Surveillance & Society

Dialogue

The Trap of Tracking: Digital Methods, Surveillance, and the Far Right

Robert Topinka
Birkbeck, University of London, UK
r.topinka@bbk.ac.uk

Alan Finlayson
University of East Anglia, UK
a.finlayson@uea.ac.uk

Cassian Osborne-Carey
University of Arts London, UK
cassian.osborne-carey@warwick.ac.uk

Introduction

Computational methods and network analysis are vital means for understanding how digital platforms are employed by political extremists. Western democracies focused on the security threat of jihadi extremism have been comparatively slow to recognise the threat of the far-right extremism (see Crosby 2021 and Rostami and Askanius 2021). Understandably, scholars have reacted to the knowledge gap about far-right extremists by practicing what we call "surveillance-as-method," or the use of computational methods to gather data on far-right activities on digital media platforms, typically in order to track keywords or phrases or to map network connections. As we suggest here, the limits of surveillance-as-method include reproducing problems associated with state surveillance (van Dijck 2014) and underestimating the messiness (Pink, Lanzeni, and Horst 2018) of digital culture. Those limits need to be appreciated and approaches combined if we are to understand online politics. In this dialogue, we urge greater caution and reflexivity in reproducing surveillant methods, and greater attention to the historical, ideological context of far-right politics.

This is for two key reasons. Firstly, surveillance-as-method reinforces an assumption that digital extremism needs only to be seen to be understood and addressed; that once it is revealed as extreme it will be seen for what it is and wither. Yet, many far-right extremists welcome academic exposure and critique because they can caricature and mock it as part of a wider ideological assault on universities, mainstream media, and liberalism. Beyond the risk of supplying far-right groups with "the oxygen of amplification" (Phillips 2018), academic surveillance risks supplying the far-right with what they want: evidence supporting their claim that the political mainstream is intolerant and exclusionary, in contrast to their pioneer-spirit of independence and freedom. This tactic is a novel "anticipatory data practice" (Kazansky 2021) that turns surveillance back on the surveillant, welcoming attention as evidence of politically motivated attack.

This problem takes us to our second point: surveillance-as-method reinforces a tactic commonly used by right-wing extremists, who claim to be "keeping an eye on" liberals, the left, and their purported co-conspirators in the mainstream media, exposing them as biased ideologues driven by an agenda. Here, surveillance becomes a central means of doing politics as a public revelation of "the truth about" politics and "what they don't want you to know" (Finlayson 2020). Such revelation affirms and sustains common-sense ideological divisions between good and bad, us and them. If scholars replicate this conflation of surveillance-as-method with surveillance-as-critique (assuming that, once unmasked as far-right politics, it has been shown to be an instance of what "everyone knows" is a bad thing), they risk perpetuating an

Topkinka, Robert, Alan Finlayson, and Cassian Osborne-Carey. 2021. The Trap of Tracking: Digital Methods, Surveillance, and the Far Right. *Surveillance & Society* 19(3): 384-388.
https://ojs.library.queensu.ca/index.php/surveillance-and-society/index | ISSN: 1477-7487

approach to politics that is constituted by, rather than derived from, the capacities and affordances of digital media. Chris Anderson (2008) somewhat notoriously argued in *Wired* that theories of human behaviour are obsolete; we don't need to know why people do what they do when we can "track and measure it with unprecedented fidelity" and "with enough data, the numbers speak for themselves." If we take this route, then politics will be nothing more or less than a conflict between "alternative facts," competing practices of surveillance that reinforce the assumptions of their respective communities.

We are not opposed to surveillance-as-method, but we argue that we also need strategies for moving beyond surveillance, integrating findings with theoretically and historically informed analysis of ideologies of the far right.

Supplementing the State

The global rise of a digitally powered far-right has been well-documented (Hawley 2017; Daniels 2018; Beran 2019; Fielitz and Thurston 2019). However, as Crosby (2021) shows in the case of Canada and Rostami and Askanius (2021) in that of Sweden, state actors have been slow to grapple with the threat of far-right extremism. The tracking and tracing of activity amongst these actors frequently falls to non-governmental organisations and academics using what we describe here as surveillance-as-method, drawing on computational methods to scrape and collect large datasets of posts, comments, and profile markers on platforms ranging from Twitter to Telegram. These datasets are analysed, categorised, and quantified in ways intended to reveal its dangerously underappreciated volume and spread. Beyond the academy, activists and anti-fascist groups adopt similar methods as they monitor, record, and publicise the goals and desires of far-right communities in order to expose and incriminate participants. Surveillance and "capture" (Agre 1994) are folded together. But it is not clear whether this necessary work is sufficient for political analysis and critique.

Surveillance, Politics, Critique

Although the alt-right and other far-right reactionary groups predate the 2016 US presidential election, the Trump campaign's willingness to recirculate alt-right memes brought these digital political subcultures to mainstream attention. The most infamous portrayed Trump as "Pepe the Frog," a formerly apolitical online comic character ironically repurposed by online communities into a far-right signifier. The Clinton campaign's "Pepe the Frog explainer"—since scrubbed from the campaign website—accurately but too earnestly explained that Pepe was, in fact, a white nationalist symbol. The problem with these explainers wasn't only that they supplied the "oxygen of amplification" to the alt-right. They also misunderstood the place of such digital political subcultures within a wider political ecology. They assumed that in "outing" digital extremism it would also be understood and addressed. The 4chan imageboard /pol/, on which Pepe was born as a right-wing meme, is perhaps obscure when seen by anyone more familiar with the user-friendly interfaces of Facebook or Twitter. But political sentiments expressed on 4chan's /pol/ board are not hidden. Racism, misogyny, and extremism are clearly and confidently expressed there. Pepe was not a covert symbol but a mascot, typically used to illustrate commentators' alliance with the alt-right and intended to "trigger" audiences of earnest liberals. The Clinton campaign was right that Pepe is a meme favored among white nationalists but missed its part in a wider political culture of trolling. Making a heavily favored presidential candidate worry over a cartoon frog was a propaganda win for alt-right communities.

Commentators have become alert to the weaponised irony of the alt-right and of the difficulties of ascertaining meaning on the "ambivalent internet" (Phillips and Milner 2017). This ambivalence problematises the quantification of right-wing subcultural tropes, memes, and in-group references. The tools of surveillance-as-method, including data-scraping, network-graphing, and keyword-tracking, are vital for identifying far-right activity online and raising awareness. But revealing their symbols, memes, and in-group references is not enough. In the "mask culture" (de Zeeuw and Tuters 2020: 215) of 4chan, anonymity and irony dominate, making it impossible to connect posts to an author or to assign a meaning to the content

of any post. But anonymity and ambivalence are not the same as obscurity. Simple exposure cannot unmask the sources of content born from a medium and a culture as much as from individual authors. Digital content circulates as untethered shares, replies, and remixes. Surveillance-as-method cannot help us make sense of subcultural spaces that are openly *and* ironically extremist. Indeed, such irony and anonymity are forms of "vernacular resistance" (Brunton and Nissenbaum 2011) to the "dataveillance" (van Dijck 2014: 198) built into digital environments. Surveillance-as-method can show whether extremist content exists but not what the context of that content is, nor the new ways in which it enacts politics.

In addition to the tracing and tracking of surveillance-as-method, we propose attending to the digital *forms* that structure and give rise to extremist propaganda online. Digital data is "a complex epistemic object" (Aradau and Blanke 2015: 4) that is not given but is always "*in-formation*" (Reigeluth 2014: 252). Consider, for example, the alt-right and the gamified conspiracy theory QAnon. At one level, these are nothing alike. Where the alt-right is self-consciously edgy and ironic, QAnon followers tend to be earnest and sincere. Where the alt-right skews young and male (Hawley 2017), QAnon is popular among women and mothers (Bloom and Moskalenko 2021). Yet both share origins in the obscurantist style of 4chan. Both coordinate an in-group through a referential repertoire significant only to the initiated, from "pede"[1] to "cuck"[2] to "breadcrumbs"[3] and "baking."[4] Both found a hero in Trump. Both have a clear—and often shared—set of enemies among the liberal elite. Both gain momentum from mainstream critiques and attempts to track and trace their every move. And, it is worth emphasizing, both operate in the open. Their references may be for the already-initiated, but they are not secrets. