

Dutton, William H.

**Article**

## Networked publics: multi-disciplinary perspectives on big policy issues

Internet Policy Review

**Provided in Cooperation with:**

Alexander von Humboldt Institute for Internet and Society (HIIG), Berlin

*Suggested Citation:* Dutton, William H. (2018) : Networked publics: multi-disciplinary perspectives on big policy issues, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 7, Iss. 2, pp. 1-15, <https://doi.org/10.14763/2018.2.795>

This Version is available at:

<https://hdl.handle.net/10419/214060>

**Standard-Nutzungsbedingungen:**

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

**Terms of use:**

*Documents in EconStor may be saved and copied for your personal and scholarly purposes.*

*You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.*

*If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.*



<https://creativecommons.org/licenses/by/3.0/de/legalcode>



# Networked publics: multi-disciplinary perspectives on big policy issues

**William H. Dutton**

*Quello Center, Michigan State University, East Lansing, United States of America,  
wdutton@msu.edu*

Published on 15 May 2018 | DOI: 10.14763/2018.2.795

**Abstract:** This special issue of Internet Policy Review is the first to bring together the best policy-oriented papers presented at the annual conference of the Association of Internet Researchers (AoIR). This issue is anchored in the 2017 conference in Tartu, Estonia, which was organised around the theme of networked publics. The seven papers span issues concerning whether and how technology and policy are reshaping access to information, perspectives on privacy and security online, and social and legal perspectives on informed consent of internet users. As explained in the editorial to this issue, taken together, the contributions to this issue reflect the rise of new policy, regulatory and governance issues around the internet and social media, an ascendance of disciplinary perspectives in what is arguably an interdisciplinary field, and the value that theoretical perspectives from cultural studies, law and the social sciences can bring to internet policy research.

**Keywords:** Publics, Networked Publics

## Article information

**Received:** 29 Apr 2018 **Reviewed:** 02 May 2018 **Published:** 15 May 2018

**Licence:** Creative Commons Attribution 3.0 Germany

**Competing interests:** The author has declared that no competing interests exist that have influenced the text.

**URL:**

<http://policyreview.info/articles/analysis/networked-publics-multi-disciplinary-perspectives-big-policy-issues>

**Citation:** Dutton, W. H. (2018). Networked publics: multi-disciplinary perspectives on big policy issues. *Internet Policy Review*, 7(2). DOI: 10.14763/2018.2.795

## PAPERS IN THIS SPECIAL ISSUE

### **Networked publics: multi-disciplinary perspectives on big policy issues**

William H. Dutton, Michigan State University

### **Political topic-communities and their framing practices in the Dutch Twittersphere**

Maranke Wieringa, Daniela van Geenen, Mirko Tobias Schäfer, & Ludo Gorzeman

### **Big crisis data: generality-singularity tensions**

Karolin Eva Kappler

### **Cryptographic imaginaries and the networked public**

Sarah Myers West

### **Not just one, but many 'Rights to be Forgotten'**

Geert Van Calster, Alejandro Gonzalez Arreaza, & Elsemie Apers

### **What kind of cyber security? Theorising cyber security and mapping approaches**

Laura Fichtner

### **Algorithmic governance and the need for consumer empowerment in data-driven markets**

Stefan Larsson

### **Standard form contracts and a smart contract future**

Kristin B. Cornelius

## NETWORKED PUBLICS: MULTI-DISCIPLINARY PERSPECTIVES ON BIG POLICY ISSUES

### INTRODUCTION: NETWORKED PUBLICS SHAPED BY CHANGING POLICY AND REGULATION

This special issue of *Internet Policy Review* is the first of a series organised in collaboration with the Association of Internet Researchers (AoIR), an academic association centred on the 'advancement of the cross-disciplinary field of Internet studies'. AoIR was inspired by the internet as a major technological innovation of the twenty-first century, holding its first conference in 2000 around the state of what was then a fledgling field focused on a new research topic. The first conference gathered academics together with those involved with the internet from technical, corporate and governmental communities as well as many early internet enthusiasts from all sectors of society. Given its diversity within and beyond academia, early debate was centred on whether and how it should be viewed as a field. Some consensus emerged through the conferences that internet studies would be an interdisciplinary field (Wellman, 2004). No single discipline could address the internet and the many issues associated with it as objects of study (Consalvo and Ess, 2011).

Since those early days, its yearly conferences have focused on the use and impacts of continuous innovations in the internet, social media, mobile internet, the Internet of Things (IoT), and related information and communication technologies. While research on internet policy and governance has been developing since the technology's inception, it was only in 2016 that the annual AoIR conference was organised around a theme of policy and governance - the concept of 'Internet Rules!'. But with the continuing emergence of major issues of policy, regulation and governance of the internet and related ICTs, most recently around the privacy and surveillance issues of big data, policy issues have begun to draw increasing attention by the field, and this has been reflected in policy issues rising in the agendas of AoIR conferences.

