives on the proper role of cryptography within states: cryptography as a tool for national security, and cryptography as a tool for state secrecy. These differing perspectives are increasingly in conflict with one another: whichever of them dominates will have important implications for the configuration of power in the state's orientation toward cryptography.

1. CRYPTOGRAPHY AND NATIONAL SECURITY

Cryptography is a key part of the apparatus of state national security: whoever has access to cryptography has a strategic advantage over adversaries by opening up lines of communication that cannot be intercepted. Thus, many states seek to shore up cryptographic resources by investing in technologies and in the best minds the discipline has to offer.

Though it is not the only use, the most common way cryptography has been used by states is in the military: for example, Herodotus writes that the use of secret writing saved Greece from being conquered by Xerxes, the Persian king, when an exiled Greek citizen sent a message in code to warn the Spartans of Xerxes' invasion plan (Singh, 1999). It is directly implicated in American involvement in both world wars; the decipherment of the Zimmermann telegram by the British led directly to American involvement in World War I. The failure to piece together deciphered intelligence indicating the attack on Pearl Harbor in time led directly to its entry into World War II (Kahn, 1967). The use of cryptography by military agencies

reached a new pinnacle during the wars, employed by nearly all nations engaged in the wars and codified through the formation of new agencies devoted to cryptanalysis and cryptography. Modern histories of World War II attribute the cracking of the Enigma machine as one of the decisive victories that led to the end of the war, while Sweden used cryptography decisively in order to maintain its neutrality (Kahn, 1967).

But cryptography also has an important national security function during peacetime, and is a part of the flowering of modern diplomacy between the 16th and 18th centuries: the principle of secrecy in diplomacy was well-established among European states after the Renaissance (Roberts, 2008), and enacted through the use of encryption of diplomatic communications between ambassadors and their home states. These communications were sometimes intercepted, opened and cryptanalysed by other states on the way, a practice pioneered by the French cryptologist Antoine Rossignol and institutionalised by the formation of Black Chambers by countless other states. The historian David Kahn writes that by the end of the 1500s, most European states kept full-time secretaries who worked to read the ciphered dispatches of foreign diplomats and develop official codes of their own. The sophistication of a state's cryptologic capabilities thus became a strategic advantage not only in war, but in peacetime as well (Kahn, 1967, p. 106-109 & 157-165).

Cryptography in national security is thus about a state's capacity to protect its own communications and to infiltrate the communications of their adversaries. In this sense, it is zero-sum: whoever has the most advanced cryptographic systems has a strategic advantage over others, and can leverage this advantage for both military and diplomatic benefits.

2. CRYPTOGRAPHY AND STATE SECRECY

Cryptography also plays an important domestic function *within* states, by enabling state secrecy. Historically, secrecy by the state was meant to symbolise and safeguard the dignity of rulers and integrity of their functions (Hoffman, 1981), canonised by Tacitus in his history of the Roman empire under the principle of *arcana imperii*, or secrecy for the state (Roberts, 2006). This orientation toward cryptography also seeks to maintain a state monopoly on the practice, but to different ends.

One of the earliest examples of the extensive use of encryption by a government can be observed within the pre-modern bureaucratic systems of the Abbasid caliphate. The Abbasids grew a vibrant commercial industry through the administration of strict laws and low tax rates. In order to maintain this system, administrators relied on the secure communication afforded by encryption to protect their

tax records and sensitive affairs of state (Singh, 1999).

More often, secrecy is used to mask corruption and impropriety among sovereigns. For example, King Charles I of England used encryption extensively in his letters, which became the subject of intrigue when they were leaked and published in 1645, revealing among other things his distaste for Queen Henrietta Marie prior to their marriage. The King made the mistake of keeping unciphered drafts of the letters in his papers, making the decipherment of the remaining texts all the easier once captured. This led to both embarrassment for the already-encumbered British royalist cause and, at the conclusion of the English Civil War, his execution for treason (Potter, 1989).

