

# **Technoliberalism in Iceland: The Fog of Information Infrastructure**

Julian von Bargen  
York University

Adam Fish  
University of New South Wales

## **ABSTRACT**

**Background** *In the wake of the 2007–2008 financial crisis in Iceland, some citizens believed the calamity was the outcome of a cultural of secrecy among the political and financial elites.*

**Analysis** *By examining an effort to legislate for a “data haven” in Iceland, this article discusses a shift in how data activists attempted to achieve data justice. This shift challenges existing ideas about cyberlibertarian and technoliberal approaches to social change. In attempting to address the inequalities inherent to the centralization of data and the internet, data activists moved away from advocacy and adopted two previously rejected strategies: formal political organizing and territorial authority.*

**Conclusion and implications** *Activism for data equity was insufficient to counter existing data power in Iceland. What comes after technoliberalism?*

**Keywords** *The internet; Information and media reform; Data activism; Data justice; Data power; Technoliberalism; Cyberlibertarianism*

## **RÉSUMÉ**

**Contexte** *Suivant la crise financière de 2007-2008 en Islande, certains citoyens se mirent à penser que ce désastre était le résultat d'une culture du secret parmi les élites politiques et financières du pays.*

**Analyse** *Par l'examen d'efforts pour légiférer un « havre de données » en Islande, cet article discute d'un changement dans la manière dont des militants ont tenté d'établir un accès plus juste aux données. Ce changement pose un défi à des idées courantes prônant une approche cyberlibertaire et technolibérale envers le changement social. Les militants, en tentant de s'adresser aux inégalités inhérentes à la centralisation des données et d'internet, se sont éloignés du plaidoyer pour adopter deux stratégies rejetées antérieurement : l'organisation politique formelle et l'autorité territoriale.*

**Julian von Bargen** is a PhD candidate in the Department of Politics at York University, Toronto, ON. Email: [jvonbargen@protonmail.ch](mailto:jvonbargen@protonmail.ch). **Adam Fish** is a Scientia Fellow in the School of Arts and Media at the University of New South Wales, Sydney, Australia. Email: [mediacultures@protonmail.ch](mailto:mediacultures@protonmail.ch).

**Conclusion et implications** *Le militantisme pour l'égalité des données s'est avéré insuffisant pour démocratiser le contrôle des données en Islande. Dans ces circonstances, qu'est-ce qui pourrait suivre au technolibéralisme?*

**Mots clés** *Réforme de l'information et des médias; Militantisme pour les données; Justice pour les données; Pouvoir des données; Technolibéralisme; Cyberlibertarisme*

## Introduction

As Rob Kitchin and Tracey Lauriault (2014) observe, though “data” have always been part of social and technological systems, in the last few decades there has been a significant increase in the volume, velocity, variety, and interoperability of data generated, and one of the key enablers is the internet. Moreover, there was a time when the state was the primary generator of data. Today, however, a diverse set of networked digital information technologies produce big data. They are put to use by a diverse set of public and private sector organizations increasingly responsible for the remediation and datafication of many aspects of everyday life, although who gets access to what data and for what purpose is unresolved. Understanding the bundle of devices, applications, networks, and infrastructures that facilitate internet connectivity, this article argues, is, therefore, also central to understanding the prospects for data justice.

Here data justice is understood as the restoration of user control over the data that people generate about themselves, the data that others generate about them, and the reclamation of the ownership of the data generated by the digital technologies that people use to go about their daily lives. In other words, data justice is about the equitable distribution, access, control, and ownership of data generated by and circulated over the internet. Data justice also includes transparency, such as the right to an accurate public record of the behaviours and beliefs of decision-makers. This definition is based on the work of Lina Dencik, Fieke Jansen, and Phillipa Metcalfe (2018) at the Data Justice Lab, where data justice is framed within the discourse and practice of social justice, and Linnet Taylor (2017), who connects digital rights and freedoms to data justice. In this article, data power and data justice are treated as a relation, an “historical and on-going struggle over power dynamics and the organisation of society” (Dencik, Jansen, & Metcalfe, 2018, section 4, para 1).

State and corporate control over the capacities to shape society inherent to the affordances of information technologies and the data they produce are the main challenges to data justice (Beniger, 1986). The current trend is toward centralization and digital enclosure: the aggregation of computational power and data in fewer and into large centralized server farms, also known as data centres, which enable cloud computing and condense data in the hands of a few owners. The growth of data and server centres is crucial to understanding the changing power relations of connectivity to the internet because with the centralization of content and computational power, more control is also given to cloud providers.