This trend is illustrated by the 2017 AoIR conference. Its focus on networked publics is not explicitly policy-oriented. The concept of networked public is broad and useful in capturing the idea that networking technologies like the internet and social media can create virtual spaces analogous to physical spaces. These permit communities to form around such activities as play, work, or political and social movements. For example, danah boyd (2008) used the term to discuss her findings on the ways American teenagers used networking for a variety of social activities. I find the term compatible with my discussion of how individuals have used networks to empower themselves *vis-à-vis* institutions to become a fifth estate, comparable to the fourth estate shaped by the role of an independent press of an earlier era (Dutton, 2009). However, whatever networked public is of interest, from teenagers finding a comfortable space for socialising to networked individuals feeling free to search for information and network with others to hold powerful institutions more accountable, the vitality - if not the very existence - of these networks will depend on their policy and regulatory contexts. Therefore, it is not surprising that a conference without an explicit policy focus has yielded a strong set of policy-oriented contributions. The future of networked publics depend on the ways in which policy and regulation facilitate or constrain individuals from accessing and producing information and connecting with other individuals in meaningful ways.

From the changing composition of contributions to AoIR conferences over the years, it became increasingly apparent to the editors of *Internet Policy Review* as well as the evolving leadership of AoIR that the annual conference would be a growing source of developing scholarship on emerging issues of policy and regulation surrounding the internet. In fact, changes in the composition of AoIR conferences reflect aspects of this shift and led to more interaction between the journal and AoIR. It was in that spirit that I was asked to be a guest editor of this special issue arising from papers presented at the 2017 AoIR conference in Tartu, Estonia, organised around the theme of networked publics.

I along with the editors of *Internet Policy Review* were encouraged by the response to our call for papers to be considered for this special issue. We are pleased to provide this special issue, which is composed of the best policy-related papers presented at AoIR 2017.

Remarkably, for what has been defined as an interdisciplinary field, the papers in this special issue are more disciplinary than might have been anticipated in those early years of the field. It is even more remarkable in that policy studies are also viewed as inherently interdisciplinary. For example, many top policy studies programmes describe themselves as 'interdisciplinary', such as the Moritz College of Law's Center for Interdisciplinary Law and Policy Studies. For this reason, this special issue refers to 'multidisciplinary' rather than 'interdisciplinary' perspectives, as each paper arguably draws primarily from a core discipline, such as sociology, science and technologies studies (STS), or law. However, it will be apparent from contributions to this special issue that disciplinary perspectives on major issues surrounding the internet and policy

can offer new insights that constructively stimulate and inform debate over policy and regulation. The contributions to this issue also raise the question over whether the field as a whole is taking a more disciplinary turn.

## **THE RISE OF NEW POLICY, REGULATION AND GOVERNANCE ISSUES**

Before describing the contributions to this issue, it is useful to acknowledge and explain the relatively late emergence of policy issues both within the field and with respect to the larger public's understanding of the internet. The shift of attention to the policy issues of the internet and related information and communication technologies (ICTs) is an inescapable observation based on mass media framing of internet-related stories – but it is also one of the most dramatic developments around the internet since its first decade of worldwide diffusion.

Early internet research was focused on issues driven primarily by technical innovations (Wellman, 2004; Dutton, 2013). Internet policy research initially arose in this field largely around limitations of access to the internet and related technologies, such as over issues of building internet infrastructures (Kahin and Wilson, 1997), reducing digital divides and skill gaps (Norris, 2001; Hargittai, 2002) and responding to global internet filtering regimes (Deibert et al., 2008, 2010). However, over the last decades, there has arguably been a shift to a greater focus on a wider array of policy issues (Mueller, 2002; Cranor and Wildman, 2003; DeNardis, 2009, 2013; Braman, 2009; Dutton, 2015). This shift aligns with the internet moving from a promising innovation at the turn of the century to an essential part of the lives of most people in the world's developed economies. Within the span of two decades, this promising innovation had connected over half of the world's population, reaching over 4 billion users (54% of the world) by 2018 (World Internet Stats, 2018).

Beyond the growing centrality of the internet, there has also been a shift in public views of the internet. Instead of being seen as a technology that fosters democracy, the internet and related technologies are increasingly identified as posing threats to democratic structures and participation in politics and society (Rainie and Wellman, 2012; Howard, 2015). In this vein, the internet is increasingly portrayed as a privacy invading surveillance technology, fueled by advances in social media, big data, the Internet of Things, and artificial intelligence (Howard, 2015). Far from the 'technology of freedom' of yesteryear (de sola Pool, 1983), the internet and related social media and big data are feared to be eroding privacy and putting democracy at risk – as politicians, governments and business and industries succumb to the potential for these new tools to help them observe and manipulate public opinion and behaviour (Morozov, 2011; Greenwald, 2014; Keen, 2015; Sunstein, 2017). More people want government and internet service providers to 'do something'!

