INTERNET POLICY REVIEW
Journal on internet regulation

Volume 9 | **Issue** 4

RESEARCH ARTICLE

OPEN ACCESS

PEER REVIEWED

VPNs as boundary objects of the internet: (mis)trust in the translation(s)

Luke Heemsbergen *Deakin University* luke.h@deakin.edu.au
Adam Molnar *University of Waterloo* adam.molnar@uwaterloo.ca

DOI: https://doi.org/10.14763/2020.4.1513

Published: 21 October 2020
Received: 18 May 2020 **Accepted:** 3 August 2020

Funding: The Alfred Deakin Institute of Globalisation and Citizenship provided funding for this publication.
Competing Interests: The author has declared that no competing interests exist that have influenced the text.

Citation: Heemsbergen, L. & Molnar, A. (2020). VPNs as boundary objects of the internet: (mis)trust in the translation(s). *Internet Policy Review*, *9*(4). DOI: 10.14763/2020.4.1513

Keywords: Boundary object, Metaphor, Regulation, Privacy, Security

Abstract: How do we come to trust, use and govern virtual private networks (VPNs)? How do these objects of the internet tack back and forth between metaphor and technical processes as they garner usership and critique? This paper aims to answer these questions by considering VPNs as boundary objects. We follow Susan Leigh Star's (2010) call to further explore the 'tacking' back and forth of boundary objects as both symbolic and technical objects. This is applied within internet-space and governance-space through empirical methods that walkthrough a typical user experience for acquiring VPN services, while also offering a systemic account of the discourse that such a user would experience in coming to understand VPNs and their function.

This paper is part of **Trust in the system**, a special issue of *Internet Policy Review* guest-edited by Péter Mezei and Andreea Verteş-Olteanu.

Introduction

This paper considers VPNs as boundary objects of the internet, in a way that opens new empirical and methodological insights about the tensions between technical materialities and symbolic registers of technology. The tensions we explore include: what discourses surround Virtual Private Networks (VPNs) for users and how does this affect their deployment? How do users come to understand VPNs as specific technologies or as part of the internet? How can we discern what these objects are as they tack back and forth between metaphor and technical processes in their use and their governance? The impacts of these tensions have profound implications for navigating socio-material practices online, as well as 'offline' through conceptualisations of how to govern these technologies.

This paper looks at the social ontologies of an exemplar boundary object of the internet: VPNs. Following Star's (2010, p. 603) clarification of boundary objects as entities that people act towards (or with) in relation to their own communities of practice, we follow Star's call to further explore the 'tacking' back and forth of such objects as both symbolic and technical objects within internet-space and governance-space. We especially note how the dialectic between symbolic register (i.e., technology as metaphor) and actual affordances-in-practice (socio-technical / standardised material capacities) influence individual uses and attempts toward regulation.

To illustrate the potential of boundary objects of the internet, consider encryption as a thought experiment. Encryption follows the polysemic tacking from math (cryptography); encryption as technical process (cryptanalysis); encryption in/as ecommerce; encryption activism; encryption as 'going dark'; and encryption law. Note here the tacking from technical to metaphorical, and then back to technical transverses and is transfigured through competing domains of power and meaning: we start in technical mathematics and computer science and end in technical legal scholarship. Uncovered through this tacking are forces of politics and policing (Rancière, 2006) that shape and shift meaning making through communities of practice linked to the various interpretive objects identified. Rancière's distinction between politics and police might be useful for the organisation/legitimising of power insofar boundary objects communally exist and are experienced. Politics is

antagonistic to policing, breaking tangible configurations to test the assumptions of equality in society (Rancière, 2006, pp. 29-30).

Using the examples of 'going dark' as a metaphor for understanding the risks posed by end-to-end encryption, the result from a law enforcement and regulatory view, based on this metaphorical interpretation as specific to a kind of problematisation, are attempts to force a re-design of the artefact itself, or ban it, or highlight those nefarious facets of what makes the boundary object what it is: encryption is for child exploitation. The use of metaphor thus flows into how courts and regulators interpret and understand technologies so as to establish and limit conditions for how it should be 'dealt with'.

End-to-end encryption is, on the one hand, a standardised mathematical and technical infrastructure that is embedded in popular mobile messaging applications. On the other, it is a discursive representation that is conceptualised within and across a range of situated institutional knowledge and settings, such as in law enforcement, the legal community, and computer science. For example, within the legal setting, as Gill (2018) notes "what does it mean to describe the encrypted machine as a locked container or building?" (2018, p. 1). How does such a symbolic interpretation influence user applications; the existence of particular kinds of standardisation in relation to how culture might inform design decisions? Or more specifically, how do government and law enforcement attempt to impact and direct "what encryption is" as a standardised technical infrastructure that becomes interpreted and applied in various contextual discourses specific to consumer privacy, patient health or citizen elections? Seeing encryption as a boundary object shows the power of influence that constructing boundary objects have in the user and policy discourse. What we make of the mathematical facts of cryptography, conditions potentials and constraints of future activities online and off. The example of encryption as infrastructure of the internet shows how our approach might be useful for the empirical study of discrete objects that become more or less standardised (Star, 2010) and perceived as internet infrastructure.