This movement toward centralized control is unsurprising considering that data are instruments in power relations as “they count the symbolic, they index the real, and, once combined and coordinated, they manipulate the social imaginary” (Peters, 2016, p. 94). Data power is, therefore, related to the consolidation of authority via the centralization of the mechanisms of measurement and categories to support and ex-

tend existing configurations of state and corporate power (Beniger, 1986). There may have been a time when connectivity promised horizontal hierarchies and greater individual autonomy and data justice. Today, however, corporate platforms are enacting new forms of enclosure and more centralization (Mansell, 2017; Mosco, 2014). Enclosure here refers to different strategies aimed at privatizing, controlling, and commodifying data flows, including intellectual property generated in interactive, online spaces wherein, “every action, interaction, and transaction generates information about itself” (Andrejevic, 2009, p. 53).

Centralization is complicated, however, since the processes of enclosure occur within an infrastructure that is heterogeneous, layered, and a non-unified whole. Heterogeneity is important because connectivity brings users into a set of similar relations with state and corporate power spread across subsystems and component parts of the internet. These relations involve users and mobile device manufacturers, users and software companies, and users and their internet service provider. Understanding these social and technical power relations is crucial and challenging for those who aim to study data power and who want to enact data justice.

This article investigates a data justice project involving the Icelandic Pirate Party (IPP) and examines what strategies organizers adopted to win legal reforms and overcome the obstacles they encountered, and how this was related to the evolution of the data activist movement. The study suggests that different contestations over digital networks led activists to consider a more formalized type of political organization to win state power and to counter the ongoing enclosure and centralization of data in the hands of a few corporate and state organizations. This struggle over data foregrounded how activists began to understand the importance of using legislation and gaining control of internet infrastructure.

### **Data activism**

A growing literature points to actions that can be ascribed as forms of data activism (Postill, 2018). Here, a data activist is distinguished from an activist that uses data. Data activists deploy technological and legal skills to win reforms to protect freedom of expression, make state institutions more transparent, and contest restrictive intellectual property regimes. According to Jessica Beyer (2014), these kinds of data activists are inspired by a hacker ideology, or cyberlibertarianism, that argues against any restriction on the transmission of information (Levy, 1984). Pirate parties such as the one in Iceland are political parties that organize around technoliberal ideals, such as the belief that technology can ameliorate the contradiction between social welfare and economic liberalism (Fish, 2017). Technoliberals, for example, might argue that the internet can create a common space or a platform for both markets and free speech and some state reforms are required to enable this.

### **Case study**

This case study explores the ways in which data activists in Iceland attempted to leverage the spatial location of components and subsystems of the internet. The objective was to examine and assess the data justice arguments developed by Dencik, Jansen, and Metcalfe (2018). Sites of action for the interviewees—who aimed to bring about

substantive democratic reform, economic rejuvenation, and data justice in Iceland—were selected as locations. Where the internet was located was important because it allowed, in this case, for sovereign laws to regulate global flows across the internet infrastructure. Laws and regulations jurisdictionally apply to where the cloud touches the ground in real and material terms. We spoke with actors involved with data justice in Iceland, people related to the Icelandic Modern Media Initiative (IMMI) who challenged the existing data power relations that structured the media landscape and undermined mechanisms for government accountability leading up to the 2007–2008 financial crisis (Cohen, 2010; Greenberg, 2012). Attempting to overcome these relations ultimately transformed the basic structure of the data activist movement in Iceland from social movement activists to a formal political party. We interviewed data activists involved in the IMMI between 2013–2015. The IMMI was a parliamentary resolution unanimously passed by the Icelandic Parliament on June 16, 2010, that aimed to make Iceland a data and media haven, with the objective of protecting freedom of expression, freedom of information, and privacy. Although the IMMI no longer exists, it is important to study this initiative because its evolution demonstrates how the centralization of the internet shifted the strategies deployed by the data activists we interviewed.

### **The Icelandic Modern Media Initiative (IMMI)**

The IMMI began not as an institution but an initiative. The initiative stemmed from a 2010 parliamentary resolution that tasked the Icelandic government with updating more than a dozen laws, including protections for whistleblowers and journalistic sources, the protection of digital intermediaries such as Web hosts, media protections from “libel tourism,” and modernizing the information freedom act. Libel tourism is the act of suing a writer for alleged defamation in a legal jurisdiction with weak libel laws. The goal of the initiative was the creation of a data haven, which is a place to protect fundamental civil rights related to privacy, access to information, media and service provider protections, and freedom of expression. As Birgitta Jónsdóttir, chief sponsor of the bill, put it, Iceland would become “the inverse of a tax haven; by offering journalists and publishers some of the most powerful protections for free speech and investigative journalism in the world. Tax havens aim is to make everything opaque. Our aim is to make everything transparent” (IMMI, n.d., pg.1, para.2).