The embrace of secrecy has harmed states' interests in modern times as well: for decades, the United Kingdom was unable to claim its invention of the first programmable digital computer. Because of the secret nature of the country's advances in cryptography during the war, the UK destroyed all records of its invention of the Colossus, the programmable digital computer used by codebreakers at Bletchley Park to decrypt messages in the days leading up to D-Day. For years, the US-made Electronic Numerical Integrator and Computer (ENIAC) was believed to be the first computer, even though Colossus was operational three years earlier. The machine itself and much of the documentation about it were dismantled or destroyed after the war and kept secret until the 1970s (Singh, 1999, Coombs, 1983).

A series of scandals relating to state secrecy in the 1970s led to an embrace of openness in the United States, though this proved to be short-lived. The Church Committee, formed by the United States Senate found that secrecy in the Executive Branch had led to widespread abuse of powers, including the surveillance of civil rights leaders, attempts at assassination of foreign leaders, and a thirty-year programme by the US National Security Agency (NSA) to obtain copies of telegrams departing from the United States (Schwarz, 2015).

A Task Force on Secrecy concluded in 1970 that "more might be gained than lost" if the US adopted "unilaterally, if necessary - a policy of complete openness in all areas of information" (Moynihan, 61). The findings of the Task Force align with the observations of the sociologist Georg Simmel that "Democracies are bound to regard publicity as the condition desirable in itself. This follows from the fundamental idea that each should be informed about all the relationships and occurrences with which he is concerned, since this is a condition of his doing his part" (Simmel, 1906, p. 469).

The spread of networked technologies has opened up unprecedented opportunities for intelligence agencies, giving them new and significantly expanded capacity to collect data not only on citizens within the country, but from people around the globe. However, unlike during the Cold War, this capacity by no means monopolised by the United States. It has led to a fracturing of the discourse within and between government agencies around the usefulness of encryption: whether or not they see cryptography to be a friend or foe is closely tied to both their incentives and views on the role of information in national security.

For example, over the past forty years, the NSA and its UK counterpart General Communications Headquarters (GCHQ) have sought to limit the use of encryption worldwide: by inserting vulnerabilities into encryption standards (for example, by compromising the random number generator in the encryption standard adopted by the US National Institute of Standards and Technology - NIST), promoting the use of backdoored encryption devices (Levy, 2001), and engaging in legal battles to enable government agencies' access to encryption keys (Harris, 2014).

Some former national security officials have expressed support for adopting a stance that recognises the benefits of encryption, siding with those who see privacy as a necessary part of national security, not an adversary to it (Friedersdorf, 2015). This is a view that the FBI does not share – and neither do the governments of the UK, China, India, Senegal, Egypt, and Pakistan, all of which have laws that highly control or criminalise public use of encryption projects or otherwise enable law enforcement authorities to compel decryption (Abelson et al., 2015; Levy, 2001). To complicate matters, state secrecy made a forceful return in the years following the War on Terror, resulting in the expansion of systems of classification and adoption of secret tribunals to make critical decisions about surveillance authorisations.

Though the narrative of encryption as a tool of the state continues to be a dominant force in encryption policy, it is increasingly complicated and fraught with inter-agency conflict. Despite these complications, it remains true that when viewed through the lens of state power, encryption becomes part of a battlefield of intelligence in which states seek to exploit the weaknesses of others to their advantage.

ENCRYPTION AND DEMOCRATIC VALUES

The third and final domain that emerged in my research is that of encryption and democratic values. The use of codes and ciphers has a longstanding tradition in the United States reaching back to the Revolutionary War: cryptography and the pseudonymous publication of pamphlets enabled the ideas at the heart of the rev-

olution to circulate and gain popularity on their merit without the risk of immediate suppression by Loyalists (Nagy, 2009).