New risks tied to the internet and social media have become popularised, including:

- search algorithms trapping internet users in 'filter bubbles' (Pariser, 2011),
- social media enabling internet users to cocoon themselves in 'echo chambers' that confirm their social and political viewpoints (Sunstein, 2017); and
- advertising incentives combining with the power of social media to promote the spread of disinformation, such as so-called unprofessional, junk, or fake news (Keen, 2007).

These threats to privacy and the quality and reliability of information have found widespread acceptance by the educated public, mass media, and politicians and regulators alike, illustrated by the establishment of inquiries and study groups on such issues as privacy (Mendell et al., 2012; Hardie et al., 2014) and the disinformation fostered by junk or fake news examined by the UK's Digital, Culture, Media and Sport Committee (2017) and a high level study group for the

European Commission (2018). Only recently has systematic empirical research been undertaken to address the validity of some of these expectations, as illustrated by the contributions to this special issue.

Of course, views of the internet as a technology of freedom or control are based on technologically deterministic assumptions that are not new and that have been challenged by empirical research over the years (Beniger, 1986). Well over a decade ago, I noted that:

Growing concerns over the lack of real information, the prevalence of misinformation, and increasing problems with information overload should ... not be viewed as aberrations within an information society. These failures are actually caused by inadequate regulation of access to information - the incorrect treatment of all information as being equal and benign. (Dutton, 1999, p. 11)

Utopian versus dystopian perspectives on the role of the internet and communication technologies has been a central issue for decades (Williams, 1982). Kenneth Laudon (1977) wrote about the potential for new interactive technologies being used to manage democracy, manipulating public opinion, rather than responding to democratic forces, long before the internet was taken seriously. Laudon was focused on interactive cable and telecommunications.

However, dystopian perspectives on the internet as a technology of control and manipulation rather than freedom and collective intelligence have gained increased currency in the aftermath of major events. These include the unraveling of what was thought to be an Arab Spring fostered by social media (Morozov, 2011), the disclosures by the whistleblower Edward Snowden of classified National Security Agency (NSA) documents that provided evidence of mass surveillance (Greenwald, 2014), the rise of the Internet of Things that will put tens of billions of devices online (Howard, 2015); and the Facebook fiasco over Cambridge Analytica, in which personal data of Facebook users was obtained by a political consulting firm via an academic researcher (Dutton, 2018; Schotz, 2018).

Equally significant developments contributing to this shift of perspective have been the increasing concentration of the internet industry, such as in the so-called FANG firms of Facebook, Amazon, Netflix, and Google. As I was writing this introduction, I received an online notification from a news feed that claimed to reveal: “Why Amazon is obsessed with getting inside of our homes”. Worry over the consequences of concentration within the internet industry has been one motivation behind calls for new policy initiatives around such aims as increasing competition, privacy and data protection, and efforts to prevent the blocking of legitimate content, such as through network neutrality initiatives (Wu, 2003).

It is within this backdrop of rising concerns over threats to the very values that once almost personified the internet as a technology of freedom that all the articles within this special issue can be seen. As a group, they address three big policy and regulatory issue areas that have risen around the internet. Simply put, these are research papers on the role of the internet in reshaping:

1. access to (dis)information in ways that could literally clarify or distort our views of local and worldwide developments - from the news to environmental crises;
2. privacy, data protection, and the security of the internet - each of which are threatened in new ways by new technologies, such as big data, computational analytics, and increasingly essential services being provided online; and

3. legal and contractual relationships between users and providers - such as through new forms of notice and consent to the use of personal information.

These are only three of many more areas of key policy issues. Concerns over freedom of expression, digital divides, sociality, and many more remain equally important. But these three areas capture big areas of concern and arise from the actual composition of the best policy-related papers at AoIR 2017. The following sections provide a broad outline of the articles in this issue grouped around these three areas. This will be followed by a short overview of several cross-cutting themes of this special issue.

## **RESHAPING ACCESS TO INFORMATION: WHO KNOWS WHAT?**

All major innovations in communication technologies have a potential to reshape access to information – what we know, who we know, what services we obtain, and what knowhow we require (McLuhan, 1964; Dutton, 1999). Mark Graham (2014, p. 100) has called this ‘augmented reality’ in that the internet not only reshapes what we know, but also what we ‘are able to know and do’. This has been viewed positively with respect to the internet creating the potential for more open and global access to information, providing access to a heretofore unimaginable range of information from anywhere at any time (Dutton, 1999). Therefore, most concern in the early period of internet diffusion was focused on efforts to block access to information online, such as through internet filtering (Deibert et al., 2010).