Jónsdóttir was an early contributor to WikiLeaks, a pro-transparency publisher, one of the co-founders of the IPP, and the parliamentary sponsor of the IMMI legislation. Fellow IPP co-founder, WikiLeaks colleague, and interview participant Smari McCarthy and Jónsdóttir were the two most important contributors to the IMMI. McCarthy expanded Jónsdóttir’s vision for Iceland by explaining that with the introduction of updated “information legislation,” “data centres would be required to follow these laws but these laws are [more] about protecting data centres ... [than] regulating them” (S. McCarthy, interview, July 25, 2015). This is one of the essential components of protecting access to information on the internet. The point was that “you want to make a clear separation between the people who are hosting the data and the people who are creating it” (S. McCarthy, interview, July 25, 2015). This way, it was stated that “when we have any kind of situation where there are source protection issues, or leaked data, or data that, for some reason, somebody wants not to be available to the public,

then you need to protect the entire chain from the source of this information” (S. McCarthy, interview, July 25, 2015).

For internet scholar Arne Hintz (2013), an important condition for the success of the IMMI was the policy window that opened following Iceland’s financial collapse. With “parts of the old political class ... delegitimized, new social actors were swept into politics, and th[e] traditional policy monopolies were broken” (p. 159). In other words, the financial collapse created an opportunity to renew the political order in Iceland.

The IMMI legislation was a response to the complicity of the media and the dominant political class in the crash. As Guðjón Idir, executive director at IMMI, remarked, the media environment in Iceland was not independent and lacked the capacity to report critically on the ruling class (G. Idir, interview, July 20, 2015). This is illustrated in a few high-profile attempts by political and financial elite to censure the press. First, Kaupthing Bank, one of the three Icelandic banks at the centre of the financial collapse, filed an injunction to prevent the RÚV (Iceland’s national news broadcaster) from reporting on leaked internal documents from the bank that revealed massive fraud, prompting a wave of public outrage. The documents were made available to the public by WikiLeaks. Later, in January 2009, editors at the TV station Stöð 2 prevented their reporters from airing a story about the same bank and its relationship to a property entrepreneur later implicated in the loans fraud scandal that came to light after the collapse. As reported, “the program, *Kompás*, was not aired, and its entire staff promptly fired” (Þóroddsdóttir, 2011, para 45). This suppression of information for the benefit of powerful financial actors was characteristic of the Icelandic media ecosystem leading up to the financial crash (Anderson, 2010). For data activists, the antidote was the IMMI.

The IMMI could also have economic implications (G. Idir, interview, July 20, 2015; B. Jónsdóttir, interview, July 23, 2015). It was to be the basis for economic rejuvenation (Ziccardi, 2013). Passing privacy- and media-friendly legislation might also have combined Iceland’s comparative advantage as a cool northern island ideal for data storage with a legal and technical infrastructure that promised a comprehensive, innovative ecology that could nurture fundamental civil rights related to privacy and access to information (Greenberg, 2012). As Idir explained, IMMI “will prove more favourable for companies in the tech and media industries to relocate parts of their operations to Iceland to benefit from the jurisdictional protections, and we have already seen data centres [have] moved to Iceland even though the legislative protections aren’t in place” (G. Idir, interview, July 20, 2015). The result would have been to have a globally connected data justice hub. The idea was to have data centres built by domestic and foreign companies in Iceland and their international clientele would be protected by the same legal framework. Meanwhile, because the global niche for ethical data storage required strong protections for civil rights, Iceland’s democratic system, newly enriched by a citizenry adequately equipped to assess its representatives and to participate, was thought to be able to safeguard these centres and their data.

Several questions remained. Was the old political class so delegitimized that it would and could not reassemble? Was it enough to defeat Iceland’s dominant political party, the Independence Party, in a single election in order to transform Iceland into a

data justice haven? What would it have taken to transform Iceland's media environment into a global leader as a data activist? Hintz's (2013) optimistic analysis was not unique, as even the creators of the IMMI initiative originally estimated the reforms would only take a few years. Unfortunately, almost none of the laws proposed to increase transparency were enacted, which later meant the initiative was not viable.

Today the IMMI is a small institute devoted to collecting laws for engineering an open, participatory legal and technical architecture for freedom of expression in a digital world. As its website explains, IMMI (n.d.) exists to "bring together the best functioning laws in relation to freedom of information, expression and speech, reflecting the reality of [a] borderless world." Jónsdóttir explained the transformation, stating that the IMMI found new life "as a database for all the best laws and praxis ... because those of us who are activists, we have to understand [that that is] the shortest route to change—that's what the lobbyists, the really good lobbyists do, they change the legal text" (B. Jónsdóttir, interview, July 23, 2015). This database of laws was to be a toolkit for data activists who won elections and took up new positions as lawmakers around the world.