It also has important roots in the experiences of marginalised communities: for example, individuals fleeing slavery in the American South through the Underground Railroad were assisted by coded messages sewn onto quilts, displayed openly by conductors at waypoints on the trip north. The quilts would indicate safe houses and hiding places, or what kinds of resources were available to passengers in their travels, and were legible only to those with the ability to read the codes hidden within them (Rosenberg, 2003). The use of encryption technologies by communities of colour is a subject particularly deserving of more attention, given the long history of the racialised application of surveillance and its deployment as a means to reify boundaries around communities of colour and enforce their marginality (Browne, 2015).

In his book *Domination and the Arts of Resistance,* James C. Scott writes of practices that enable resistance in the face of the powerful. Scott writes that powerless groups often use what he calls 'hidden transcripts' to enact critiques in the face of the powerful; using disguised forms of expression such as rumors, gossip, folk tales, songs, jokes, and gestures to "insinuate a critique of power while hiding behind anonymity or behind innocuous understandings of their conduct" (Scott, 1990, p. xiii). Here, encryption is a subversive force that balances out asymmetries of power resulting from the increased surveillance capacities of both state and market actors.

By the 1980s and 1990s, amateur cryptographers were experimenting with new ideas about encryption software as an enabler of freedom (Hellegren, 2017). Calling themselves "cypherpunks", this community envisioned a new world in which individuals would gain agency through anonymity. They anticipated the dangers of a fully connected world, and put their hopes in encryption technologies as a means to resist the forces of surveillance. For decades, they worked to build tools compatible with innovations in networked technologies that would allow citizens to disconnect, to protect their privacy, and communicate anonymously. They imagined an internet that put privacy, not connectivity, at its centre, and in so doing sought to use encryption as a form of resistance against institutional power. Their work was not without flaws: many of the tools built by cypherpunks were difficult to use, and they spent relatively little time trying to encourage mainstream computer users to adopt them. However, the evolution of ideas about cryptography in response to the advancement of networked communications between the 1970s and early 2000s laid important ideological foundations for the work of privacy advocates in the present day.

For example, Chinese netizens have developed elaborate systems of coded internet slang known as *e'gao* that can be used in public on social media platforms to circumvent censorship by authorities. By reappropriating common terms and their homophones to distort or subvert their commonplace meaning, everyday citizens engage in resistance against government oversight. One well-known example is a meme in which netizens adopted the term "river crab" as a stand in for its homophone "harmonious", the signature ideology of then-Chinese president Hu Jintao. As the construction of a "harmonious" society by Hu Jintao came to be accompanied by ever-stricter levels of censorship, netizens began saying that they were "river-crabbed" in place of "harmonised" to signal to others that their words had been censored (Nordin & Richaud, 2014). The adoption of codes in this manner enabled activists to communicate outside the purview of increasingly invasive tactics by the state.

Encryption technologies have also proven useful to whistleblowers, journalists, and human rights defenders. The most famous of these cases is Edward Snowden, who used encrypted tools to protect his communications with the journalist Glenn Greenwald and filmmaker Laura Poitras while blowing the whistle on mass surveillance by the National Security Agency. Encryption enabled Snowden to mask his communications from the NSA long enough to escape to Hong Kong and publish the initial articles from the files he leaked. But, concerningly, the use of encryption by human rights advocates has increasingly served as a justification for oppression by the state: for example, the Zone 9 bloggers, a collective of journalists in Ethiopia who write about political issues and human rights abuses, were arrested and charged, among other things, for using encryption tools to protect their correspondence with sources.

In response to such actions there has been a recent effort to associate encryption with international human rights law. Following the Snowden revelations, the United Nations adopted a resolution on the right to privacy in the digital age. In 2013, then-Special Rapporteur on freedom of expression Frank La Rue drew a connection between the resolution and the use of encryption, writing that "States must refrain from forcing the private sector to implement measures compromising the privacy, security and anonymity of communications services, including requiring the construction of interception capabilities for State surveillance purposes or prohibiting the use of encryption" (Human Rights Council, 2013).