This remainder of the paper is focussed on empirical exploration of one such boundary object where encryption is employed through the internet: Virtual Private Networks (VPNs). We look at VPNs through observing the discourses available to users when constructing understandings of VPNs, and relatedly, how VPN providers construct their products and its governance. In other words, VPNs function as a technical artefact that reconfigures communication in particular ways, and as an imagined capacity for the conduct of conduct, which Foucault identifies with respect to how individuals govern themselves (Foucault, 1994 p. 237). The

work adds to the literature in two ways. The first is empirical, unpacking VPNs in ways that combine literatures on boundary objects (Star, 2010) and internet studies. Our work here subsequently clarifies the stakes of political implications endemic to collisions between the standardisation and representational translations of boundary objects across different organisational, institutional, and user-centric settings. The second is more theoretical, in that instead of considering boundary objects 'on' the internet we move to conceptualise boundary objects 'of' the internet, which we argue opens a fruitful reconfiguration of Star's work for internet research.

Boundary objects *of* the internet offer a methodological framework that helps discern agonisms within (and without) technologies' conceptualisations, which together form the social and political terrain through which user applications and governance materialise. Identifying and potentially shifting the symbolic registers through which these objects come to be understood provides a unique point of leverage for those regulating and deploying these technologies.

Existing research literature

There is a resurgence in studying boundary objects in the digital age, with Language, Communication and Culture (searched via Australian and New Zealand Standard Research Classification FOR 'code' 20*, which spans these disciplines) publication mentions of the term more than doubling from 2010 through writing of this article (Digital Science & Research Solutions Inc, 2020). This trend indicates a revitalised consideration of the work of Star (see Bowker et al., 2016) whose work is closely related to the sociology of science and science and technology studies. The concept of boundary objects has proven useful for researchers as a means to conceptualise and make sense of the various experiential objects that come into existence via technological practices acted upon and through digitally distributed networks.

A sample of recent research utilising boundary objects that is of interest to internet researchers includes imagining news and technology nexus in terms of process, participation and curation (Lewis and Usher, 2016), digitisation and mixed document authorship (Huvila, 2019), Free-Libre and Open Source Software (FLOSS) documentation (Østerlund and Crowston, 2019), humor online (Gal, 2018), and charting discourses of power legitimisation via competing images of the internet itself (Shepherd, 2018). What is perhaps missing from this sample is a distinction of and reflection on the extent these objects may be thought of as *of* the internet; as technical artefacts and infrastructures that are sung into existence through dis-

tinct online cultures, practices and needs of internet use(rs), and software developers. These are of course constructed in relation to a broader apparatus of institutions that are tasked with a responsibility to regulate uses of these same artefacts and their multiple purposes on interconnected networks (i.e., the internet and its governance (DeNardis, 2014)). Within these discourses and varying levels of agency, we ask what are the implications for freedoms and controls over how users and regulators tack back and forth between technical and metaphorical claims of the technologies that enable products and features of internet life.

This approach similarly includes interest in how such objects come to be (dis)trusted insofar as they facilitate specific expectations of use, or what can be referred to as 'technological affordances-in-practice' (Costa, 2018). We contend that this sense-making practice is a deeply political one (see Rancière, 2006, pp. 29-30) that establishes conditions for not only how technologies are used, but for how standards and regulations are set, which in turn can influence future design and deployment, and thus craft the political-structural affordances specific to artefacts themselves. The 'political affordances' (Heemsbergen, 2019) of boundary objects of the internet set experiential rules as well as tactical use cases. They also establish conditions of possibility for how and in what ways objects of the internet are used by specific communities and to what ends. In essence, we mean to call into question how boundary objects are inherently about (re)arrangements of power, and how this links to the expectations of the conduct of conduct through and with them.

A focus on power and deployment embodies the ethos of Star's work. It aligns to a feminist approach to technology studies, which for Star, linked lived experience, technologies, and silences (in Olsen & Selinger, 2007, p. 227) in ways that proved political. Our work enables boundary objects to, more than explicate functional processes within communities, consider how socio-technical relationships are made through them (Star, 2010) and to consider the extent that these objects involve mediational qualities that are facilitative or inhibitory (Fox, 2011) of cross-boundary communication. Thus, our work is interested in contexts from which a boundary object is embedded (commercial, cultural), the ways in which boundary objects are interpreted; explanations that assert some intrinsic or essential property of the object that describe its functionality and; the regulatory environment that apprehends the object through symbolic (and often metaphorical) terms as a matter of policy or law.

To foreshadow the importance of these delineations, consider that the technical definitions of malware and some VPN products intermesh (Ikram et al., 2016),

while users (dis)trust each in dichotomous ways that uphold specific political-economic systems - or break down socio-political ones. The regulation of VPN and malware is of course vastly different based on user perceptions and the literal affordances in practice that similarly coded software is perceived to have through varying levels of user autonomy in its use and transparency in its goals and mechanisms. These differences play out in user discourse and policy discourse to stark political effect.