However, it has long been argued that just as new media open up new channels of access, they can also exacerbate existing inequalities in the production and consumption of information around the world. This led the McBride Commission to call for a new world information order (ICCP, 1980), and contemporary internet scholars to call attention to continuing inequalities in access to production and consumption of information in a networked world (Castells, 1996; Graham, 2014).

As noted above, in the early years of the internet, the focus was on access to the technologies and skills to be online in a networked world, giving rise to issues over digital divides (Dutton, 1999; Norris, 2001). As increasing proportions of the world have gained access to the internet and social media, the focus has shifted to the quality and bias of information served up and consumed on these networks.

One of the most compelling arguments has been that the rise of search, and the algorithms that underpin the personalisation of its results, could be limiting access to information by diminishing the diversity of information, such as by creating a ‘filter bubble’ in which ‘what you’ve clicked on the past determines what you see next ...’ (Pariser 2011 p. 16). A similar but complementary thesis is that social media not only personalise information, but they also enable individuals to more easily and almost unwittingly cocoon themselves in what Cass Sunstein (2017p. 6) coined as ‘echo chambers’ – built by ‘people’s growing power to filter what they see’, which adds to the power of providers to filter ‘based on what they know about us’. Many – from scientists to casual news readers – wish to confirm their beliefs through what they read and hear. This ‘confirmatory bias’ is greatly enabled in principle by the new social media at our fingertips (Sunstein, 2017). Therefore, rather than simply opening up new information vistas, the new media could narrow and distort our views of reality.

In many fundamental respects, this is not a new concern. A key issue with the mass media has long been focused on the quality of news and the degree that propaganda or even documentary and entertainment media coverage might distort our views of the real world and key events, ranging from the reporting of car accidents in local news to the reporting of war correspondents in remote areas. For instance, continuing debates centre on the degree to which mass media coverage might well ‘cultivate’ misperceptions of the real world (Gerbner et al., 1986), such as through consuming news portraying the world as more violent than it is in fact when coverage tends to focus on stories that attract readers – the rule of thumb in many newsrooms that ‘if it bleeds, it leads’. But as the internet has become more central to the consumption of news, new concerns have been raised, such as around the disinformation sown by junk or fake news, and the biases introduced by filter bubbles and echo chambers described above.

The first article in this issue addresses concerns over filter bubbles and echo chambers by focusing on what the authors call ideological ‘topic-communities’ forming in the Dutch Twittersphere that are focused on politics. To what degree are they diverse and can the levels of homophily observed on Twitter be explained by either the notion of a filter bubble or an echo chamber? Maranke Wieringa, Daniela van Geenen, Mirko Tobias Schäfer, and Ludo Gorzeman’s article, ‘Political topic-communities and their framing practices in the Dutch Twittersphere’, questions the explanatory value of a filter bubble as overly deterministic in light of their findings, but they lend some support to the significance of an echo chamber among one of their observed ideological communities. Their research is focused on two weeks of normal politics – the research was not conducted during a major campaign or election – and draws on a creative and rigorous use of multiple methods to provide a strong case for their findings. Nevertheless, their work raises further questions: Are their findings a reflection of Twitter users seeking to convey, rather than consume, partisan or ideological political perspectives? Are they retweeting and framing media coverage to influence others, rather than being naïve, cocooned readers, trapped in an echo chamber?

The next article by Karolin Eva Kappler, entitled ‘Big crisis data: generality-singularity tensions’, is far removed from discussions of filter bubbles and echo chambers in political discourse. Nevertheless, Kappler forces us to consider how the use of big data in the identification and monitoring of emergencies, disasters, and crises are changing the way we see these real world events, and even whether they can sustain attention when the crisis has past. For example, when social scientists collect data through any means, whether a survey or by direct observation, their method of observation shapes what they can see as well as what might be less visible through their particular methodological lens. Kappler explores the potential of a big data bias in perception, drawing on sociological perspectives to critically compare three platforms designed to capture big data about crisis events. She identifies a variety of implications common and distinct to these different platforms’ approaches to capturing crisis data, such as the idea that they make each crisis unique – a singular event – rather than a more general crisis or just another emergency. How does what she calls the ‘platformization’ of emergencies shape what we know about them? This article is refreshing in the way it moves away from the hype about big data capturing reality to critically assessing what realities these platforms see, observe, valorise, produce, and appropriate. They are, according to Kappler, all about ‘doing singularity’ – making the event a unique rather than general phenomenon.