His successor, David Kaye, went on to link encryption explicitly to core values of human rights, arguing that it helps to lower barriers to the free flow of information and creates a zone of privacy necessary to make free expression possible (United Nations, 2015; Kaye, personal communication, 2017). Amnesty International has

taken this a step further, declaring that encryption is itself an 'enabler' of human rights: "Encryption is a basic prerequisite for privacy and free speech in the digital age. Banning encryption is like banning envelopes and curtains. It takes away a basic tool for keeping your life private," said Sherif Elsayed-Ali, Amnesty's Deputy Director for Global Issues.

In seeking to associate encryption with human rights, these advocates are establishing that encryption may be a precondition for democratic self-expression and association, by fostering zones of privacy where communities of individuals can join together without fear of surveillance. Cryptography thus can play an important role in creating possibilities for the formation of networked publics. This use of encryption is especially important for marginalised communities that are disproportionately exposed to the gaze of surveillance by corporations and the state under the conditions of surveillance capitalism (Zuboff, 2015; Browne, 2015; Eubanks, 2017).

CONCLUSION

My analysis treats encryption as not just a technical, but sociocultural process. Though encryption is often treated in an instrumental way - as technologies that can be used for the protection of privacy and security - I argue that cryptography has always been innately intertwined with the interrelationships between written language and culture. This has led to the development of cryptographic imaginaries, concepts about how encryption can be used to configure relationships between information and power that are embodied in technological architectures and social practices.

As I have explored in depth, several different imaginaries centred around encryption have arisen, each of which develops distinct understandings of its purpose and use. The existence of multiple co-existing cryptographic imaginaries is in part why encryption has become the subject of so much controversy: not only do encryption debates centre on different ideas about policy, or about what is mathematically possible, they invoke fundamentally different ideas about the value systems and power discrepancies encryption addresses.

For policymakers attuned to thinking of encryption as a tool for criminals and terrorists, its value as a tool for the protection of privacy may feel trivial. For military and intelligence professionals who see cryptography as a valuable national security resource, it makes sense that it would be regulated in a similar fashion to weaponry. For activists and human rights defenders who rely on cryptography to safely conduct their work, access to cryptography is an enabler of democratic

freedoms and necessary precondition for free expression.

Each of these perspectives is informed by particular configurations of access to information, and thus particular ideas about the role of cryptography in a networked society. As I have outlined, cryptography can serve as a corrective for some of the harms networked communications infrastructures make possible - namely, that the technologies that connect and empower us can also be used to surveil and hurt us. Cryptography can create new spaces of possibility for communities to form in an environment of mass surveillance; it can enable those with marginalised identities or marginalised views to create spaces for expression and cultivate relationships with like-minded individuals.

Our ability to communicate with one another across time and space through writing is accompanied by an inevitable need to retain a zone of privacy and disconnection. As historian of cryptography, David Kahn, writes, "as soon as a culture has reached a certain level, probably measured largely by its literacy, cryptography appears spontaneously – as its parents, language and writing, probably also did. The multiple human needs and desires that demand privacy among two or more people in the midst of social life must inevitably lead to cryptology wherever men thrive and wherever they write" (Kahn, 1967, p. 84).

The imaginaries we develop around the cultural meaning of cryptography will inevitably surface in what kinds of encryption technologies are built, adopted, and implemented in infrastructure. They shape the regulatory policies designed to govern them. Lastly, and perhaps most importantly, they emerge in our social imaginaries about the possibilities of our networked infrastructure.

REFERENCES

Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W., Neumann, P. G. (2015). Keys under doormats: mandating insecurity by requiring government access to all data and communications. *Journal of Cybersecurity, 1*(1), 69–79. doi:10.1093/cybsec/tyv009

Agre, P. E. (1997). *Computation and human experience*. Cambridge, UK: Cambridge University Press.

Amnesty International. (2016). Encryption: A Matter of Human Rights. *Amnesty International*. Retrieved from https://www.amnestyusa.org/reports/encryption-a-matter-of-human-rights/2/

Angwin, J. (2014). *Dragnet Nation: A quest for privacy, security and freedom in a world of relentless surveillance*. New York, NY: Times Books.