How metaphors transfigure technological practices and shape policy and legal structures has history in the digital age. Data itself, abstracted from binary or code, has been repeatedly conceptualised as a natural force or exploitable resource (Puschmann & Burgess, 2014) that through data streams, data mining, or data clouds, offers liquid, solid, and gaseous states of matter that beget industrial thinking on how to and who should exploit it (Hwang and Levy, 2015). Such discourses often juxtapose critical views of big data with statements that suggest data is people (Lemov, 2016), and should be regulated as such.

Such contradictions matter. If the metaphors with which new technologies are identified are sufficiently linked to existing 'things that we already have rules about' (Hwang and Levy, 2015) similar logics of regulation will flow onwards to the new technology. There are fewer institutional settings where the stakes are more profound than in the context of law. As Gill (2018) notes, metaphors have the power to define realities, and in so doing, sanction legal rules and social conduct, which often includes the very reach of the state into private life. Likewise, a lack of clear link to existing regulated things causes confusion. The multiple metaphors for what "big data" is (and can do) results in a scattering of potentially relevant ethics codes as discourses around data cultures that shape data's material, cultural, and political impact (Stark & Hoffman, 2019).

One might measure one 'tack' of the internet itself as a boundary object, from technical to abstract on the following departure: pipes and warehouses; packets and protocols; content distribution networks / shaping practices; "net neutrality"; civic capacities; and finally, public representation. What is key here is realising that the metaphors of clouds and torrents, flows and packet sniffing, relate to potentials that sit between the abstract and technical; subsequently, regulatory protocols are trained on what relates to these metaphors – that is, it becomes knowable and therefore governable – in this case targeted through arguments related to net neutrality.

Boundary objects as a methodology then, allows rigorous consideration of the in-

fluence of metaphorical and technical as objects tack back and forth from intrinsic natures and abstract metaphors to elicit policy consideration. These policy considerations are not born of consensus but how different options come to be chosen (Mol, 1999), and what the implications are for enacting associated politics and policing of the object. The article now discusses the potential for studying boundary objects of the internet by further detailing a suitable research design.

Research design and methodology

The design and approach of examining VPNs as a boundary object is drawn from Science and Technology Studies (STS) that acknowledges the mutual shaping of sociocultural and technical processes (Latour, 2005). Further the seemingly multiplicity of experiences created through the same or similar digital boundary object puts into new relief how digital media can move 'past formalising a world taken for granted' and realise 'forms designed to produce alternative worlds' (Flusser, 1999, p. 28). That is to say that not only are digital 'objects' generative, the same code might transfigure a multitude of experiences depending on context and perceived use potentials and user experimentation. The heterogeneity of boundary objects of the internet is, in part, due to their digital materialisations; the designs with which code can be reconfigured, interfaces re-skinned, and potentials only constrained via a spectrum of bandwidth. At the same time, what their technical constructions facilitates or inhibits (Fox, 2011) remains our concern in relation to the environment in which these potentials come to be rhetorically constructed. While the boundary object we focus on is the VPN, the research design that we discuss is potentially useful in examining other inquiries of boundary objects of the internet. We've already noted how end-to-end encryption, net neutrality, or the internet itself might apply. In short, our work is designed to assess discourses that surround search, discernment, choice, activation and governance of, in this case, VPN services.

Our methods present a 'work in process' that synthesises the strengths of discourse analysis for internet related phenomenon (Brock, 2018; Johnstone, 2018; Jones et al., 2015; Mautner, 2005) and the experiential phenomenological modes of inquiry in walk through methods (Light et al., 2018). This synthesis expands scope in relation to what boundary objects are and afford both technically and politically. Our focus in particular is on the ecology experienced by users that comes before in-app user experience. Symbolic and representational registers tied to user experiences of learning of and deciding to use a VPN presents rich data for mapping the facets of boundary objects. Similarly, competing registers amongst regula-

tory agencies surrounding VPNs also becomes a reflexive matter of concern.

Instead of focussing on the user experience or the political economy of a specific app we attempt to heed Star's advice regarding the scale and scope of boundary objects. Star (2010) signals that she is less interested in actual specified things (e.g., a flag or an app), as it is

> more interesting to study people making, advertising, and distributing [the specified thing], and their work arrangements and heterogeneity than to simply say that many people have different interpretations of the [specified thing] (Star, 2010, p. 613).

Thus the processes which are involved in creating the phenomenon-as-presented to potential users of the boundary object are of interest. How VPNs are marketed, how popular search results organise the discourse around VPNs, and how regulators envision policy *vis-à-vis* these presentations of object all offer insights to the competitive heterogeneity of boundary objects as well as the heterogeneity of people making, distributing, using, and regulating them.

Second, in some regards VPNs, while diverse at a level of specific app choice, share as a goal the potential to become standardised technical infrastructure. VPNs that 'just work' in tech parlance, disappear for their users and become part *of* the internet, as opposed to being things to do or use *on* the internet. For a related example, consider the proliferation of Hypertext Transfer Protocol Secure (HTTPS) connections to websites, which shows an additive security protocol becoming infrastructure. Securing the HyperText Transfer Protocol, became a common website design feature after Snowden's (2013) whistleblowing highlighted the potential for widespread surveillance of user activity as well as growing recognition of third party man-in-the-middle content injection or de-anonymisation (Basques, 2015). By 2019, most modern browsers flag non-HTTPS webpages to the user as 'non-secure' anomalies; HTTPS now just works as an invisible part of the internet. HTTPS allows and enforces new forms of security and privacy for and between publishers and readers of web content through code and governance schemes that most users never consider. At the same time, it affords novel forms of connectivity that otherwise would not be possible (e.g., 'getUserMedia()' calls and geolocation services) that have ushered in evolving use cases by individuals; its material and imagined capacities for users are real, while its regulation has been confined to a protocol that allows the internet to function.

VPN products provide similar profiles insofar that browsing and communication *experiences* are meant to be changed as little as possible for perceived day to day use. At the same time, VPNs provide, among other services, geo-anonymisation and data-anonymisation as ways to obfuscate identities and patterns of browsing behaviours so as to enable new experiences. Yet, VPN use does not hinge on, nor is it defined by, specific interface experiences past signals to users that the service is active; walking through the actual interface users experience to start up or manage VPN sessions becomes less important than mapping the decision to implement a VPN solution when explaining both the power, purpose, and experience of VPNs.

This is not to discount notable differences in apps and their effects; most notably how peculiarities of interface (Poulsen, 2018; Richardson and Hjorth, 2017) afford not only user interaction potentials, but relate to use cases based on social contexts (Heemsbergen, 2019). Our mode of inquiry in fact highlights how communicative affordances (Schrock, 2015) and those in-practice experiential affordances (Costa, 2019) are distinct. Indeed, considering the above HTTPS example again, while the underlying technical-communicative and even technical-governmental affordances of HTTPS differ dramatically from HTTP, any *perceived* change in user communication experience is minimal. This perceived likeness does not, of course, speak to other novel potentials that users institute through HTTPS (or as we will encounter below, VPNs). The likeness demonstrates how infrastructural change *of* the internet has effects that are not apparent to users in Human Computer Interaction (HCI) terms, or in ways that are easily investigated by walkthroughs; an abstraction to the process of user practice is required to rigorously understand boundary objects of the internet.

Third, the user (experience) presents only one of many distinct populations that define the boundary object. While user experience on-app is important, it is not definitive of the object. Our aim is then to focus less on user interface arrangements, functions and features, and more on contextual content and tone, or the symbolic representation of the object as a user is being drawn to enter into a relationship with it. Walkthrough methods (Light et al., 2018) of course direct as much, and we mean to acknowledge the importance of 'environment' and abstract up to a level of ecology; the many actants and formations that come to collectively contest and define any boundary object.

Our methodology then offers a walkthrough of how a user would come to experience a boundary object as a product by way of observing the political economy and regulatory ecology that makes up these objects *of* the internet. While this

method has various limitations, it offers a work in process insofar it encounters the discourses that contribute to the projects that boundary objects represent for the various communities that contribute to their existence. This entails a consideration of how the discourse around VPNs governs the limits of its normative place and use in society. As systems that are presented to users, we acknowledge the power of discourse to shape not only these experiences, but the regulation of their materiality. We assess discourses that surround search, discernment, choice, and activation of the apps that provide - in this case VPN services. That process builds data towards interpretation of the various facets of boundary objects that users are exposed to. In short, we seek to include market, experiential, and government pressures that come together at the boundaries of VPNs to create these shared yet disputed objects.

Understanding boundary objects *of* the internet, as opposed to *on* the internet has notable outcomes. The difference speaks to our interest in shared but contested objects that make the internet work, as opposed to things that work on the internet. As an example, social media work on the internet. Encryption makes the internet work. Passwords work on the internet. VPNs make the internet work (differently). Further, interpreting boundary objects of the internet also opens up the contextual heterogeneity that shapes specific objects like VPN via app and their larger industries. Finally, the focus on objects *of* the internet aligns with consideration of how boundary objects can become infrastructure. In Star's (2010, p. 605) words, some interpretations of a particular boundary object become 'standardised' and help define life past the socio-technical assemblage of the object itself.

In terms of relevance of our direction, there are clear and present debates on whether encryption is good, and what is it good for (and is to be legislated for), while VPNs provide a product category of 'encryption' that is marketed across multiple use cases, and contribute to the infrastructures *of* the internet. One resultant tack from technical to abstract for VPNs could imagine protocols (IPSec, SSTP, etc.); systems; anonymity and privacy devices; speech acts; commercial/market ecosystems. [1] These abstract concepts of market ecosystems for VPN content tack back to the technical through metaphors that reconfigure meaning: do VPN markets offer security and safety, or spying and vulnerability, a commercial data opportunity, or an ability to circumnavigate commercial or government censorship?

1. IPsec refers to 'Internet Protocol Security', which is a secure network protocol used to authenticate and encrypt data packets between two computers over an internet protocol network. SSTP refers to, 'Secure Socket Tunneling Protocol', which is a secure network protocol that also encrypts data packets between a VPN client and VPN server.