## COMPETING PERSPECTIVES ON PRIVACY AND SECURITY

The next set of three articles provides different disciplinary perspectives on the issues of privacy and security. The first, by Sarah Myers West, entitled ‘Cryptographic imaginaries and the networked public’, provides a fascinating historical and comparative perspective on what she calls ‘cryptographic imaginaries’ – how people think about encryption whether through cyphers (that transpose letters of an alphabet) and codes (that replace words) in different social, cultural, and political contexts. Specifically, she looks at encryption in three different cultures: the occult, affairs of state (national security and secrecy), and in democratic systems, where it provides a means to enable private communication essential to some movements by avoiding surveillance and potential social or political sanctions. Anchored in an STS approach, this comparison illustrates how similar technologies take on quite different meanings and roles in different cultural settings. Such insights support policy-making in this area by demonstrating how the technologies of encryption need to be understood not only in a technical sense, and not only cross-nationally, but also in the more specific social, cultural, and political contexts in which they are used. Technologies do not determine universal solutions as the role and impact of encryption, for example, is also shaped by their socio-cultural contexts of use.

The next article, by Geert van Calster, Alejandro Gonzalez Arreaza, and Elsemiek Apers, entitled ‘Not just one, but many ‘Rights to be Forgotten’’, is based on a comparative analysis of national law and policy anchored in what has become known as the ‘right to be forgotten’ (Mayer-Schönberger, 2009). While general support for such a right emerged in Europe initially through the courts and later through the European Commission, initiatives to legally define and implement this right have diffused widely across the world. This article conducts a comparative survey of over two dozen cases of concrete legal implementations of this right to be forgotten. The research team finds far more case law variations, such as in the territory over which the right would be enforced, than commentary on this universal right would lead us to expect. The article demonstrates the value of close and comparative legal analysis how general legal principles are implemented in case law across different national jurisdictions. Their study is reminiscent of early American research on implementation, which tracked how a policy spawned in Washington DC changed dramatically by the time it was implemented in local communities (Pressman and Wildavsky, 1973). One clear implication of their findings is the degree that even widespread acceptance of a general legal principle can still lead to cross-national differences. As various evolving principles of policy and regulation for the digital age move into national courts and legislatures, will the resulting patchwork of national case law be another force underpinning an increasing fragmentation of a global, open internet, that frustrates efforts at harmonisation?

Closely aligned with the right to privacy is an associated right to security. Computer scientists have long approached this issue in the information age through a focus on cyber security, defined to include the ‘technologies, processes, and policies that help to prevent and/or reduce the negative impact of events in cyberspace that can happen as the result of deliberate actions against information technology by a hostile or malevolent actor’ (National Research Council, 2014, p. 2). If privacy is in part defined by unauthorised access to personal information, then a lack of cyber security, such as the inability to prevent unauthorised access to internet devices or infrastructures, is one critical route to infringing privacy. Take, for instance, the US government’s efforts to unlock a smartphone to gain access to personal information in an investigation of terrorism (Benner and Lichtblau 2016).

The next article in this issue moves the discussion of cyber security from a general aim to a more concrete set of goals in more specific domains. By focusing on concrete domains or institutional contexts of cyber security, it is clear that cyber security takes on somewhat different meanings across each domain. Laura Fichtner's article, entitled 'What kind of cyber security? Theorising cyber security and mapping approaches', provides a critical, social scientific perspective on the concept of security and also distinguishes between four domains of cyber security, largely defined by the major values and purposes they prioritise in their particular contexts. These are: 1) data protection, such as protecting data files from unauthorised access; 2) safeguarding financial interests, such as preventing credit card fraud; 3) protecting public and political infrastructures, like securing electronic voting machines; and 4) information and communication flows, as in failing to prevent the exposure of diplomatic cables of the US State Department by WikiLeaks (Leigh and Harding, 2011). Anchored in an STS approach to her study and a focus on computer ethics, Fichtner builds a strong case that each of these arenas of cyber security involve not only different priorities, but also different ecologies of actors and prototypical responses. For example, compare the tolerance of the actors involved in credit card fraud (banks), where some losses are expected, to those ensuring against voting fraud (governments), where electronic voting is not allowed in most jurisdictions for fear of undetectable fraudulent voting (Jones and Simons, 2012). Here again, a closer look at the implementation of a global concept illuminates differences across domains that are important to address in policy and practice.

## **SOCIAL AND LEGAL INSIGHTS ON ISSUES OF CONSENT**

The final set of articles in this special issue address one of the most concrete but insurmountable issues of consumer protection in the digital age – how to notify and obtain the informed consent of internet users on the ways personal and trace data created by them can be used? This principle of a notice and consent process is simple to understand, but almost impossible to implement in ways that satisfy such important and obvious values as informed consent. I have witnessed many sessions at privacy and security conferences and panels that devoted disproportionate amounts of time critiquing the problems with contemporary approaches to notice and consent. Most notice and consent forms are long, technical, and not read. From here, agreement stops, as it has been more difficult to provide a clear and compelling alternative.