Barzilai-Nahon, K. (2008). Toward a Theory of Network Gatekeeping: A Framework for Exploring Information Control. *Journal of the American Society for Information Science and*

Technology, 59(9), 1493-1512. doi:10.1002/asi.20857

Benkler, Y. (2016). Degrees of Freedom, Dimensions of Power. *Daedalus, 145*(1): 18-32. doi:10.1162/DAED_a_00362 Available at http://www.benkler.org/Degrees_of_Freedom_Dimensions_of_Power_Final.pdf

boyd, d. (2010) Social Network Sites as Networked Publics: Affordances, Dynamics, and Implications. In Z. Papacharissi (Ed.), *Networked self: Identity, community, and culture on social network sites*. Abingdon, UK: Routledge.

Browne, S. (2015). *Dark matters: On the surveillance of blackness*. Durham: Duke University.

Calaway, J. C. (2003). *Benjamin Franklin's Female and Male Pseudonyms: Sex, Gender, Culture, and Name Suppression from Boston to Philadelphia and Beyond* (Honors Project). Illinois Wesleyan University. Retrieved from https://digitalcommons.iwu.edu/history_honproj/18/

Castells, M. (1996). *The rise of the network society*. Cambridge, MA.: Blackwell.

Couldry, N. and Hepp, A. (2016). *The Mediated Construction of Reality*. Cambridge, UK: Polity Press.

Deibert, R. (2013). *Black Code: Inside the Battle for Cyberspace*. Toronto, CA: McClelland & Stewart.

DeSeriis, M. (2015). *Improper Names: Collective Pseudonyms from the Luddites to Anonymous*. Minneapolis, MN: University of Minnesota Press.

Eamon, W. (1985). From the Secrets of Nature to Public Knowledge: The Origins of the Concept of Openness in Science. *Minerva*, *23*(3), 321-347. doi:10.1007/BF01096442

Edwards, P. (1996). *The Closed World: Computers and the Politics of Discourse in Cold War America*. Cambridge, MA: MIT Press.

Ellison, K. (2017). *A cultural history of early modern English cryptography manuals*. Abingdon, UK: Routledge, Taylor & Francis Group

Eubanks, V. (2017) *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. New York, NY: St. Martin's Press.

Eve, M. (2016). *Password*. New York, NY: Bloomsbury.

Fagone, J. (2017). *The Woman Who Smashed Codes: A True Story of Love, Spies, and the Unlikely Heroine Who Outwitted America's Enemies*. New York, NY: Dey Street Books.

Friedersdorf, C. (2015, July 30). Former National-Security Officials Now See the Peril of Weakening Encryption. *The Atlantic*. Retrieved from https://www.theatlantic.com/politics/archive/2015/07/former-national-security-officials-see-the-peril-of-weakening-encryption/399848/

Gill, L. (2018, in press). Law, Metaphor, and the Encrypted Machine. Osgoode Hall Law Journal, 55(2). Working paper version retrieved from https://ssrn.com/abstract=2933269

Gillespie, T. (2006). Engineering a Principle: 'End-to-End' in the Design of the Internet. *Social Studies of Science*, *36*(3), 427-457. doi:10.1177/0306312706056047

Gürses, S., Kundnani, A., & Van Hoboken, J. (2016). Crypto and empire: The contradictions of counter-surveillance advocacy. *Media, Culture & Society*, *38*(4), 576-590. doi:10.1177/0163443716643006

Harris, S. (2014). *@WAR: The rise of the military-Internet complex*. Boston, MA: Houghton

Mifflin Harcourt.

