The power to structure: exploring social worlds of privacy, technology and power in the Tor Project

Ben Collier

School of Law, University of Edinburgh, Edinburgh, Scotland

Email: ben.collier@cl.cam.ac.uk
Twitter: @johnnyhistone

Acknowledgements:

I would like to thank the Tor community and all my interviewees for their generosity and kindness throughout this research. I would additionally like to thank my supervisors Richard Jones and James Stewart for their guidance and support, and to thank Jamie Buchan, Shane Horgan, Louise Brangan and Ben Matthews for their invaluable theoretical insights. I would also like to thank my colleagues in the Cambridge Cybercrime Centre and the staff and students in SPS at the University of Edinburgh who gave comments on the draft of this paper.

The power to structure: exploring social worlds of privacy, technology and power in the Tor Project

This paper contributes to the literature on resistance to power in information and communication networks. As Internet freedom movements build infrastructures to promote online privacy, they enrol types of technological work very different from that of the hackers and online protests which much of this research has covered (Coleman & Golub, 2008; Musiani, 2015). I explore the cultures of the wider forms of technical work involved in these struggles through a sociological study of the Tor Project, involving twenty-six qualitative interviews with people in the Tor community and extensive archival research in Tor's mailing lists and design documents. Tor is an online privacy infrastructure whose own practice of radical transparency makes it uniquely accessible, and it constitutes an example of a successful, widely-used infrastructure which directly undermines the centralisation of governmental power online. Tor is not united around a single worldview, instead exhibiting three distinct framings of its work. Using Star's (2010) social worlds framework, I characterise these three 'social worlds' of Tor. I argue that Tor has in the past accommodated its internal clashing perspectives through an ambiguity around politics and a shared construction of the users of Tor, which allow individuals to bridge and translate between these worlds. In recent years, this political ambiguity has become unsustainable. As Internet platforms and infrastructures extend further into social life around the world, so too are they being forced to come to terms with the shaping forces they exert on society and the values they represent. Tor is not exempt from this, and as it navigates these issues it is becoming increasingly mindful of its own relationships to power, values and politics.

Introduction: Tor, Internet freedom and hacker politics

The Internet has long been a site of political struggle. Its most vocal proponents and architects in its early days saw it as promoting liberation, allowing free access to information, and decentralising power (Yar, 2012). In fact, governmental power has proven extremely resilient. Use of the Internet in the present era necessarily brings one into contact with the mass-scale systems of surveillance which underpin the key governmental strategies used to discipline online space (Lyon, 2015). Simultaneously, the growth of 'surveillance capitalism', by which online services are provided for free through the collection and monetisation of personal data, has transformed the way we interact online (Zuboff, 2019). Issues of privacy and power are therefore at the forefront of debates about the politics of the Internet.

There is a substantial research literature on online privacy, including scholarship on governance and policy (Bennett & Raab, 2017), people's perceptions and experiences of privacy (Viseu, Clement & Aspinall, 2004; Lyon, 2017), and privacy's place in social and political life (Nissenbaum, 2009; Rider, 2018). The academic literature on privacy recognises that it is in fact composed of a range of related concepts and values (Solove, 2008) and understood very differently in different contexts and cultures (Nissenbaum 2009; Steijn & Vedder, 2015). Privacy is a core value through which liberal democracies construct their systems of government (though by no means exclusive to them) and underpins many of the conceptions of rights and public goods therein (Wright & Raab, 2014; Raab, Jones &Szekely 2015). As the mechanisms through which states and corporations govern the Internet expand to involve increasingly intimate surveillance of everyday life, the platforms and infrastructures of the Internet have become key sites of resistance, and these struggles are often framed around conceptions of privacy (Lyon 2015; Raab, Jones, & Szekely 2015)

In this research, I explore an attempt to create privacy through infrastructure, and describe how building privacy technologies necessitates bringing together conflicting understandings of privacy in practice. By conducting archival research and empirical qualitative interviews with members of the Tor Project, an organisation which develops the widely-used Tor anonymity network, I map out the different values, discourses, and understandings through which this community makes sense of Tor and privacy technology. I explore how these come together in conversation and conflict in the Tor community, and what this means for understanding infrastructures as sites of social action where constructions of privacy are worked out and realised.

The increasingly authoritarian governance of online space is matched by a burgeoning social movement of 'Internet freedom activists' (Marechal, 2015). This movement is increasingly involved in the creation of infrastructures that help users circumvent mass surveillance and censorship online (Marechal, 2015). Undoubtedly the most successful of these is the Tor anonymity network, accessed through the free, open source Tor browser, which provides strong security and privacy guarantees to its users. Whereas some privacy technologies aim to help everyday users of the Internet and others are expert tools for high-security use cases, Tor combines these, relying on being fast enough to attract large numbers of innocuous, privacy-conscious users which allow high-security users to 'hide in the crowd'. Tor encrypts user Internet traffic and the routing information it uses to get to its destination, bouncing this around three 'relays' chosen at random from a network of servers run by volunteers around the world, each of which decrypts one layer until the final 'exit' relay makes the link to the target website. In practice, Tor is fast enough for everyday use, and secure enough to frustrate all but the most well-resourced nation state adversaries' attempts to surveil or censor web traffic (Dingledine, 2004).

As well as a technical design, Tor also comprises an infrastructure (maintained by the network of volunteer 'relay operators' who bounce the signals of Tor users between their servers), an organisation (the Tor Project), and a community of activists, developers, maintainers and supporters who often contribute on a volunteer basis. This globally-dispersed community contributes resources to the network and to its vibrant public life, and Tor has developed a strong public identity. While there is a wide body of technical research on Tor (Dingledine, Matthewson & Syverson 2004; Murdoch & Danezis, 2005; Snader & Borisov, 2008), sociological and criminological research have largely focused on its users, and in particular its capacity for misuse (McCoy, 2008; Aldridge & Decary-Hetu, 2016). The few studies to tackle the Tor Project itself, in particular, the work of Marechal (forthcoming), and of Giel (2018), provide welcome explorations of its place in the Internet freedom activist movement and its attempts to cultivate legitimacy respectively. I identify three diverging ‘social worlds’ of understanding within the Tor Project, exploring how they work together and navigate conflicting understandings of privacy and politics. The paper concludes with an exploration of what happens when this détente is shaken by crisis, and how the Tor community navigated this change.

Exploring Tor through the social worlds framework: fieldwork, theory and methodology

The Tor Project has a core team of developers and other staff who contribute to the project, with individuals often performing a variety of roles. In addition, it is supported by a much wider community of volunteers who maintain its infrastructure, train users and support it in other ways. Fieldwork for this research was undertaken in 2017, involving qualitative, semi-structured interviews with twenty-six members of the Tor community. I interviewed a range of people from the core team and the wider community in person, via email and over online video chat. I aimed to interview members of the community with a spread of different roles and length of time with the Tor Project, including people from a range of genders and nationalities. My sample of interviewees was broadly reflective of the diversity of the Tor community. This included nine developers (from fairly new members of the Tor team to some who had been involved since its early days), three other core contributors to the Tor Project who were not developers, eight relay operators, three developers of Onion Services, and three other members of the broader Tor community. Based on the information available, nineteen of my participants identified as men and seven did not. My participants were based in a range of countries, including Australia, Canada, France, Germany, Greece, Italy, Russia, Spain, the UK, and the USA.

I also conducted extensive research in the Tor Project's online archives, analysing five years' worth of postings on their open-access development and community mailing lists. Although I focus on the interview data in this paper, this archival research also informs my analysis. This paper forms part of a larger research project on the Tor community and will be accompanied by other papers currently under submission (Collier, forthcoming A, B, C and D).

This research was cleared by the ethics board at the author's institution, and ethical considerations, particularly around anonymity and harm, were taken into account actively throughout the research. Given the small size of the community (and the fact that many respondents actively sought anonymity), all participants' contributions are presented anonymously, and care has been taken to remove any identifying information from quotes. When this research was conducted, Tor was in the process of recovering from a serious crisis in which a prominent community member had just been fired for allegedly engaging in sexual violence and abusive behaviour, which several participants linked to the changing values of the Tor Project. As a result. I sought to conduct these interviews sensitively, and to discuss these issues sensitively in this analysis, focusing on the organisational and cultural changes which resulted from these events.

When setting out, I expected to find strong, shared values in the Tor community, as the Tor Project now presents itself as a strongly value-driven organisation. In fact, my first finding was that Tor's values were remarkably contested, with different people articulating very different understandings of the project. An initial pilot study of four interviews showed that respondents would often draw from multiple mutually contradictory perspectives when talking about Tor. An analytical method focused on actors or social groups was insufficient to capture the complex landscape of discourses and values in the Tor community, and I drew instead from the social worlds framework, a theoretical approach which takes discourse as its unit of analysis (Star & Griesemer, 1989). The social worlds framework has proven useful for understanding how different groups of people collaborate together on knowledge-making projects, and has been applied to a range of subjects, including museums (Star & Griesemer, 1989), art (Schlossmann, 2017), education (Bayat, Naiker & Combrinck, 2015), and online knowledge communities (through the related 'communities of practice' framework) (Angouri, 2016; Lave, 1991). The research presented here constitutes its first use (of which I am aware) to explore how groups attempt to realise their visions of online privacy in practice by building their own Internet infrastructures.

Clarke and Star (2008) describe social worlds as ‘universes of discourse’, drawn on and evoked by communities of collective understanding, action and meaning-making (Unruh, 1980). Individuals can be members of multiple social worlds, which constitute a set of shared understandings which shape the individuals who draw on them, and hence ‘form the basis for collective action’ (Clarke & Star, 2008). They are a particularly useful framework for understanding communities engaged in infrastructural, engineering or knowledge-making work, and how their values and understandings shape and are shaped by infrastructures, technologies and practices. Infrastructures are core parts of social worlds and are embedded with their key values and logics; they are ‘frozen discourses that form avenues between social worlds and into arenas and larger structures’ (Clarke & Star, 2008).

Many of the core actors in Tor play multiple roles and draw on a range of ways of making sense of the project. My participants appeared to contradict themselves because they were, in fact, articulating multiple social worlds. While privacy is a central value in the Tor community, they understand the links between privacy technology, power and politics in a range of different ways. After conducting further interviews, I was able, through inductive coding and analysis, to cluster these contradictory perspectives into discrete, self-consistent frameworks of understanding within the Tor community. These were clustered with a mind to perspectives which drew from the same underlying ways of seeing the world, generating three main social worlds linked to particular types of work. These worlds, which I describe in this paper, construct different understandings of the links between privacy and technology, reconstructing debates well-known within Science and Technology Studies, namely, the tension between framings of technology’s political agency as structuring action, constituting action or supporting action (Berg, 1998).