The idea was that lawmakers might have wanted to also pass legislation to protect civil liberties, and the toolkit could be used to help them build a legal framework conducive to an open, transparent society. The IMMI provided a toolbox, including legal reforms based on "looking at the best practices from all over the world that actually work[ed], ... not best practices only on paper" (B. Jónsdóttir, interview, July 23, 2015). Jónsdóttir's reasoning was that policy windows, such as instances in which there is a breakdown in the political, economic, social, or ideological order (Hintz, 2013), that disrupt policy monopolies pass quickly. To take advantage of the opportunity, a repository of best laws and practices, it was thought, might help politicians operating in these small windows to effectively implement laws to strengthen press freedom and free speech. This was, in fact, one strategy data activists did take to try and strengthen freedom of expression and transparency in government. In addition to transforming the IMMI initiative into an institute, Jónsdóttir and McCarthy cofounded the IPP in November 2012.

Why? What happened to the initiative? The problem was twofold: first, overcoming the opposition to the data-haven vision for Iceland required more than forcing the prime minister to resign, criminally charging bankers, or even winning a seat in the Althingi, the national parliament of Iceland. Second, instead of a singular, universal, global, monolithic technology, the internet was thought of as an assemblage (Srinivasan & Fish, 2017). The internet assemblage includes cables, routers, protocols, applications, and devices. An assemblage is a collection of discrete, heterogeneous, and autonomous components that are related; it also includes related subsystems that, together, are a recognizable whole (Kitchin & Lauriault, 2014). The parts retain their heterogeneous interiority while entering relations with other component parts. For example, in Iceland data activists faced a variety of challenges including slow domestic internet speeds because all the cables connecting Iceland to the global internet were owned by a public-private monopoly, domestic internet access was controlled by a few phone companies, applications were owned by American corporations and subject to

American law, and media organizations unwilling or unable to criticize the decision makers. These component parts of the internet are often sites of different struggles about shaping the future of the internet. As these interviews reveal, these different sites of struggle required significant political clout, resources, initiative, and formal political structures to reform. In the beginning, the IPP approach was a form of technoliberalism. That is, many of the data activists and the Pirate Party of Iceland believed that networked technologies could resolve long-standing social problems by empowering individuals (Fish, 2017). The turn to formal political organizing reflected at the very least an extension—if not a shift away from—the horizontal, participatory, protest-movement activism that characterizes technoliberalism.

### **Struggles with/in technoliberalism**

Icelandic data activists were challenged with leveraging the main components and subsystems of the internet to catalyze media reform and economic development and restore trust through accountability in Icelandic politics after the financial collapse. The main challenges were existing data power relations, domestic politics, and the layered, heterogeneous, territorialized structure of the internet. These challenges offered insights into why the strategies data activists adopted to create a data haven changed over time. Data activists early on were inspired by arch-cyberlibertarian John Perry Barlow, whose 2008 talk at a digital freedoms conference in Iceland helped catalyze the idea of Iceland becoming “the Switzerland of bits” (Economist, 2010). Data activists in Iceland were not themselves cyberlibertarians.

Some clear commitment shared by Icelandic data activists that distinguished them from cyberlibertarians was their embrace of the role of the state as a regulator, protector of civil rights to free expression, an investor in research, and a fiscal supporter of the development and construction of networked technologies and infrastructure. The acceptance of this role by the state, however, was a rejection of a key cyberlibertarian principle, which is to repudiate any intervention of the state in the regulation of the global flow of data. Instead this was part of a larger shift in strategy that emphasized formal political organizing as necessary to win control of the state and to regulate global data flows by applying Icelandic law. This shift suggested that some of the data activists had moved away from or were expanding upon existing conceptions of the meaning of technoliberalism.

The following interviews illustrate an array of obstacles and adversaries the IMMI designers encountered in trying to actualize their vision for a data and transparency haven, and why data activists were forced to confront the limitations of both cyberlibertarianism and technoliberalism.

The most important goals of the designers of the IMMI initiative were to reform Iceland’s democracy and rejuvenate its economy following the 2007 financial collapse. They decided on a strategy to build a formal political party, contest elections, win elected positions in municipal and national governments, and use these positions to change laws. They did this, according to Jónsdóttir, because reforms had failed in the past since data activists “don’t go to the heart of it. We are like on the fringes and nobody really needs to talk to us, because we are so disorganized” (B. Jónsdóttir, interview, July 23, 2015). Jónsdóttir explained the need to organize formally as a political party,

win elections, and write new, better laws that protect the basic tenets of data justice, instead of merely protesting against injustices. She advocated for data activists to move beyond activism and protest movements.