The first article in this section, by Stefan Larsson, is entitled 'Algorithmic governance and the need for consumer empowerment in data-driven markets'. Larsson provides an insightful critique of contemporary policy and practice on notice and consent that brings this discussion into the big data age of consumer profiling. He highlights the lack of transparency in user agreements, which are exceedingly complex, and the need for policy to strengthen consumer protection in this area. In the end, his analysis leads him to question the ability of internet users to ever be able to protect themselves in the age of big data analytics. He then makes a case for the necessity of structural reform that moves responsibility from internet users to consumer protection authorities. In many respects, this is a more specific example of the case for data protection authorities in other areas. However, his article should stimulate debate on alternative remedies. It also should raise questions over the need for all users to understand all aspects of such user agreements. If only a few users discover a problem with a notice and consent process, then their objections can become a means for holding providers more accountable to users in general. Also, will consumer protection authorities themselves be adequately resourced to hold global internet service providers to account? Will consumer protection authorities have the staff

and skills to understand how data are used by a complex ecology of actors in ways that truly protect users?

The final article is by Kristine B. Cornelius, entitled ‘Standard form contracts and a smart contract future’. Her legal perspective on contract law and practice adds an extremely useful background to the debate over how to regulate notice and consent, terms of service and other online contracts. Her historical points remind readers that standard form contracts (SFC) are not new. They have had a very positive role in making some legal issues manageable by the lay public and consumers that expert systems could augment (Susskind, 2008). However, her review argues that these SFC have been too slow to adapt to the digital context, such as in being too anchored to legacy paper-based forms. Moreover, she argues that the shift in medium has implications for the procedural process, which can pit the needs of consumers against the ideologies of business and industry. This need not be the case. She argues that smart contracts can be used to actually enhance the freedom of individuals to complete transactions online. In such ways, Cornelius provides insights about smart contracting in the digital context, such as in permitting more decentralised control, which might provide new approaches to such intractable issues as notice and consent.

## **POINTS OF SUMMARY AND CONCLUSION**

This brief editorial has sought to put the contributions to this special issue in a broader context and illuminate some of the relationships between the articles. While I have noted basic points of each contribution, I have avoided detailed summaries of their evidence and arguments. I therefore encourage you to read these contributions on their own terms, as each is succinct and useful in advancing the study of policy and regulation in the field of internet studies. That said, I found several themes relevant across these contributions which I will note as a personal observation. They all remain relatively anecdotal as they are tied simply to this sample of articles from one but nevertheless an important conference for the field of internet studies. Hopefully they will generate questions about whether they are more generally applicable.

## **DISCIPLINARY PERSPECTIVES**

First, it is arguable that each article is anchored in more or less of a disciplinary perspective, such as in sociology, science and technology studies (STS), computer ethics and law. It is remarkable in that internet studies and policy studies are purportedly more ‘interdisciplinary’ fields and yet these contributions are more grounded in disciplinary than interdisciplinary perspectives. And, from my point-of-view, each article makes an original contribution to internet and policy studies by virtue of bringing a disciplinary approach to bear on their topic. Rather than an interdisciplinary treatment of a topic, which might surface commonalities across disciplinary divides, these contributions tend to foreground the details and differences that might be overlooked in more general treatments. For example, we see comparisons across platforms for tracking big crisis data (Kappler, this issue), multiple implementations of the right to be forgotten (Calster et al., this issue), and four distinct approaches to cyber security (Fichtner, this issue).

Another consequence of these disciplinary approaches might have been the avoidance of a degree of advocacy that invades and undermines many policy-oriented pieces. The objective of each article is more tied to theorising or refining their theoretical or empirical approach than advocating a particular policy or practice. In many ways, this leads to analyses that can be useful to the design of policy and practice by those from multiple positions on any given issue. For

example, whether you support or oppose initiatives on the right to be forgotten, it is extremely useful to know that this right differs across legal jurisdictions in ways not well recognised in general debates.

## **A GREENFIELD FOR HISTORICAL, LEGAL, SOCIAL AND CULTURAL THEORISING**

A greenfield in urban planning and development is ideal in that the developer does not need to grapple with all the constraints imposed by an existing built environment. In some respects, internet policy studies are theoretical greenfields for which theoretical ideas from many disciplines might prove valuable to explore. The contributions to this special issue, for example, underscore the degree that many theoretical approaches from cultural studies and the social sciences could be valuable to relatively under-theorised areas of internet policy studies. Work in this area is so new and so under-researched and theorised that prevalent perspectives, such as STS, have much to add to the literature. For instance, histories of the internet and internet policy and regulation have only become foci for serious historical research in the last decade, as the internet has become recognised as central to information societies in the digital age (Haigh et al., 2015). Perhaps this issue can be a call for historians, legal scholars, critical cultural theorists and social scientists across a variety of disciplines to bring their theoretical perspectives to bear on this new empirical terrain.