Hellegren, Z. I. (2017). A history of crypto-discourse: encryption as a site of struggles to define internet freedom. *Internet Histories*, *1*(4), 285–311. doi:10.1080/24701475.2017.1387466

Homeland Security Committee. (2016, June) Going Dark, Going Forward: A Primer on the Encryption Debate. *House Homeland Security Committee Majority Staff Report*. Retrieved from https://homeland.house.gov/press/house-homeland-security-committee-releases-encryption-report-going-dark-going-forward-primer-encryption-debate/

Huffington Post. (2009). Google CEO On Privacy (VIDEO). *Huffington Post*. Retrieved from http://www.huffingtonpost.com/2009/12/07/google-ceo-on-privacy-if_n_383105.html

Hull, D. (1985). Openness and Secrecy in Science: Their Origins and Limitations. *Science, Technology & Human Values*, *10*(2): 4-13. doi:10.1177/016224398501000202

Human Rights Council. (2013). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. *United Nations General Assembly*.

Jagodzinski, C. (1999). *Privacy and print : Reading and writing in seventeenth-century England*. Charlottesville, VA: University Press of Virginia.

Kahn, D. (1967). *The codebreakers; the story of secret writing*. New York, NY: Macmillan.

Kelty, C. (2005). Geeks, Social Imaginaries, and Recursive Publics. *Cultural Anthropology*, *20*(2): 185-214. doi:10.1525/can.2005.20.2.185

Kreiss, D, and McGregor, S. (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, 35*(2): 155-177. doi: 10.1080/10584609.2017.1364814

Lauer, J. (2017). *Creditworthy: A History of Consumer Surveillance and Financial Identity in America*. New York, NY: Columbia University Press.

Levy, S. (2001). *Crypto: How the code rebels beat the government--saving privacy in the digital age*. New York, NY: Viking Books.

Mackrackis, K. (2010). Confessing Secrets: Secret Communication and the Origins of Modern Science. *Intelligence and National Security*, *25*(2). doi:10.1080/02684527.2010.489275

Marcus, G. (1995). Ethnography in/of the World System: The Emergence of Multi-Sited Ethnography. *Annual Review of Anthropology*, *24*, 95-117. doi:10.1146/annurev.an.24.100195.000523

Mundy, L. (2017). *Code Girls: The Untold Story of the American Women Code Breakers of World War II*. New York, NY: Hachette Books

Nagy, J.A. (2010). *Invisible Ink: Spycraft of the American Revolution*. Yardley, PA: Westholme.

Nordin, A. & Richaud, L. (2014). Subverting official language and discourse in China? Type river crab for harmony. *China Information, 28*(1). doi:10.1177/0920203X14524687

Oxford. (2017). Encryption. *Oxford English Dictionary*. Retrieved from https://en.oxforddictionaries.com/definition/encryption

Pasquale, Frank. (2014). *The Black Box Society*. Cambridge, MA: Harvard University Press.

Potter, L. (1989). Secret rites and secret writing: Royalist literature, 1641-1660. Cambridge; New York: Cambridge University Press.

Rogaway, P. (2015). The Moral Character of Cryptographic Work. *IACR Cryptology ePrint Archive*, 1162. Available at https://eprint.iacr.org/2015/1162.pdf

Rosenberg, A. (2003). *Cryptologists: Life Making and Breaking Codes*. New York, NY: Rosen Publishing Group.

Schneier, B. (2015). *Data and Goliath : The Hidden Battles to Collect Your Data and Control Your World*. New York, NY: W.W. Norton and Co.

Schwarz Jr., F. (2015). *Democracy in the Dark: The Seduction of Government Secrecy*. New York, NY: The New Press.

Scott, J.C. (1990). *Domination and the Arts of Resistance: Hidden Transcripts*. New Haven, CT: Yale University Press.

Shapin, S. and Schaffer, S. (1985). *Leviathan and the Air-Pump*. Princeton, NJ: Princeton University Press.

Simmel, G. (1906). The Sociology of Secrecy and of Secret Societies. *American Journal of Sociology*, *11*(4), 441-498. Available at http://www.jstor.org/stable/2762562

Singh, S. (1999). *The code book: The evolution of secrecy from Mary Queen of Scots to quantum cryptography*. New York, NY: Doubleday.