Two other issues inspired the IMMI initiative. One, there existed a shared perception among key organizers that the internet was centralizing; and two, the heterogeneous, layered socio-technical assemblage known as the internet required intervention in different layers to achieve sought-after reforms. The centralization of the internet challenged the cyberlibertarian ideals because the ideology advocated for the importance of a decentralized internet in which any two users connected to the internet could share information without the permission of a third party. Yet, for data activists in Iceland, the centralization and enclosure of the internet also presented an opportunity.

Marius Ólafsson, chief technical officer for Internet Iceland Ltd (ISNIC), the top-level domain registry in Iceland, was one of the engineers who first connected Iceland to the internet. He was committed to a classic technoliberal model of the internet, as he considered it to be a decentralized, participatory, and peer-to-peer network that was also a platform for market access. According to Ólafsson, his ideal for an open internet was shattered when the telecom industry took over the internet infrastructure and began to centralize it and limit its social liberal potential. As Ólafsson put it,

[the protocol wars are a] very interesting story and it hasn't really come out yet because, this war is still being fought. TCP/IP [transmission control protocol/internet protocol] won all the battles but lost the war. ... The internet is owned by the phone companies today. ... The phone companies were absolutely, vehemently opposed to [TCP/IP]. They wanted the OSI [Open Systems Interconnections], client-side model, where they control everything, and you have a dumb pipe to your house, blah blah blah, this whole thing. And they absolutely wanted that, and they fought, that was the protocol wars for years. And we won all the battles and lost the war. (M. Ólafsson, interview, July 14, 2015)

The OSI model for the internet differed from the model idealized by Ólafsson and that reflected the early ideals of data activists. Similar to the internet, the OSI model was designed to facilitate interoperability between systems designed by different manufacturers. Despite this shared starting point between OSI and TCP/IP, according to many critics, OSI was a rigid, prescriptive abstraction inappropriate for internetworking the vast diversity of digital networks that began to emerge starting in the late 1970s (Russell, 2006). The International Organization for Standardization (ISO) developed the OSI because it recognized the importance of standardizing connections between networks (Russell, 2006). However, it imposed these standards in a slow, top-down manner that favoured the interests of major national telecommunications and computer companies (Russell, 2013).

French and American engineers, breaking from OSI and the ISO, developed the TCP/IP. Defenders of TCP/IP insisted that if the internet was to extend from the relatively small interconnected networks of universities, corporations, and states, theoretical top-down impositions of standards would never account for all the unpredictable and idiosyncratic ways people might want to use it. As the famous defender of TCP/IP

and early internet engineer David Clark put it, “we reject: kings, presidents, and voting” (as quoted in Russell, 2006, p. 49); TCP/IP was designed to facilitate a permissionless environment. In other words, Ólafsson’s vision for the internet was technoliberalism, whereby private individuals and small businesses standing shoulder-to-shoulder with the social, political, and corporate elite would each have their own space to truck, barter, and trade in the marketplace of bits.

This better frames Ólafsson’s thinking and concerns about OSI. What made the internet special for him was that all connectors could host their own content. The goal was to maintain the heterogeneity of the nodes and, for him, the OSI model prescribed against this ideal. As Ólafsson explained,

Before the phone companies took it over, there was no concept on the internet as a client and a server. Every client is a server and every server is a client. And there is this parity between the providers of information and consumers of information. And that parity was destroyed by the phone companies, because they said, “Ah, this is the connection to your home.” So basically, what you need is enough bandwidth to you but no bandwidth from you. Because you’re not going to provide any services, we are going to provide the services. And [it] has been going downhill ever since. (M. Ólafsson, interview, July 14, 2015)

Put another way, Ólafsson saw the OSI model as an attempt by the telecoms to enclose content and computational power. He worried that the OSI model reduced users to a passive audience. Users in the OSI model no longer had the necessary bandwidth to host their own information on their own websites or blogs. Instead, users were offered what amounted to a “dumb” terminal through which they accessed and passively consumed media provided by the ISPs. For Ólafsson, this meant that the technoliberal idea of empowered individuals exchanging information across a decentralized infrastructure had been replaced.

