Selected Papers of #AoIR2019:
The 20th Annual Conference of the
Association of Internet Researchers
Brisbane, Australia / 2-5 October 2019

VPNs AND ENCRYPTION AS BOUNDARY OBJECTS OF THE INTERNET: (MIS)TRUST IN THE TRANSLATION(S)

Luke Heemsbergen, Deakin University

Adam Molnar, Waterloo University

Introduction

How do users come to trust VPNs? How do they understand end-to-end encrypted messaging technologies? How can we discern what these objects are as they tack back and forth between metaphor and technical processes to garner usership and critique? This paper aims to answer these questions by considering VPNs and e2e encryption as boundary objects of the internet pertinent to a study of (dis)trust in the system.

Our aim is to follow Star's (2010: 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. Our contribution adds to the literature in three ways, the first is empirical, unpacking VPNs and e2e encryption as boundary objects, which is novel for the literature. The second is through an exegesis of boundary objects 'on' the internet to consider conceptualizing objects 'of' the internet, which opens a fruitful reconfiguration of Star's work for internet research. And lastly, it sheds light on the ways that competing and sometimes contradictory symbolic registers of technology have profound implications for socio-material practices online.

Existing Research Literature

In the five years leading to this paper's writing, citations to boundary objects have more than tripled in literatures categorized as Communication and Media Studies, Cultural Studies, and Film, Television and Digital Media (Dimensions 2019). This trajectory is owing to a revitalized consideration of the work of Susan Leigh Star (see Bowker et al.,

Suggested Citation (APA): Heemsbergen, L., & Molnar, A. (2019, October 2-5). *VPNs and Encryption as Boundary Objects of the Internet*. Paper presented at AoIR 2019: The 20th Annual Conference of the Association of Internet Researchers. Brisbane, Australia: AoIR. Retrieved from http://spir.aoir.org.

2016) translated from science and technology studies, while also showing how the concept of boundary objects proves useful to conceptualize and configure the various experiential objects that come into existence via technological practices acted upon and through digital, networked - and as consequence - polysemic worlds.

A sample of recent research utilizing boundary objects that is of interest to internet researches includes news and technology nexus in terms of process, participation and curation (Lewis and Usher, 2016), digitization and mixed document authorship (Huvila, 2019), FLOSS documentation (Østerlund and Crowston, 2019), humor online (Gal, 2018), and charting discourses of power legitimization via competing images of the Internet itself (Shepherd, 2018). What is perhaps missing from this corpus is a distinction of and reflection on how these objects may be thought as *of* the internet; artefacts that are sung into existence from and through distinct online cultures, practices and needs of internet use(rs), as they tack back and forth between their technical ontologies and metaphorical claims.

Methodology

For AOIR we lend such research towards how such objects come to be (dis)trusted, and then policed and politicized (see Rancière and Corcoran, 2006: 29-30). In this way, the paper returns to the ethos of Star's work by considering a feminist approach to technology studies, which for Star, linked lived experience, technologies, and silences (in Olsen, 2007: 227) in ways that proved political. Our work enables boundary objects to, more than explicate functional processes within communities, consider socio-technical relationships made through them (Star, 2010) and the extent that these objects are facilitative or inhibitory (Fox, 2011) of cross-boundary communication. Thus, our discussion considers: contexts from which a boundary object is embedded (commercial, cultural, etc), the ways in which it is interpreted, and explanations that assert some intrinsic or essential property of the object that explains its performance.

Our methods to do so present a 'work in process' that synthesize the strengths of discourse analysis for internet related phenomenon (Brock, 2018) and the experiential phenomenological modes of inquiry that have more recently brought to life through walkthrough methods (Light, Burgess, & Duguay, 2018).

This is not to discount notable differences across apps and their effects; peculiarities of interface (Poulsen, 2018) and affordances can have a profound impact on use cases and social outcomes. Yet, (lack of) user interfaces in VPNs demonstrate how infrastructural change 'of' the internet have effects that are not apparent to users in HCI terms alone.

Discussion

Our work on 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 and Corcoran, 2006) that shape and shift meaning making through communities of practice linked to the various interpretive objects identified.

Likewise for VPNs we consider interpretations of the object as they flow through protocols (eg. SSTP); virtual private networks as system; anonymity and privacy devices; speech acts; commercial/market ecosystems; malware. 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. For instance, technical definitions of Malware and some VPN products intermesh (Ikram et al., 2016) on technical standpoints, while users (dis)trust each in dichotomous ways that uphold political-economic (or break down socio-political) systems.

Our discussion on VPNs and encryption 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. Future work on a more systematic appraisal of discourses around these boundary objects, including public policy and market voices is warranted through extension of our methods.

Conclusion

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 contextualizing these concerns for future research 'of' the internet.

References

Bowker GC, Timmermans S, Clarke AE, et al. (2016) *Boundary objects and beyond: Working with Leigh Star*: MIT Press.

Brock, A. (2018). Critical technocultural discourse analysis. *New Media & Society, 20*(3), 1012-1030.

Fox NJ. (2011) Boundary Objects, Social Meanings and the Success of New Technologies. *Sociology* 45(1): 70-85.

Gal N. (2018) Ironic humor on social media as participatory boundary work. *New Media & Society*: 1461444818805719.
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.
Ikram M, Vallina-Rodriguez N, Seneviratne S, et al. (2016) An analysis of the privacy and security risks of android vpn permission-enabled apps. *Proceedings of the 2016 Internet Measurement Conference.* ACM, 349-364.
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.
Lewis SC and Usher N. (2016) Trading zones, boundary objects, and the pursuit of news innovation: A case study of journalists and programmers. *Convergence* 22(5): 543-560.
Light, B., Burgess, J., & Duguay, S. (2018). The walkthrough method: An approach to the study of apps. *New Media & Society, 20*(3), 881-900.
Olsen J-KB. (2007) *Philosophy of technology : 5 questions,* [Erscheinungsort nicht ermittelbar]: Automatic Press.
Østerlund C and 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*.
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.
Rancière J and Corcoran S. (2006) *Hatred of democracy*: Verso London.
Shepherd T. (2018) Discursive Legitimation in the Cultures of Internet Policymaking. *Communication Culture & Critique* 11(2): 231-246.