Methods to map VPNs as boundary objects of the internet

Our study design takes into account the jurisdictional geolocation and political context of Australia. People searching for VPNs in Australia will probably not be using VPNs. Australia provides an interesting case: an intellectual property morass of 'geoblocked' content streams that has allowed VPNs to proliferate (Lobato and Meese, 2016), while its data-retention regime has triggered fears of violation of privacy (Mann, 2018) in a developed and liberal democracy that is sliding to increasing authoritarian secrecy, surveillance, and suppression of speech (Molnar, 2017; Lidberg and Muller, 2019)

The specific 'in process' walkthrough of VPNs identified below show the discourses that users encounter when products are being explained to users. These steps involve movement of descriptions of the boundary object from the technical specifics and into the abstract metaphorical registers. First, as any potential user of VPNs might, we start as an (anonymised) google.com session that proceeds to work through a series of search decisions that expand discourses encouraging object knowledge, user discernment, choice, and activation.

User flow: search --> discourses encouraging activation --> discernment --> material choices --> activation

Following Light et al.'s (2018) walkthrough method, we followed the flow from search to activation to consider the environment (vision, operating models, and governance) that is disclosed from a user's position. Splitting from the app walkthrough method, the app interface itself is a less important site of (mis)trust building compared to those pre-interface experiences that engender its use. Search as research here is reflected through the socio-epistemological 'source standing' (Rogers, 2015 p. 99) that Google search offers queries to what a VPN is and does - we are less interested in what search excludes but its algorithmic authority in developing the boundary object. We also thus grant our user-process some breadth in activity, cross referencing common search results sites that explain the specific boundary objects and/or review of one product over another. The discourses presented illustrate a rich and multifaceted creation of boundary objects that allows deeper consideration of the relevant communities that create them.

Specifically, websites that compared VPNs, explained their purpose, and advertised their features factored in to the discourses that our search registered. While we systematically assess the available information to users seeking VPN functionality,

we did not move past the second page of google.com results as we felt this reflected long standing statistical implausibility (Van Deursen and Van Dijk, 2009). Specifically, we followed links positioned via google.com results with an ostensible click through rate of >5% (Advanced Web Ranking 2019 - *suggests 5 organic*). We also included the adwords entries displayed, usually four, which produced some overlap from organic results. We ran three anonymous search sets from different IPs in the Melbourne area and all returned the same list, albeit sometimes with different order of ads.

For our "VPN" search term Google auto-suggested adding the terms: free and Australia, so our assumed user followed Google's advice. This led to an overlapping set of 27 URLs from organic and adwords links, which we narrowed to recurring results that would ostensibly garner >5% clickthrough. One initial interesting finding is the homogeneity of these search results. 27 links (four ads per search, and five organic results) coalesce into 14 independent URL paths for the user to pursue. Of these, nine were various 'guides' to VPNs and five were VPN products themselves.

Based on these URLS, and significant linked pages (i.e., privacy policy, terms and conditions, 'about' pages, etc.) limited to two-hops, we open coded for 'vision', 'operating models' and 'governance' as per Light et al. (2018), making axial distinctions once we felt saturation was reached or our texts exhausted. The guides were coded somewhat differently as they reflected various levels of editorial and advertorial content about VPN boundary objects. The insights gained from these discourses suggest an assortment of themes that converge and conflict to create heterogeneous boundary objects of VPN. In these discourses we then consider how, when, and by whom, any tacking from the technical to the abstract can be observed, and how this relates to use and regulation of the technology.

Thus, a large part of our methods pursues interactions that are typical of user experience for acquiring VPN services, while also offering a systemic account of what such a user would experience. Our approach has distinct limits on these assumptions; the political economy of technical knowledge is experienced-based and gendered, as well as offers multifaceted 'search' layers and paths through friend groups and online forums, not to mention media market based measures like embedded links and ads. User generated narratives of VPN use, or how they change over time, while beyond the scope of this article, are another important avenue for inquiry. Thus, while precise, our method can only offer preliminary analysis of the object discourse presented to generic search-users. Future research that offers in depth ethnographic study to align registers of boundary object tacking to various socio-political contexts and practices, such as in fields of criminal and civil law, of-

fer novel sites for inquiry. Similarly, in-depth search as research techniques across geographies (Roberts, 2019 p. 107) would further enrich contributions to the range of communities encountering VPNs as boundary objects.

Nevertheless, our methodological move allows consideration of how and where populations in Australia might encounter the boundary object, and put this phenomenological understanding in relief to the other technical and social aspects that explain the objects to/by users as the objects 'tack' back and forth in meaning from the technical to the abstract. How does the performance of boundary objects inform formations of trust in the ecology of internet-based boundary objects? What do users experience when coming to terms with the object? How do decisions of VPN product use come about in relation to their construction as multifaceted boundary objects of the internet?

VPN data, and discussion

The two experiences prospective users of VPNs wade into via "VPN" search include direct product solicitation by VPN companies and second-hand aggregation sites that review VPN products. Both are designed to encourage use and enhanced sharing as reasons for using VPNs. Both sets of experiences detail distinct processes that come to terms with the multifaceted nature of what VPNs are and what they do as boundary objects of the internet.

The overwhelming sense of purpose or mission VPNs have, as advertised in the Australian geolocation, relates to 'security' and 'privacy'. [2] These two descriptors were consistent across all sites surveyed, while not always specifying what was being secured (from) or what was made private (or from whom). When security and privacy were explained, the latter was often referred to as a 'right' while the former was at risk 'nowadays' with increasing 'vulnerabilities' to 'cybercrime' and surveillance from criminals, ISPs, and governments. To a remarkable degree, the security and privacy measures VPNs employ were only spoken about in abstract terms, with only some sites mentioning but not explaining - nor offering links to explicate - specific protocols (IPSec, IKEv2, OpenVPN, and WireGuard). Cognitive metaphors (Lakoff, 1987) to describe VPNs were scarce, but included bears digging tunnels, armoured vans, packages in a box, parking garages, and traffic lights to signal technical standards. One site summarised:

2. While VPNs might have legal consequences for various reasons not limited to privacy and data protection questions, including intellectual property concerns, our data does not show that.

> Of necessity, discussion on VPN protocols and the nitty-gritty…is highly technical. Alternatively, our handy OpenVPN encryption chart uses a traffic-light system to give an at-a-glance assessment of the VPN's security that even the most tech-phobic out there should easily understand. (Crawford, 2018)

The standardisation of security and privacy as mission and vision might be construed in Star-ian terms with relation to infrastructure. But, we must remember that these descriptions provide facets of the boundary object that do not include regulators' accounts, for which further research is required but currently out of scope. When security is mentioned in more ordinal technical specifications, it is mostly described through superlative terms to differentiate market offerings as "best possible" or "military grade". Privacy is a feature described through banal adjective additives: "solid/great/strong"

Further, it seems that for a potential casual user of VPNs, when the object is signalled through security and privacy claims, it is disproportionately defined in terms of markets and features. These tack past protocols, private networks as systems, and gloss over VPNs' specific capacities (and limitations) as anonymity and privacy devices or speech acts. Instead, the discourse centres around commercial ecosystems and markets that offer products that are most often differentiated in terms of generic consumer features such as speed, ease of use, or customer service. The small minority (n:3) that mentioned Australia/Australians specifically, emphasised geo-blocked content and other Australian specific censorship or data-retention regimes in relation to mission or features past the more standard representations of privacy and security.

In terms of operating models presented, there were clear distinctions between review sites (n:10) and VPN product sites (n:4). Most review sites were upfront about their affiliate links business model, but there was a great deal of diversity in explaining editorial independence *vis-à-vis* recommendations. A minority of these sites' missions seemed to fit unabashed advertorial design and language, with vacuous descriptors and inaccurate or contradictory language designed to sell various VPN services. Some review sites cobbled together editorial content via keyword-sentences such as "global threats to individual privacy with long maintained rights to anonymity and net neutrality being undermined with a cloak of legitimacy" as reasons to consider VPNs. It seemed those review sites with the least to say about their business model offered the least capable advice on which service to choose: often the best picks that had been called out in various online media as products with obvious security threats or failures, for example. Most others offered VPNs as

a solution or partial solution to external threats, while only a small minority of sites considered the limits and risks of VPNs themselves. Only one review site reflexively questioned the VPN industry in terms of a trust equation that weighed relative risks: "It is important to keep in mind that when you are using a VPN, you are effectively transferring trust from your ISP to the VPN provider" (Protonvpn, 2017).

VPN businesses themselves offered surprisingly diverse business models. Past a simple subscription model, various VPN providers suggested their teams were available for IT security consultation, offered affiliate programmes for influencers (with up to 50% of subscription fees given to partners), as well as crowdsourced and foundation-funded revenue streams. This mix of business models reflects the diverse missions linked to the abstracted ideas of increasing 'security' and 'privacy' of users. These included profit motives and normative assumptions about the need to operationalise a 'free' internet as imagined "the way it was first envisioned – free from crime, censorship, and surveillance" (NordVPN, 2020).

The utopian and business desires of VPN providers are enforced by governance schemes that operationalise VPN user capacities into specific terms and conditions and require various forms of trust. Interestingly, we find a long list of forbidden activities on VPN services that border from abstractions of anything 'illegal' (jurisdiction not defined) to specific sets of practices that include creating spam, hacking, exploiting children, violating third party rights (e.g., IP and data privacy), harassment in various specified forms, promoting bigotry, use for military purposes, etc. These normative qualifications are not standardised across VPN providers, nor do they seem to be tied to specific geo-jurisdictional structures. The VPN businesses seem largely to make these terms up to protect themselves and their users as they see fit, and to craft the communicative world they wish to enable.

The terms and conditions offer an interesting 'middle ground' between the technical and abstract to understand the boundary object of VPNs. On the one hand they do not detail technical specificities of why and what can(not) be accomplished via VPNs. On the other, while some reference violation of "general ethic or moral norms, good customs and fair conduct norms", others offer a level of specificity that tacks to specific types of harm or abuse. VPN vendors chose to highlight activities they feel are outside the communicative world they are creating and do so at a level—not of legal or technical information—but use practice that constitutes problematic activity they do not want to be associated with.

Whether internal governance discourse is based on public perception/public rela-

tions framing or past alleged abuses is unclear. Regardless, these differences in terms and conditions show the multiplicity of worlds that VPN vendors and users think the products afford; security and privacy (and from whom and for what) is contested across the VPN ecosystem.