Jónsdóttir perceives a similar but different pervasive and dominant power relation underpinning existing internet connectivity: the United States. For Jónsdóttir, however, it was not merely about American power but about the “incredible” (B. Jónsdóttir, interview, July 23 2015) *de jure* data power, that is the legal sovereign authority that accrues to different national security organizations in the U.S. because American corporations own many of the world’s most popular cyberspaces and cable/cloud infrastructures, and they are subject to American law. As Jónsdóttir explained,

The fact of the matter is if you have your social media, or your digital shadow, whatever it is, it is much more than you ever think it is, then you cannot be protected by any country in the world if [your data] is hosted anywhere in the world by an American corporation, that’s the reality of the situation. (B. Jónsdóttir, interview, July 23, 2015)

To combat this centralization of data power by the U.S., the IMMI initiative was supposed to make Iceland a haven for data justice that could resist U.S. data power. By leveraging territorial sovereignty, the hope was that sovereign law could be exercised to resist the *de jure* right of the U.S. to legally surveil people globally by using software,

devices, and/or infrastructure owned by American corporations. As Jónsdóttir succinctly put it, “without the law you are, to put it mildly, fucked” (B. Jónsdóttir, interview, July 23, 2015). She suggested passing legislation that would attempt to protect the right of Icelandic citizens—and most importantly any individuals storing their information in data centres in Iceland and to keep their information and communications private from intrusion and collection by any state actor. The *de facto* power of the U.S., with its military and financial power relative to Iceland’s, could not be ignored. Unsurprisingly, in spite of this technoliberal ideal, technology did not solve this problem. Sovereign law was considered to be a necessary form of power to be exerted in this case.

Jónsdóttir’s thinking marked another serious shift in data activism. Barlow and other early technology visionaries believed in an internet that was singular, universal, and existed outside of culture and territory. As Barlow (1996) wrote in his famous manifesto directed at the governments that were then trying to regulate the internet, “[Cyberspace] is a world that is both everywhere and nowhere, but it is not where bodies live” (p. 6). He continued: “Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is no matter here” (p. 7).

McCarthy, Jónsdóttir, and also Jason Katz, another co-founder of the IPP and early contributor to WikiLeaks, did not share this belief. In a 2012 report, for instance, McCarthy (2012) argued for the opposite. He wrote that “locale is rapidly becoming one of the most important competitive differentiators in the provision of cloud-based information technology services” (p. 4). He reiterated much the same in an interview:

The reality is that different countries around the world do have different laws about all of these issues. About issues like net neutrality and about issues like, simply, what is legal to publish. In some countries pornography is legal and in other countries you have every kind of variation more or less. You need to accept the fact that that means, because we still have the concept of the nation-state, we’re going to have [to] deal with all of these inter-jurisdictional conundrums that come up over the next several decades. (S. McCarthy, interview, July 25, 2015)

McCarthy and Jónsdóttir understood that the internet was not singular or monolithic but differentiated by nation states, cultures, politics, and economics. They also realized that as the internet centralized, and in particular as computational power and data converged in centralized data centres, protecting these centres from threats to remove certain content or breaches in privacy became an opportunity for a form of data justice. Protests and activism were no longer enough, and instead it became clear that collective political action by an organized, formal political party could win political power and secure collectively held data and computational capacity with state jurisdictions.

Katz picked up from Jónsdóttir and McCarthy and wanted to move beyond simply building a data haven with legal reforms. According to Katz, the challenge was,

How do you create, how do you change the world more toward a direction where for the last ten years its been moving against that. Against freedom of speech, against freedom of ideas, against people expressing themselves because they are afraid of expressing themselves the wrong way... You’ve

got to make an example, you've got to make a pilot, somewhere. How do you make a pilot out of a country? You go to a really small country maybe and you see if it works. (J. Katz, interview, July 13, 2015)

To be clear, his concerns here were not that “political correctness” was leading to self-censorship. Katz was concerned about the intimidation of journalists, whistleblowers, and activists by state and corporate forces. He thought these problems could not be addressed with only legal reforms. Rather, resolution required the construction of a protective “stack” (J. Katz, interview, July 13, 2015). This stack rests on the legal because it:

Allow[s] the rest of the technical and cultural measures to be put into place. Why are Swiss bank accounts secure? Yeah, because they have legal enshrinement but also, you're going to ask about my clients' bank accounts in Switzerland? I'd never do that because that's my professional pride. You wrap it up into a facet of other factors and now it is much harder to overcome. (J. Katz, interview, July 13, 2015)

The intertwining of these different components of the stack to strengthen protections was essential for Katz. His ideas complemented reforms sought by Jónsdóttir but were not the same. Where Jónsdóttir's concern was with implementing laws that protect data centres and citizens from surveillance, Katz's focus was on the *de facto* data power of the U.S. His concern was that even if laws were in place, the power of the U.S. could force Icelandic lawmakers to break the law in order to comply with its demands.