Working together on Tor necessitates an accommodation between these different perspectives. Within social worlds theory, translation between social worlds occurs through ‘boundary objects’ (Star & Griesemer, 1989). Boundary objects are situationally specific constructions which exist within multiple social worlds, allowing for collaboration between different perspectives and kinds of work. Both ‘adaptable to different viewpoints and robust enough to maintain identity across them’ (Star & Griesemer, 1989), they have some elements which are shared between multiple social worlds, and others which are more amorphous, changing in different contexts. This paper argues that, in Tor, constructions of privacy act as a boundary object, featuring well-defined areas of shared understanding, and elements which are left ambiguous to accommodate difference.

The social worlds of Tor

Tor’s community is diverse, involving a range of perspectives and kinds of work, which I characterise as three main ‘social worlds’. The first of these is the *engineer* perspective, which stems from the design and development work on Tor and understands privacy technology as rewriting structures of power in technical networks. The second is the *activist* perspective, which is linked to the campaigning, lobbying and advocacy work of the Tor Project, and sees privacy technology as engaged in political work, a social movement in its own right. The final perspective is that of the *infrastructuralist*, arising from the maintenance and administration work done by the Tor community, which is deeply agnostic about the political character of privacy technology, preferring a ‘neutralised’ ethos of service provision. In this section, I characterise each of these social worlds, and how they articulate different understandings of Tor’s relationship to power and politics.

Engineers: privacy as a structure

The highest-profile work involved in the Tor Project is undoubtedly the development of Tor itself, and this work is characterised by what I term the *engineer* perspective. Tor has a small core team of full-time development staff who work on the project, supported by a larger Open-Source community of volunteer developers. In addition to this, many other projects – in particular ‘Onion Services’, which use the Tor network to provide anonymous and uncensorable web services – contribute to the broader Tor ecosystem (Tor Project, 2019). Their developers, and the large community of academics who develop privacy technologies, also contribute to the engineer perspective on Tor.

While it shares some commonalities, Tor’s engineering work is distinct from the practices of creative tinkering which are traditionally conceived of as ‘hacking’ (Levy, 1984). Rather than subverting or repurposing technologies which already exist, Tor’s engineers are engaged in the creation of something new: a massive, stable infrastructure which needs to be reliable. This entails the planning and design processes of modern engineering, and balancing between privacy, usability, resilience and security (Dingledine, Matthewson & Syverson, 2004). Although the Tor engineers are engaged in the same debates about privacy and Internet freedom (and often on the same side) as many conventional ‘hackers’, their understanding is framed by a different set of practices, logics and goals, which align more with Coleman and Golub’s expanded conception of hacking as including attempts to engage in politics through the creation of technologies and infrastructures (Coleman and Golub, 2008).

The engineer social world is shaped by a deep technical understanding of Internet infrastructure, combined with a practical engagement with its systems through design processes. Through this work, the Tor engineers construct politics and power as enacted through the structural forms which systems take, mapping ‘choke points’ which the topology of the Internet creates and how this gives power to the particular actors who control them. While hackers share this understanding of power as baked into the structures of information systems, they see their work as slipping between cracks and exploiting weaknesses in these structures, while engineers see themselves as reshaping the landscape entirely:

> But the act of [running a Tor node], just like the act of creating an Internet service provider where there wasn’t one before, is a political act, right? It changes the landscape, and the relationship between people, and what people can do, and can’t do, you know, so it’s, I mean, yes, it is… People who say that the choice to do this is not political are deluding themselves.
>
> Participant A - Tor community member

Musiani (2013) argues that perspectives like these represent part of an ‘architectural’ turn in Internet governance discourse. In the engineer world, privacy is a quality of the structures of technosystems whose designs produce different types of privacy and topologies of power. What is distinctive about the engineer perspective is that it does not make value judgements about *who* has this power, rather it critiques the accumulation of this structural power itself:

> I see the work that I do as decentralising and distributing power. Because I think that’s always a good thing. *laughs* I see that as a fundamental… like, if nothing else is true in the world, distributing power in this world is a good thing. And, so… when you’re threat modelling, it’s a case of, how do we take this cluster of power here… and how do we remove that from the equation?
> Participant B - Onion Service developer

This is not a disavowal of the politics of privacy technology; rather, privacy is understood through topologies of informational power. and making the Internet more private is seen as a process of redistributing this power. Thus, Tor is seen by the engineer perspective as reshaping the landscape of power online through network structures, reframing political questions about the technology in ways which can be tackled through design and development processes.

Activists: privacy as a struggle

Many of Tor’s intended use cases involve explicit interventions in political struggles, either in the broader social movement for Internet privacy, or as a tool used by activists for secure communication. As a result, Tor’s community includes a wide range of people who engage with civil society, activist movements and policymaking, who embody an *activist* perspective. There is a substantial body of research on Internet freedom activists, and so this section has been left brief other than a few remarks on the specific contours of Tor’s activist world (Marechal 2015).