## **NEED FOR INTERDISCIPLINARY PROBLEM-SOLVING**

Multidisciplinary research is used here to refer to bringing together research anchored in specific disciplines. In contrast, interdisciplinary research refers to research that is at the intersections of disciplines or which is a synthesis of disciplinary perspectives. It does not mean a lack of or no discipline or an 'indiscipline' (Shrum, 2005). That said, at the end of the day, internet policy is inherently a problem-oriented field (Dutton, 2013). How to inform and stimulate debate on policy and regulation appropriate to mitigating problems with such issues as junk news, big data, encryption, the right to be forgotten, cyber security, and notice and consent are likely to require interdisciplinary thinking. But that does not require every study or every paper to be anchored in interdisciplinary research. As just noted above, disciplinary enquiries can prove to be very useful.

Instead, it suggests that disciplinary research needs to be brought together within more interdisciplinary projects, teams and centres that can understand, work with, and appreciate the contributions across the disciplines. In fact, that may well be a role that special issues on policy can play for the field of internet studies. The contributions to this special issue certainly demonstrate the value of systematic and critical disciplinary research to address the validity of key issues and concerns over the policy implications of the internet and related media, information and communication technologies.

## REFERENCES

- Beniger, J. R. (1986). *The control revolution*. (Cambridge, MA: Harvard University Press).
- Benner, K., and Lichtblau, E. (2016, March 28). U.S. says it has unlocked iPhone without Apple. *New York Times*. Retrieved from <https://www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html>
- boyd, d. m. (2008). *Taken Out of Context: American Teen Sociality in Networked Publics* (Phd Dissertation). University of California, Berkeley. Retrieved from <https://www.danah.org/papers/TakenOutOfContext.pdf>
- Braman, S. (2009). *Change of state: information, policy, and power*. Cambridge, MA: MIT Press.
- Castells, M. (1996). *The Rise of the Network Society: The Information Age*. Oxford: Blackwell Publishers.
- National Research Council. (2014). *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues*. (D. Clark, T. Berson, & H. S. Lin, Eds.). Washington, DC: National Academies Press. doi:10.17226/18749
- Consalvo, M., & Ess, C. (Eds.). (2011), *The Handbook of Internet Studies*. Oxford: Wiley-Blackwell.
- Cranor, L. F., & Wildman, S. S. (Eds.). (2003). *Rethinking Rights and Regulations*. Cambridge, MA: MIT Press.
- de Sola Pool, I. (1983). *Technologies of Freedom*. Cambridge, MA: Harvard University Press.
- Deibert, R., Palfrey, J., Rohozinski, R., Zittrain, J. (Eds.). (2008). *Access Denied: The practice and policy of global internet filtering*. Cambridge, MA: MIT Press. Available at <https://mitpress.mit.edu/books/access-denied>
- Deibert, R., Palfrey, J., Rohozinski, R., Zittrain, J. (Eds.). (2010). *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*. Cambridge, MA: MIT Press. Available at <https://mitpress.mit.edu/books/access-controlled>
- DeNardis, L. (2009). *Protocol politics: the globalization of internet governance*. Cambridge, MA: MIT Press.
- DeNardis, L. (2013). The emerging field of internet governance. In W. H. Dutton (Ed.), *The Oxford Handbook of Internet Governance* (pp. 555-575). Oxford: Oxford University Press.
- Dutton, W. H. (1999). *Society on the Line*. Oxford: Oxford University Press.
- Dutton, W. H. (2009). The fifth estate emerging through the network of networks, *Prometheus*, 27(1), 1-15. doi:10.1080/08109020802657453
- Dutton, W. H. (2013). Internet Studies: The Foundations of a Transformative Field. In Dutton, W. H. (Ed.), *The Oxford Handbook of Internet Studies* (pp. 1-23). Oxford: Oxford University Press. Available at: <http://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780199589074.001.0001/oxfordh>

b-9780199589074-e-1

Dutton, W. H. (2015). Putting Policy in its Place: The Challenge for Research on Internet Policy and Regulation. *I/S: A Journal of Law and Policy for the Information Society*, 12(1), 157-84. Retrieved from <http://moritzlaw.osu.edu/students/groups/is/files/2016/09/10-Dutton.pdf>

Dutton, W. H. (2018, March 21). Regulating Facebook Won't Prevent Data Breaches, *The Conversation*. Retrieved from <https://theconversation.com/regulating-facebook-wont-prevent-data-breaches-93697>

European Commission, Directorate-General for Communication Networks, Content and Technology. (2018). A multi-dimensional approach to disinformation: report of the independent high level group on fake news and online disinformation. Brussels: European Union. doi:10.2759/739290 Retrieved from <https://www.cato.org/publications/policy-analysis/risky-business-role-arms-sales-us-foreign-policy>

Gerbner, G., Gross, L., Morgan, M., & Signorielli, N. (1986). Living with Television: The Dynamics of the Cultivation Process. In J. Bryant & D. Zillman (Eds.), *Perspectives on Media Effects*. Hilldale, NJ: Lawrence Erlbaum Associates.