At the same time, the underlying technical infrastructures that afford these specific communication regimes are largely unmentioned. Encryption technologies within the VPN product work unseen to enable freedom from surveillance and censorship. What is made visible in the terms and conditions seems designed to guide the political and policing structures that relate to affordances in practice (Costa, 2019) made possible through these technical capacities.

Another topic that is frequently tied to VPNs in our corpus are logs of use(r) data. Almost all VPNs claim they do not keep any logs. Others claim that while they once did keep some basic activity logs such as time-stamped user access (as proven in assistance to police investigations), now claim they no longer keep logs. In any of these scenarios, users are supposed to trust these statements. Interestingly, this trust is manufactured without infrastructure; there is no active or real-time way to check that non-existent logs don't exist. This type of trust harkens back to Web 1.0 interactions, where anonymous users created communities on an electronic frontier (Rheingold, 1993), as opposed to gardens walled by Web 2.0 corporate regulations. This is the difference between trusting someone on Craigslist and trusting someone on AirBnB (Lingel, 2020). Traceable audits of actor behaviour are not available in the former set of relations.

Some VPN providers seek to buttress trust via audits that employ trusted third parties (e.g., PwC) to explore and back claims. This is interesting in the creation of boundary objects for two reasons. First, the requirement for verification, or infrastructures of trust around consensual claims (you pay me, I don't log you) negates the ethos of an internet free from surveillance and the normative project that extends from VPNs. Second, the audits are unsatisfactorily focussed on the past; each auditor can only provide witness on what is, not what was, or will become via a few extra lines of code in the VPN. Note here how issues of (dis)trust offer competing valences in respect to the object itself and the systems that the object is acting upon. How users interpret the object says much about how they situate trust in relation to the policing/political actions that the object acts upon.

Conclusion

Our discussion on VPNs brings to light how users of internet objects come to trust

them for what they are and what they do, and the extent these trusts are misplaced in relation to the connective polysemy (Gal, 2018) that boundary objects provide as larger ecosystems. Here, among other normative/political pressures, we again find a unique ability of internet-based boundary objects to 'tack' back and forth from abstract to technical in a way that concurrently translates meaning across communities to engender (mis)trust. For instance, trust in mathematics belies mistrust in application deployment, the existence of nefarious geopolitical actors, and so on.

Our work suggests the back and forth 'tacking' of abstract to concrete does not just manifest as a universal and singular, but is made manifest from multiple community vantage points. This complexification shows how digital objects of the internet feed and are fed by multiple use cases and relational practices across commercial, security, rights based, and identity practices that they underpin, undercut or act upon. Users trusting the politics of one case may miss a need to police the other; we conclude by contextualising these concerns for future research *of* the internet.

Future research might then look at how 'metaphor' is used to shape multiple boundary objects through contextualised user and regulatory imaginaries about how boundary objects of the internet (i) make sense of the technology as a tool, (ii) consider and condition their contextual understanding of affordances-in-practice, and (iii) have follow on implications for attempts at regulation, both by entities promoting the object and institutional forms of governing. We hope future research can develop this methodology in ways that combine the best of recent progressions of walkthrough methods and Star's concept of the boundary object to enhance capacity for understanding boundary objects of the internet. This paper has offered one such step by walking through the interfaces that craft user perceptions of encountering and deciding to interact with the VPN boundary object.

References

Basques, K. (2015). *Why HTTPS matters.* Google Web.Dev. https://web.dev/why-https-matters/

Bowker, G. C., Timmermans, S., Clarke, A. E., & Balka, E. (Eds.). (2016). *Boundary objects and beyond: Working with Leigh Star*. MIT Press.

Costa, E. (2019). Affordances-in-practice: An ethnographic critique of social media logic and context collapse. *New Media & Society*, *20*(10). https://doi.org/10.1177/1461444818756290

Crawford, D. (2018). *ProPrivacy's VPN Review Process Overview*. ProPrivacy. https://proprivacy.com/vpn/guides/review-process-overview

DeNardis, L. (2014). *The global war for internet governance*. Yale University Press. https://doi.org/10.12987/yale/9780300181357.001.0001

Digital Science & Research Solutions. (2020). *Overview: Language, Communciation, and Culture; Boundary Object*. Dimensions. https://app.dimensions.ai/analytics/publication/overview/timeline?search_mode=content&search_text=%22Boundary%20Object%22&search_type=kws&search_field=full_search&or_facet_for=2220

Foucault, M. (1994). *Dits et Ècrits: Vol. IV*. Gallimard.