> It enables individuals to, you know, be anonymous – that is a human right, and so, I feel that because of [that], the nature of the software, in my personal opinion, is political.'
> Participant C – Tor contributor

These discourses, drawn from the practices and experiences of privacy activism and providing security training to journalists and activists around the world, frame Tor's work as explicitly political. While they are anxious that Tor not abuse its influence, they are generally happy for Tor to engage in political debates which touch directly on its work, for example, to condemn far-right users as they did following the far-right marches in Charlottesville which resulted in the death of one counter-protester, and some far-right websites proposing moving to Tor.

> We've heard that the hate-spewing website Daily Stormer has moved to a Tor onion service. We are disgusted, angered and appalled by everything these racists stand for and do… Tor stands against racism and bigotry wherever and whenever such hatred rears its ugly head. It is our work to provide everyone with the best possible security and privacy tools so human dignity and freedom can be promoted all over the world.
> Tor Project Blog 2017

The activists see privacy technology as part of a social movement, a battle between authoritarian forces and surveillance capitalists on one hand, and privacy activists on the other. They see it as connected intrinsically to other struggles, whether women's liberation, LGBTQ rights, or harm reduction for criminalised practices such as drug-taking or sex work. While this framework is drawn on by policy workers and activists in the Tor community, many developers and relay operators are also involved in campaigning and advocacy, drawing on the activist perspective in understanding the broader meaning of their work.

Infrastructuralists: privacy as a service

As a globally-distributed infrastructure with millions of daily users, Tor relies on a substantial quantity of 'invisible work' in administering and maintaining its infrastructure (Star, 1999). The infrastructuralist perspective which typifies this labour is drawn on by Tor's relay operators and volunteer maintainers, concerned with the maintenance and upkeep of the network rather than design and engineering. Rather than 'hacking' (as creative tinkering) or 'engineering', they are involved in maintaining infrastructure, which needs to be stable and robust. The relay operators are the largest group of these 'invisible labourers' and so this section focuses on them; however other maintenance work, such as bugfixing and patching, also feeds into this perspective.

Most relay operators have little understanding of the inner workings of Tor (generally they are not anonymity or encryption experts) and so their understanding is shaped by the practices of running the network itself. Relay operation involves a number of elements, including finding an Internet service provider willing to host a Tor relay, setting it up, paying for bandwidth, maintenance and updates, and dealing with abuse complaints where law enforcement or other actors trace malicious user behaviour back to their Tor node. Despite sharing practices through wikis, mailing lists and IRC discussions, the relay operator community has been atomised for much of Tor's history, more a collective of individuals than a coherent group.

> I think [Tor works] probably because it's easy to work together. We don't actually have to work together! The Tor Project has made it so simple to start a relay and just run it, and not actually interact with anyone... they've made it so easy to act like a big community when actually we're not really. I think we might be a bunch of individuals…We don't have to co-operate with each other, apart from running the same software.
>
> Participant D – Relay operator

This is part of Tor's strength: anyone with the capacity to set up a server can contribute, no matter their motivations. This allows for collective action without the need for shared political allegiances, and a large, broad-church community of contributors. This frame is therefore deeply agnostic to Tor's relationship to power, and anxious to 'neutralise' the politics of their work as much as possible (despite their deep connection to explicitly political values around freedom of speech and privacy). Coleman describes a similar sensibility in the Free and Open Source Software community, which she terms 'political agnosticism' (Coleman, 2004). Coleman describes this as an expression of the interaction between the liberal values and technical practices of 'hacker' culture: 'what grows out of this particular life world of intense, lifelong programming and networked sociality is an overt aesthetic dislike for politics and a culturally embodied experience of freedom that conceptually shuns politics.'(Coleman, 2004).

Within this 'neutralised' politics lies a common commitment to deeply political values: the vision of a privacy-focused Internet where the flow of information, capital and communication proceeds without surveillance or censorship. The infrastructuralist world expresses these 'hacker ethic' values through forms of practice more rooted in infrastructural labour than hacking, framed around an ethic of service provision rather than creative breaking. This frames Tor's relationship to power and politics through a 'neutralised' variant of technoliberalism.

> I think most of us believe that we want to provide the tools so others can exercise their powers and their influences. People that understand society better, maybe. And we are just the infrastructure providers. Right? I think that's a notion that a lot of hackers have, is that ultimately they don't want the political influence, they just want to provide the infrastructure. For democratisation.
>
> Participant E – Tor contributor

This is distinct from the engineer perspective. Where the engineers see Tor as a political attempt to redraw the maps of informational power online, infrastructuralists are more agnostic about Tor's relationship to power, understanding privacy as a 'service' they provide to users who engage in political action themselves. Getting involved in normative conversations about how the network is used becomes a dangerous game, and so this perspective strongly resists any attempts on the part of the organisation to decry or promote particular use cases, legal or illegal, or to claim that Tor itself represents any specific set of values outside a neutral service for protecting data in transit. By constructing themselves as apolitical actors, they shift the moral character of the network onto the users, allowing them to contribute without feeling responsible for the traffic which their relay serves.