Graham, M. (2014). Internet Geographies: Data Shadows and Digital Divisions of Labor. In M. Graham & W. H. Dutton (Eds.), *Society and the Internet* (pp. 99-116). Oxford: Oxford University Press.

Greenwald, G. (2014), *No Place to Hide*. New York: Metropolitan Books.

Haigh, T., Russell, A. L., & Dutton, W. H. (2015). Histories of the Internet: Introducing a Special Issue of *Information & Culture*. *Information & Culture*, 50(2), 143-159. doi:10.7560/IC50201

Hardie, T., Cooper, A., Chen, L., O'Hanlon, P., & Zuniga, J. C. (2014). *Pervasive surveillance of the internet: Designing privacy into internet protocols*. IEEE 802 Tutorial. Retrieved from <https://mentor.ieee.org/802-ec/dcn/14/ec-14-0043-01-00EC-internet-privacy-tutorial.pdf>

Hargittai, E. (2002) Beyond logs and surveys: In-depth measures of people's web use skills. *Journal of the Association of Information Science and Technology*, 53(14), 1239-1244. doi:10.1002/asi.10166

Howard, P. N. (2015). *Pax Tehnica: How the Internet of Things May Set Us Free or Lock Us Up*. New Haven, Connecticut: Yale University Press.

International Commission for the Study of Communication Problems (Ed.). (1980). *Many voices, one world: communication and society, today and tomorrow: towards a new more just and more efficient world information and communication order*. Paris; London; New York: UNESCO; Kogan Page; Unipub.

Jones, D., & Simons, B. (2012), *Broken ballots: Will your vote count?* Stanford, CA: CSLI Publications.

Kahin, B., & Wilson, E. (Eds.). (1997). *National information infrastructure initiatives: Vision and policy design*. Cambridge, MA: MIT Press.

Keen, A. (2007). *The Cult of the Amateur*. New York: Doubleday.

- Keen, A. (2015). *The Internet is Not the Answer* London: Atlantic.
- Laudon, K. (1977). *Communications Technology and Democratic Participation*. New York: Praeger.
- Leigh, D., & Harding, L. (2011), *WikiLeaks*. London: Guardian Books.
- Mayer-Schönberger, V. (2009). *Delete: The Virtue of Forgetting in the Digital Age*. Princeton and Oxford: Princeton University Press.
- McLuhan, M. (1964). *Understanding Media: The Extensions of Man*. London: Routledge.
- Mendel, T., Puddephatt, A., Wagner, B., Hawtin, D., & Torres, N. (2012). *Global survey on internet privacy and freedom of expression*. Paris: UNESCO.
- Morozov, E. (2011). *The Net Delusion: How Not to Liberate The World*. New York: Allen Lane.
- Mueller, M. L. (2002). *Ruling the root: Internet governance and the taming of cyberspace*. Cambridge, MA: MIT Press.
- Norris, P. (2001). *Digital divide: Civic engagement, information poverty, and the internet worldwide*. Cambridge, UK: Cambridge University Press.
- Pariser, E. (2011). *The Filter Bubble*. New York: Penguin.
- Pressman, J. L., & Wildavsky, A. (1973). *Implementation*. Berkeley, CA: University of California Press.
- Rainie, L. & Wellman, B. (2012). *Networked: The New Social Operating System*. Cambridge, MA: MIT Press.
- Schotz, M. (2018, March 17). Cambridge Analytica Took 50M Facebook Users' Data – And Both Companies Owe Answers, *Wired*. Retrieved from: <https://www.wired.com/story/cambridge-analytica-50m-facebook-users-data/>
- Shrum, W. (2005). Internet indiscipline: Two approaches to making a field, *The Information Society*, 21(4), 273-5. doi:10.1080/01972240591007599
- Sunstein, C. R. (2017). *#republic: Divided Democracy in the Age of Social Media*. Princeton, NJ: Princeton University Press.
- Susskind, R. (2008). *The End of Lawyers?* Oxford: Oxford University Press.
- United Kingdom Digital, Culture, Media and Sport Committee. (2017). *Fake news inquiry - publications*. Retrieved from: <https://www.parliament.uk/business/committees/committees-a-z/commons-select/digital-culture-media-and-sport-committee/inquiries/parliament-2017/fake-news-17-19/publications/>
- Wellman, B. (2004), The Three Ages of Internet Studies, *New Media & Society*, 6(1), 123-129. doi:10.1177/1461444804040633
- Williams, F. (1982), *The Communications Revolution*. Beverly Hills, CA: Sage.
- World Internet Stats (2018), *World internet user statistics*. Retrieved from

<https://www.internetworldstats.com/stats.htm>

Wu, T. (2003), Network neutrality, broadband discrimination, *Journal of Telecommunications and High Technology Law*, 2, 141–179.□

#### FOOTNOTES

1. See AoIR website for more information: <https://aoir.org/about/>