Solove, Daniel J. (2007). "I've got nothing to hide" and other misunderstandings of privacy. *San Diego Law Review*, *44*(4), 745-772. Available at https://scholarship.law.gwu.edu/faculty_publications/158/

Star, S. L., & Ruhleder, K. (1996). Steps toward an ecology of infrastructure: Design and access for large information spaces. *Information systems research, 7*(1), 111-134. doi:10.1287/isre.7.1.111

Star, S.L. (1999). The Ethnography of Infrastructure. *The American Behavioral Scientist, 43*(3): 377. doi:10.1177/00027649921955326

Taylor, C. (2004) *Modern Social Imaginaries*. Durham, NC: Duke University Press.

United Nations. (2015). Report on encryption, anonymity, and the human rights framework. *United Nations Human Rights Office of the High Commissioner*. Retrieved from http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx

Van Dijck, J. (2013) Facebook and the engineering of connectivity: A multi-layered approach to social media platforms. *Convergence*, *19*(2), 141-155. doi:10.1177/1354856512457548

West, S. M. (2017). Data Capitalism: Redefining the Logics of Surveillance and Privacy. *Business & Society*. doi:10.1177/0007650317718185

Williams, J. (2001). The Invisible Cryptologists: African Americans, WWII to 1956. *Center for Cryptologic History, National Security Agency*. Retrieved from https://www.nsa.gov/about/cryptologic-heritage/historical-figures-publications/african-americans/

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology, 30*(1), 75-89. doi:10.1057/jit.2015.5

Contributors

EDITORIAL BOARD

The Editorial board of the *Internet Policy Review* is made up of internet researchers nominated for a period of two years. The Editorial board provides guidance and advice on the academic orientation of the journal and helps to promote it. The members also engage in peer reviewing research articles submitted to the *Internet Policy Review*. The Editorial board is composed of:

Maria Lilla' Montagnani – Bocconi University
INTELLECTUAL PROPERTY LAW

Federico Morando – Politecnico di Torino
ECONOMICS, INTELLECTUAL PROPERTY LAW, COMPETITION LAW

Leandro Navarro – Universitat Politècnica de Catalunya
COMPUTER SCIENCE, DISTRIBUTED SYSTEMS

Jo Pierson – Vrije Universiteit Brussel
MEDIA, COMMUNICATIONS

Jean-Christophe Plantin – LSE
MEDIA, COMMUNICATIONS

Bernhard Rieder – University of Amsterdam
NEW MEDIA, DIGITAL CULTURE

Nicola Searle – Goldsmiths, University of London
ECONOMICS, DIGITAL MEDIA

Carlos Affonso Pereira de Souza – Institute for Technology and Society
INFORMATION TECHNOLOGY LAW, CONTRACT LAW, HISTORY OF LAW

MANAGING BOARD

The Managing board of the *Internet Policy Review* is a six-member board of senior internet research scholars. The board ensures quality of the journal and makes recommendations about ethical, methodological and other academic questions that are raised by the editorial team. The Managing board is composed of:

Mélanie Dulong de Rosnay – ISCC-CNRS, Université Paris-Sorbonne

Natali Helberger – IViR, University of Amsterdam

Jeanette Hofmann – HIIG

Martin Kretschmer – CREATe, University of Glasgow

EDITORIAL TEAM

The Editorial team operates the journal on a daily basis. The academic editors are responsible for finding reviewers for each manuscript that is in their care, providing a scholarly check when it comes to the handling of theories and methodologies, as well as ensuring the texts employ the proper academic style (APA 6 references, etc). Academic editors coordinate with the managing editor to deliver comprehensive peer reviews.

Internet Policy Review is a peer-reviewed journal on internet regulation.

@PolicyR

editor@policyreview.info

:// policyreview.info

published by:

Alexander von Humboldt Institute for Internet and Society

in cooperation with:

Institut des sciences de la communication CNRS/PARIS SORBONNE/UPMC

CREATe

UOC R&I IN3 Internet interdisciplinary Institute Universitat Oberta de Catalunya