Relational perspectives

I argue that the above social worlds constitute three instantiations of liberal technopolitics, refracted through different kinds of labour. Much like the practices on which they rest, these social worlds do not exist in isolation. They are *relational,* defining themselves in opposition to one another. For example, the willingness of activists to link Tor to explicit political causes clashes with the infrastructuralist perspective, providing a foil against which they can contrast their own 'neutrality'. Some relay operators on the periphery of the Tor community are even sceptical that the other worlds of discourse really exist:

> I think it's neutral. Definitely, yeah. I think it's neutral… I think the people behind the Tor Project, are they free of values? I'm not sure if it was marketing they put on the front page… of course every privacy project in the Internet has to put some big strong words on their front page… But I think most of the people which are connected to the Tor Project, I think they are seeing it more… as a tool. A tool for people doing whatever they want.

> Participant F - Tor relay operator

While the engineers have less hostility to political work, they see it as frustrating, an arena in which they are ill-equipped and unempowered which they prefer to circumvent.

> I'm quite averse to getting involved in policy issues… I'd rather just implement a technical fix that prevents their law from being effective.
> Participant G - Tor developer

These social worlds represent 'ideal types', a typology which aims to differentiate and accentuate the characteristic qualities of each of these worlds, stressing commonalities within particular categories without claiming to correspond with the views of any particular person or group of people (Aronovitch, 2012). While the perspectives of individual people in the Tor community tend to be aligned with one of these worlds based on their role, they often draw from others, bridging between different worlds. Identities and roles in Tor are hence often multiple or ambiguous:

> I think I avoid having an identity too much. Not in terms of anonymity, but in terms of a self-image of what I am. Because it, I feel like that's limiting somehow.
> Participant H - Tor developer

While some members of the community may only be involved in engineering, policy, or infrastructural work, many of the core team are involved in all of these to some extent. Some of the engineers also carry out a variety of maintenance work, such as bugfixes, patching and monitoring the network, and outreach or policy work. Where they roll out updates and patches, they interact directly with the relay operators through mailing lists and IRC conversations. This means that many of the core developers, while primarily viewing Tor through the engineer lens, draw on framings from the activist or infrastructural perspectives when talking in more abstract terms about the place of Tor in the world. Similarly, there are some relay operators who see the work they do as part of their political activism (and developers and activists also contribute to the relay network), or as restructuring power relations online.

Within individual interviews, participants would often tack between different ways of making sense of Tor, drawing from different social worlds in different contexts. For example, in the following pair of responses, when discussing their broader motivations for being part of the community the participant describes Tor as part of a political movement for privacy as a human right, then, when discussing the practices of operating a relay and the traffic which flows through it, describes Tor as neutral tool whose politics stem entirely from its users.

> If you can see in Europe in United States, in Asia, in Russia, in Africa, there are a lot of crimes actually, against free speech, against human rights, about anonymity, you know United Nations has enlisted online anonymity as a basic human right more than a year ago… [Tor is] very important because the, yes, people have the right to think freely, to speak free, to speak from their hearts, not from fear of governments that will punish them
> Participant I – Tor relay operator

> Because the tool is something that helps you to do something. But uh, you know, what you will do, with this tool, is up to you. Crime happens not on the hard drive of the Bond movie producer, crime happens not on the Silk Road drug store, no. Crime happens inside people's mind… Neither Tor or other software authors, nor people who are running even exit nodes, no they're not responsible. They are not responsible for another people's thoughts and actions. They are not. Tor is just a tool
> Participant I – Tor relay operator

As Unruh (1980) describes, it is this multiplicity of membership in social worlds which forms the 'glue' that binds them together. Part of Tor's success has been precisely due to the productive tension between these three perspectives (which have grown and developed alongside the infrastructure at different points), and due to the fact that many of the core team can translate between these social worlds.

Collaboration, conflict and transformation

Privacy as a boundary object

Despite this heterogeneity, Tor has been remarkably successful at fostering collaboration within its diverse community. In this section, I explore how these worlds coexist, and how individuals are able to bridge between them. Although they differ in their understandings of the politics of privacy technologies, these social worlds share important sites of agreement, giving them a shared link between the diverse kinds of work they do and the animating values and goals of the project.

When asking participants about the most important use cases of Tor, they conceptualised these as falling within two distinct categories which took a common form across all three social worlds. The first of these, which I characterise here as everyday privacy, are everyday users of the Internet.

> The whole reason that Tor Browser existed is because there was a belief that privacy should be for everyone, it shouldn't just be for techie people who are able to pull together all these obscure components.
> Participant J – Tor developer

This constructs a type of privacy rooted in the quotidian rhythms of users' daily lives. It argues that while any individual piece of information gathered may be innocuous, the aggregated datasets of web traffic which governments collect for whole populations amounts to deeply intrusive surveillance. Many of the participants linked this to protecting democratic values, the right to free speech, and halting what they saw as a dangerous trend towards authoritarianism.

This is contrasted with the use of Tor to protect people in cases where detection of a single piece of information might mean imprisonment, death or other serious consequences.

These high-risk users, which include political dissidents, freedom fighters, CIA field agents, journalists, and human rights activists, tended to incur substantial interest from powerful actors and hence need protection through rigorous security practices.

> [journalists] are getting people to speak to them in a truly free way that they would not in almost any other context. You know, there's no… parking garage where you can go to speak to Woodward and Bernstein any more, that's over. [Tor Onion Services] is that parking garage.
> Participant K - Onion Service developer

Some community members prioritise high risk use cases, while others place more emphasis on everyday privacy. While individuals differ in which of these they see as important, they agree that Tor's construction of privacy encapsulates these two distinct forms.

> I think you couldn't have Tor when you didn't have all of those things. Anonymity loves company, and you couldn't have the Chinese dissident anonymity system, or the US military open intelligence gathering system, it doesn't make sense. So, I think, if there's one thing that's the most important, it would be that all of these things can interact on the same system. I'm sure everyone will have their own preferences… I'm happier that people who are trying to promote human rights are able to have their job facilitated through Tor. That's probably what I personally think, but I recognise that it would be useless to have just that sort of group.
> Participant J – Tor developer

These constructions arise from Tor's design. Tor was initially created in collaboration between US Naval researchers and 'cypherpunk' technologists wanting to shape the Internet as a privacy-preserving social space. Its design involves large numbers of everyday users acting as 'cover traffic' for higher-security use cases.

> The old Cypherpunks and the US Navy are facing the same problem and are therefore looking at similar solutions. You need broad public use of the system to provide you with cover traffic and we want to see such a system deployed to provide the citizens with privacy. We are allies, not enemies.

Or-dev mailing list 1997

The three social worlds of Tor draw their constructions of the user from the logics embedded in its technical design, which provide a common point of stabilisation between Tor's worlds. From the engineer perspective, this frames user categories through the patterns they trace in technical systems, and envisions privacy in terms of the decentralisation of structures of power and control in the Internet. The world of the activist understands everyday privacy as a civil rights movement in its own right and sees high risk use cases as important for activists and journalists involved in social justice struggles the world over. The infrastructuralist perspective resonates with the 'content agnostic' nature of this user classification, which classifies users according to security criteria and the patterns of their use rather than their politics or allegiances.

In this way, privacy acts as a boundary object (Star & Griesemer, 1989), with a shared construction of privacy in the user allowing individuals to bridge between otherwise irreconcilable social worlds. This has historically allowed Tor to leave the political dimension of privacy ambiguous, giving its community the freedom to conceptualise the links between privacy technologies and power in different ways. Until recently this détente has proven remarkably resilient, helping Tor has to navigate these conflicts and draw on the interpretive power of these different social worlds.

Cultural change and boundary breakdown

However, boundary objects, are not immutable (Star & Griesemer, 1989). The détente between Tor's worlds and their distinct constructions of both privacy and the role of privacy technologies as sites of social action has proven durable for much of its life; however, a series of internal crises and cultural changes have in recent years made this untenable. As it has had to be clearer about its core values and what it stands for, so too has the cultural landscape of the Tor community changed. In this section, I explore the nature of this challenge and how Tor has navigated it, how a social worlds perspective helps us to understand the deeper implications of this, and the resulting transformations in Tor's social worlds.

Following the Snowden revelations, the Tor community saw a massive influx of new members, galvanised by the social backlash against mass surveillance by the US, and a more activist perspective on Tor. At the same time, a shift in the broader culture of the tech industry was underway, bringing a more critical sensibility to prominence, and calling out a history of misogyny and abuse in these communities. This was accompanied by an increasingly critical trend in public discourses about online platforms, focused on the power and politics of the people behind these technologies. For Tor, this came to a head in June 2016, when several members of the Tor community accused Jacob Appelbaum, a member of the core team and one of Tor's most prominent representatives, of engaging in a pattern of abusive behaviour and sexual assault. This resulted in Appelbaum being fired from the project, the replacement of the project board and the installation of Shari Steele as director. Steele led a programme of professionalization, remaking Tor into a modern NGO with more developed organisational practices and structure and a well-defined set of core values (Marechal - forthcoming). This has met with praise from some sections of the community and considerable opposition from others, and has shaken the détente between the social worlds of Tor.

A social worlds perspective allows us to understand this crisis as not just a clash between groups within the Tor community, but as the rupture of a previously-stable equilibrium between different ways of understanding the project. From the activist perspective, Tor is inherently political, promoting values of liberation and democracy, so this change was a necessary part of Tor's growth as a modern activist organisation. Equally, despite their suspicion of 'policy' work, the engineers seem to have welcomed this formalisation of Tor's values, especially against harassment. I contend that this is because of how this has been framed – as attempts to redistribute and decentralise power within the Tor Project.

> Tor has definitely become more open in the last year or so… And I still think they're going through this evolution of wondering where they fit in the world.... And they're getting better at addressing all these issues, they've done a lot of work in making sure that accusations of sexual assault and harassment are addressed, and opening up the power structures, and restructuring that.
> Participant B– Onion Service developer

However, for some of those adopting a purist infrastructuralist perspective, these changes were less welcome. Asserting Tor as embodying feminist principles and attempting to transform Tor into a diverse, modern organisation with explicit values has, for some in the community, undone the political ambiguity which enabled them to feel aligned with its goals.

> This changed to, Tor is now about women's rights as well... They are probably right, with everything they say, so don't get me wrong. But Tor isn't specifically about empowering women and technology. I mean, they can do that, whatever. Take turns, do workshops, whatever. But that's not why I'm running a Tor relay. I'm running a Tor relay because there are people in Turkey and they're in jail for things they write, because people in Syria are getting killed if they are found reporting from certain areas. People in China just disappear if they are found using Tor, that's why I'm running Tor relays, Tor bridges. That's what I care about. Women's rights - fine, but, just, sorry, not my department! And saying that out loud makes people upset.
> Participant L – relay operator

The assertion of political neutrality to rule feminist concerns out of scope for technical projects has historical precedent in 'traditional' hacker and OSS culture (Nafus, 2012). In Tor's case, the firing of Appelbaum and the resulting organisational changes led to a minority within the community leaving outright. The atomised nature of the relay operator community meant there were no real leaders to drive an exodus, and no strong sense of a shared social meaning (in fact, the infrastructuralist understanding of Tor precludes this). Many who understood Tor from this perspective were still able to see themselves in the infrastructural labour of the organisation; however, some felt unable to in the public life of Tor, feeling that Tor's values now excluded their way of understanding it.