Katz raised a second challenge to the data-haven ideal, one related to internet connectivity. For Katz, even with a completely implemented IMMI initiative but without reasonably priced, high-speed internet in and out of Iceland, the country would struggle to develop a data centre industry. For Katz the problem was Farice, a mostly state-owned telecommunications provider, that dominated Iceland's connection to the global internet. As he put it:

Iceland's thing that is holding it back with most hosting services is transit pricing. ... We thought this cable was coming. ... I was very hopeful. It's dead. Effectively it's dead. Because it costs a huge amount of money to run submarine cables anywhere. ... How do you run a \$100,000,000 cable unless you're Google or you're Facebook; they funded their own?... Iceland is very costly for transit compared to the rest of the world. Very costly even to own a domain name here. So why wouldn't you go to Germany? (J. Katz, interview, July 13, 2015)

Katz did not explicitly advocate for the Icelandic state to fund a cable, but he did appreciate the huge capital investment required to introduce competition into the Icelandic market. Farice was the major provider of international connectivity in Iceland. Katz was essentially making a technoliberal argument for the state to intervene with business-friendly market reforms to force competition and drive down transit fees. If it does this, he thought, the state could also protect digital civil liberties and provide data justice. Otherwise, the data haven would never attract customers and the whole project would be moot. In contrast to Ólafsson, who idealizes the natural exchange between individuals, Katz encourages competition.

Taken together, this set of interviewees highlighted three main obstacles to data justice in Iceland and around the world: 1) the importance of place, 2) the centralization of the internet, and 3) local and international social and political forces that possess data power. These obstacles countered the assumptions and strategies of technoliberal data activists in Iceland.

## **Conclusion**

In Iceland after the financial crisis of 2008, data activists advocated for governmental transparency and media reform. These reforms were influenced by much emancipatory rhetoric around data and networked digital information technologies. Internet connectivity was also supposed to catalyze mass participation and inform collective decision-making. In Iceland this thesis seemed on the verge of becoming a reality. Ultimately, however, activist led, data-driven, technologically savvy advocacy to transform Iceland into a hub for data justice was insufficient because it was unable to overcome existing political and economic interests that had long dominated Icelandic politics and internet infrastructure. Normative claims and technological design were not enough to counter the centralization and privatization of critical internet resources. Where many had previously been committed to horizontal grassroots and media activism, their encounter with social and technological political economic forces in Iceland, as well as their confrontation with global data power in the U.S., instead led to new strategies that saw the centralization and territorialization of the internet as an opportunity.

This research demonstrates that data activists were aware of the centralization of the internet and the data power relations at the core of connectivity. Jónsdóttir, Ólafsson, Katz, and McCarthy discussed different facets of centralization. Jónsdóttir was concerned with American data power based in U.S. law. For Ólafsson, TCP/IP's lost "war," as he called it, against the telecoms and their OSI model represented the defeat of a decentralized, democratic, and open internet. For Katz, the struggle was to compel a state-corporate monopoly to introduce competition and lower the cost of data transmission. Each pointed to different obstacles existing in different layers or "stacks" of the internet. Similarly, centralization for them was also an opportunity, albeit for different reasons. For McCarthy, the focus was to leverage the differentiated space brought together by a global internet to build a hub for data justice. For Jónsdóttir, a political party that took power rather than one that protested from the fringes could tinker with and create laws to protect data justice. For Katz, centralizing data and computational capacities in data centres protected by data justice laws could allow the Icelandic economy to transform and thrive as part of a just networked future.

For data justice to materialize, entrenched data power needs to be contested. Contestations over the internet are not homogenous, just as the internet is heterogeneous. This means different component parts and subsystems of the internet contain their own contests over data power. In Iceland, the data justice movement was not powerful enough to counter existing data power. This realization of the importance of the control over information infrastructure, as well as the implications of the heterogeneous materiality of the internet are part of the reasons for the rise of the Pirate Party and the IMMI in Iceland during the period following the global financial crisis.

## Research interviews

- Idir, Guðjón. (2015, July 20). Reykjavik, Iceland  
 Jónsdóttir, Birgitta. (2015, July 23). Reykjavik, Iceland.  
 Katz, Jason. (2015, July 13). Reykjavik, Iceland.  
 McCarthy, Smari. (2015, July 25). Reykjavik, Iceland.  
 Ólafsson, Marius. (2015, July 14). Reykjavik, Iceland.