Fox, N. J. (2011). Boundary Objects, Social Meanings and the Success of New Technologies. *Sociology*, *45*(1), 70–85. https://doi.org/10.1177/0038038510387196

Gal, N. (2018). Ironic humor on social media as participatory boundary work. *New Media & Society*, *21*(3), 729–749. https://doi.org/10.1177/1461444818805719

Gill, L. (2018). Law, Metaphor, and the Encrypted Machine. *Osgoode Hall Law Journal*, *55*(2). https://digitalcommons.osgoode.yorku.ca/ohlj/vol55/iss2/3/

Heemsbergen, L. (2019). Killing secrets from Panama to Paradise: Understanding the ICIJ through bifurcating communicative and political affordances. *New Media & Society*, *21*(3), 693–711. https://doi.org/10.1177/1461444818804847

Huvila, I. (2019). Authoring social reality with documents: From authorship of documents and documentary boundary objects to practical authorship. *Journal of Documentation*, *75*(1), 44–61. https://doi.org/10.1108/JD-04-2018-0063

Hwang, T., & Levy, K. (2015). 'The cloud' and other dangerous metaphors. *The Atlantic*. https://www.theatlantic.com/technology/archive/2015/01/the-cloud-and-other-dangerous-metaphors/384518/

Ikram, M., Vallina-Rodriguez, N., & Seneviratne, S. (2016). An analysis of the privacy and security risks of android vpn permission-enabled apps. *Proceedings of the 2016 Internet Measurement Conference*, 349–364. https://doi.org/10.1145/2987443.2987471

Johnstone, B. (2018). *Discourse analysis* (3rd ed.). John Wiley & Sons.

Jones, R. H., Chik, A., & Hafner, C. A. (Eds.). (2015). *Discourse and digital practices: Doing discourse analysis in the digital age*. Routledge. https://doi.org/10.4324/9781315726465

Lakoff, G. (1987). *Women, fire, and dangerous things: What categories reveal about the mind*. University of Chicago Press.

Latour, B. (2005). *Reassembling the social: An introduction to actor-network-theory*. Oxford University Press.

Leigh Star, S. (2010). This is not a boundary object: Reflections on the origin of a concept. *Science, Technology, & Human Values*, *35*(5), 601–617. https://doi.org/10.1177/0162243910377624

Lewis, S. C., & Usher, N. (2016). Trading zones, boundary objects, and the pursuit of news innovation: A case study of journalists and programmers. *Convergen*, *22*(5), 543–560. https://doi.org/10.1177/1354856515623865

Lidberg, J., & Muller, D. (2018). In the Name of Security Secrecy. *Surveillance and Journalism*.

Light, B., Burgess, J., & Duguay, S. (2018). The Walkthrough Method: An Approach to the Study of Apps. *New Media & Society*, *20*(3), 881–900. https://doi.org/10.1177/1461444816675438

Lingel, J. (2020). *An Internet for the People: The Politics and Promise of Craigslist*. Princeton University Press. https://doi.org/10.23943/princeton/9780691188904.001.0001

Lobato, R., & Meese, J. (2016). *Australia: Circumvention goes mainstream* (E. D. I. T. E. D. B. Y. R. A. M. O. N. LOBATO, Ed.).

Mann, M., Daly, A., Wilson, M., & Suzor, N. (2018). The Limits of (Digital) Constitutionalism: Exploring the Privacy-Security (Im)Balance in Australia. *International Communication Gazette*, *80*(4), 369–384. https://doi.org/10.1177/1748048518757141

Mautner, G. (2005). Time to get wired: Using web-based corpora in critical discourse analysis. *Discourse & Society*, *16*(6), 809–828. https://doi.org/10.1177/0957926505056661

Mol, A. (1999). Ontological politics. A word and some questions. *Sociological Review*, *47*(1), 74–89. https://doi.org/10.1111/j.1467-954X.1999.tb03483.x

Molnar, A. (2017). Technology, Law, and the Formation of (il)Liberal Democracy? *Surveillance & Society*, *15*(3/4), 381–388. https://doi.org/10.24908/ss.v15i3/4.6645

NordVPN. (2020). *Social Responsibility: Promoting equal opportunities in the digital age*. NordVPN. https://nordvpn.com/social-responsibility/

Olsen, J.-K. B., & Selinger, E. (Eds.). (2007). *Philosophy of technology: 5 questions*. Automatic Press.

Østerlund, C., & Crowston, K. (2019). Documentation and access to knowledge in online communities: Know your audience and write appropriately? *Journal of the Association for Information Science and Technology*. https://doi.org/10.1002/asi.24152

Poulsen, S. V. (2018). Becoming a semiotic technology – a historical study of Instagram's tools for making and sharing photos and videos. *Internet Histories*, *2*(1–2), 121–139. https://doi.org/10.1080/24701475.2018.1459350

ProtonVPN. (2017). Understanding the VPN Threat Model [Blog post]. *ProtonVPN Blog*. https://protonvpn.com/blog/threat-model/

Rancière, J. (2006). *Hatred of democracy* (S. Corcoran, Trans.). Verso.

Rheingold, H. (1993). *The virtual community: Homesteading on the electronic frontier*. Addison-Wesley Publishing Company.

Rogers, R. (2013). *Digital methods*. MIT Press.

Rogers, R. (2019). *Doing digital methods*. SAGE Publications Limited.

Shepherd, T. (2018). Discursive Legitimation in the Cultures of Internet Policymaking. *Communication Culture & Critique*, *11*(2), 231–246. https://doi.org/10.1093/ccc/tcx020

Published by
Alexander von Humboldt Institute for Internet and Society

in cooperation with
CREATe
centre internet et société
R&I IN3 Internet interdisciplinary Institute
Universitat Oberta de Catalunya