> And then with the Jake fallout and different conflicts… a bit of the dynamics changed… I mean Tor is trying to become a professional NGO. Tor Project Incorporated. And I think that's a change over the previous idea of being deeply rooted in a lot of different communities. When you want to become a professional NGO, you make decisions. You have to make decisions. Before, you can be very flexible, and in different situations with different people act very differently. And it's not necessarily that there were any mistakes, it's just the growth is now changing things. And also, of course, changing who… stays around and what their incentives and motivations are for still hanging around and doing this kind of work.
> Participant E – Tor contributor

This is not merely the sidelining of one group in favour of another, rather it is representative of a transformation in how the Tor community understands itself as the organisation has matured. Accordingly, the infrastructuralists' world has also begun to change, moving from an 'atomised' model of relay operation to a collaborative one based around in-person meetings and a more engaged community with a shared sense of purpose.

> And then there's also this element of, we should all get to know each other, because we're kind of in this boat together. Uh, even if we disagree on a lot of things, like, there's clearly something that's binding us together, so we should at least meet and talk about it.
> Participant D - Relay operator

The engineer perspective is also transforming. Its topological understanding of power is increasingly turned on Tor itself, critiquing the developers' own 'power to structure' in designing these systems. This is indicative of a broader trend in the Internet freedom community, as through organisations like Tor, Tactical Tech and Open Privacy there is a concerted effort to extend this understanding of power in network structures to specific, subjective local contexts rather than universalising abstractions.

Infrastructures require a range of different kinds of work to function, bringing together people, cultures and perspectives in complex ways. In navigating this, Tor drew on privacy as a boundary object to unite the community around a shared sense of the meaning of their work. Through a common construction of Tor users, they were able to leave Tor's links to politics and power ambiguous, enabling many of the core team to bridge between these worlds. As the context of Tor changed through the Snowden revelations, the increasing prominence of the activist perspective, and broader cultural changes in the information security community, this tension came to the surface, erupting in the firing of Jacob Appelbaum and the professionalisation of Tor. The result of this has been the tentative formation of a new détente, reflecting changing understandings of politics, power and practices in each of these three worlds. How it navigates this will be deeply consequential for the kind of organisation Tor becomes and its role in struggles over privacy, politics and power online.

Conclusion

Tor is both a technical project and an exercise in meaning-making, an alignment of different perspectives and people to create an infrastructure and thus realise a set of visions of privacy. Across our societies there is an ongoing struggle over the role of privacy in Internet technologies and platforms. As our spaces of social action become increasingly embedded in complex, technical ICT infrastructures, so now are the designers of these infrastructures becoming important in shaping the properties and values of these social spaces. Understanding these values and where they come from is therefore a vital project.

Infrastructures involve many different types of work, some of which, though they may occupy the same terrain as ‘hacking’ (in its guise as the crafty subversion of technosystems), are based on logics and practices which look very different (Levy, 1984; Coleman and Golub, 2008). Each of these brings with it a different way of making sense of privacy and the role of privacy technology as a site of social action. In understanding the cultures which underpin the technologies and infrastructures of the Internet, we need to look beyond conventionally-conceived ‘hackers’ to include wider types of work and how they navigate conflict and consensus. A social worlds perspective is a fruitful framework for exploring these technologies and the people behind them, making sense of values in infrastructural projects composed of a range of different perspectives. How they navigate conflict and consensus are important for understanding the social meaning which these infrastructures come to inhabit, and how they shape the world.

Tor exhibits three distinct social worlds with different understandings of privacy technologies’ links to power, grounded in the logics and practices of particular types of work: privacy as a structure, privacy as a struggle and privacy as a service. Tor has been remarkably successful at accommodating these dissonant perspectives through the cultivation of ambiguity in its privacy politics. The myth of technology as politically neutral has substantial power, enabling groups to collaborate despite conflicting politics, helping individuals to bridge between different perspectives, and reframing social questions in a language in which technical workers feel they have more expertise. However, in recent years, the figleaf of ‘technological neutrality’ has become less able to hide questions about power, values and politics for Internet technologies. From Google to Facebook, these infrastructures and platforms are increasingly being held to account for the shaping forces they exert on social life. Tor is not, and could never be, exempt from this wider social change. As it navigates these changes it is part of an evolving politics of the Internet which is increasingly reflexive about the infrastructural power it wields.

Declaration: The author is unaware of any conflicts of interest.

Bibliography

Aldridge, J., & Decary-Hétu, D. (2016). Cryptomarkets and the future of illicit drug markets. *The Internet and drug markets*, 23-32.

Angouri, J. (2016). Online communities and communities of practice. *The Routledge Handbook of Language and Digital Communication*, 323-338.

Aronovich, H (2012). Interpreting Weber's ideal-types. *Philosophy of the Social Sciences*, 42(3), 356-369.

Bayat, A., Naicker, V., & Combrinck, T. (2015). Towards an Understanding of How School Administrative Clerks Negotiate Their Work in Public Schools: A Social worlds Perspective. *International Journal of Educational Sciences*, *8*(2), 293-303.

Bennett, C. J., & Raab, C. D. (2017). *The governance of privacy: Policy instruments in global perspective*. Routledge.

Berg, M., 1998. 'The politics of technology: on bringing social theory into technological design', *Science, Technology and Human Values*, 23(4), 456-490

Clarke, A. E., & Star, S. L. (2008). The social worlds framework: A theory/methods package. *The handbook of science and technology studies*, *3*, 113-137.

Coleman, G., 2004. The political agnosticism of free and open source software and the inadvertent politics of contrast. *Anthropological Quarterly*, 77(3), pp.507-519.

Coleman, E. G., & Golub, A. (2008). Hacker practice: Moral genres and the cultural articulation of liberalism. *Anthropological Theory*, *8*(3), 255-277.

Collier, B., forthcoming A, *Growing Onions: an exploration of privacy worlds in the design and development of Tor, an online anonymity network*

Collier, B, forthcoming B*, Open secrets, hidden work: exploring resilience cultures and infrastructural high policing in Tor, an online anonymity network*

Collier, B, forthcoming C, *Allergic to Onions: infrastructure, visions of the Internet, and technologies of control*

Collier, B, forthcoming D, *Infrastructural power: mapping struggles over meaning, crime, and control in the Tor anonymity network*

Dingledine, R., Mathewson, N., & Syverson, P. (2004). *Tor: The second-generation onion router*.

Gehl, R. W. (2018). *Weaving the Dark Web: Legitimacy on Freenet, Tor, and I2P*. MIT Press.

Lave,J (1991). Situating learning in communities of practice. *Perspectives on socially shared cognition*, 2, 63-82.

Levy, S. (1984). *Hackers: Heroes of the computer revolution* (Vol. 14). Garden City, NY: Anchor Press/Doubleday.

Lewis, S.J., (2017) *Queer Privacy,* Marscherari Press

Lyon, D. (2015). *Surveillance after Snowden*. John Wiley & Sons.

Lyon, D. (2017). Digital citizenship and surveillance| surveillance culture: Engagement, exposure, and ethics in digital modernity. *International Journal of Communication*, *11*, 19.

Maréchal, N. (2015). Ranking digital rights: Human rights, the Internet and the fifth estate. *International Journal of Communication*, *9*(10), 3440-3449.

McCoy, D. et al. (2008), Shining light in dark places: understanding the Tor network' In *International Symposium on Privacy Enhancing Technologies Symposium* (pp 63-67). Springer, Berlin, Heidelberg

Murdoch, SJ & Danezis, G. (2005). Low-cost traffic analysis of Tor. In *2005 IEEE Symposium on Security and Privacy* (S&P05) (pp. 183-195). IEEE

Musiani, F. (2013). Network architecture as Internet governance. *Internet Policy Review*.

Musiani, F. (2015). Practice, plurality, performativity, and plumbing: Internet governance research meets science and technology studies. *Science, Technology, & Human Values*, *40*(2), 272-286.

Nafus, D. (2012). 'Patches don't have gender': What is not open in open source software. *New Media & Society*, *14*(4), 669-683.

Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

Raab, C. D., Jones, R., & Székely, I. (2015). Surveillance and resilience in theory and practice. *Media and Communication*, 3(2).

Rider, K. (2018) The privacy paradox: how market privacy facilitates government surveillance, *Information, Communication & Society, 21*(10), 1369-1385

Schlossman, D. (2017). *Actors and Activists: Performance, Politics, and Exchange Among Social worlds*. Routledge.

Snader, R. & Borisov, N. (2008). A tune-up for Tor: improving security and performance in the Tor network. In *NDSS* (8): 127

Star, S. L. (1999). The ethnography of infrastructure. *American behavioral scientist*, *43*(3), 377-391.

Star, S.L., (2010). ‘This is not a boundary object: reflections on the origin of a concept’, *Science, Technology & Human Values*, 35(5): 601-617

Star, S.L. and Griesemer, J.R., 1989. ‘Institutional ecology, ‘translations’ and boundary objects: amateurs and professionals in Berkely’s Museum of Vertebrate Zoology, 1907-39’, *Social Studies of Science*, 19 (3): 387-420

Solove, D. (2008). Understanding privacy. Cambridge, MA: Harvard University Press.

Steijn, W. M., & Vedder, A. (2015). Privacy under construction: A developmental perspective on privacy perception. *Science*, *Technology*, *& Human Values*, 40(4), 615-637.

Unruh, D. R. (1980). The nature of social worlds. *Pacific Sociological Review*, *23*(3), 271-296.

Viseu, A., Clement, A., & Aspinall, J. (2004). Situating privacy online: Complex perceptions and everyday practices. Information, Communication & Society, 7(1), 92-114.

Wright, D., & Raab, C. (2014). Privacy principles, risks and harms. *International Review of Law, Computers & Technology*, 28(3), 277-298.

Yar, M. (2012). Virtual utopias and dystopias: The cultural imaginary of the Internet. *Utopia: Social Theory and the Future*, 179-95.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*, Public Affairs.