## References

- Andrejevic, Mark. (2009). Privacy, exploitation, and the digital enclosure. *Amsterdam Law Forum*, 1(4), 47–62. URL: <https://ssrn.com/abstract=1509361> [January 26, 2020].
- Anderson, Anna. (2010, October 8). The watchdog that didn't bark. *The Reykjavik Grapevine*, 8(Oct 1–Nov 3). URL: <https://grapevine.is/mag/feature/2010/10/08/the-watchdog-that-didnt-bark/> [January 26, 2020].
- Barlow, John Perry. (1996). *A declaration of the independence of cyberspace*. URL: <https://www.eff.org/cyberspace-independence> [June 17, 2019].
- Beniger, James. (1986). *The control revolution: Technological and economic origins of the information society*. Cambridge, MA: Harvard University Press.
- Beyer, Jessica. (2014). The emergence of a freedom of information movement: Anonymous, Wikileaks, the Pirate Party, and Iceland. *Journal of Computer-Mediated Communication*, 19(2), 141–154. doi:10.1111/jcc4.12050
- Cohen, Noam. (2010, February 21). A vision of Iceland as a haven for journalists. *The New York Times*. URL: <https://www.nytimes.com/2010/02/22/business/media/22link.html> [April 4, 2019].
- De Filippi, Primavera, & McCarthy, Smari. (2012). Cloud computing: Centralization and data sovereignty. *European Journal for Law and Technology*, 3(2), 1–26.
- Dencik, Lina, Jansen, Fieke, & Metcalfe, Phillipa. (2018). A conceptual framework for approaching social justice in an age of datafication. *The Data Justice Project*. URL: <https://datajusticeproject.net/2018/08/30/a-conceptual-framework-for-approaching-social-justice-in-an-age-of-datafication/> [April 5, 2019].
- Economist. (2010, June 17). The Switzerland of bits: A conversation with one of the authors of a press law approved this week by Iceland's parliament. *Economist*. URL: <https://www.economist.com/babbage/2010/06/17/the-switzerland-of-bits> [April 8, 2019].
- Fish, Adam. (2017). *Technoliberalism and the end of participatory culture in the United States* [ebook]. Basingstoke, UK: Palgrave MacMillan. doi:10.1007/978-3-319-312569\_1
- Greenberg, Andy. (2012). *This machine kills secrets: Julian Assange, the cypherpunks, and their fight to empower whistleblowers*. New York, NY: Plume.
- Hintz, Arne. (2013). Dimensions of modern freedom of expression: WikiLeaks, policy hacking, and digital freedoms. In B. Brevini, A. Hintz, & P. McCurdy (Eds.), *Beyond WikiLeaks: Implications for the future of communications, journalism and society* (pp. 146–165), London, UK: Palgrave MacMillan.
- IMMI. (n.d.). *IMMI resolution*. URL: <https://en.immi.is/immi-resolution/> [June 17, 2019].
- Kitchin, Rob, & Lauriault, Tracey. (2014). Towards critical data studies: Charting and unpacking data assemblages and their work. In J. Eckert, A. Shears, & J. Thatcher (Eds.), *Geoweb and big data*. Lincoln, NE: University of Nebraska Press. URL: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2474112](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2474112) [January 26, 2020]
- Levy, Stephen. (1984). *Hackers: Heroes of the computer revolution*. Garden City, NY: AnchorPress/Doubleday.
- Mansell, Robin. (2017). Bit of power: Struggling for control of information and communication Networks. *The Political Economy of Communication*, 5(1), 2–29. doi:10.13140/RG.2.2.13321.44648
- Mosco, Vincent. (2014). *To the cloud: Big data in a turbulent world*. Boulder, CO: Paradigm Publishers.
- Peters, Benjamin. (2016). Digital. In B. Peters (Ed.) *Digital keywords: A vocabulary of information society and culture* (pp. 93–108), Princeton, NJ: Princeton University Press.
- Postill, John. (2018). *The rise of nerd politics*. New York, NY: Pluto Press.

- Russell, Andrew. (2006). Rough consensus and running code and the internet-OSI standards war. *IEEE Annals of the History of Computing*, 28(3), 48–61. doi: 10.1109/MAHC.2006.42
- Russell, Andrew. (2013, July 30). OSI: The internet that wasn't: How TCP/IP eclipsed the Open Systems Interconnection standards to become the global protocol for computer networking. *IEEE Spectrum*. URL: <https://spectrum.ieee.org/tech-history/cyberspace/osi-the-internet-that-wasnt> [June 17, 2019].
- Srivinasan, Ramesh, & Fish, Adam. (2017). *After the internet*. Cambridge, UK: Polity.
- Taylor, Linnet. (2017). What is data justice? The case for connecting digital rights and freedoms globally. *Big Data & Society*, 4(2). doi: 10.1177/2053951717736335
- Þóroddsdóttir, Valgerður. (2011, February 10). Information without borders: Iceland, WikiLeaks and the electronic frontier. *The Reykjavik Grapevine*, 2(February 4–March 10). URL: <https://grapevine.is/mag/feature/2011/02/10/information-without-borders/> [June 17, 2019].
- Ziccardi, Giovanni. (2013). *Resistance, liberation technology and human rights in the digital age*. New York, NY: Springer.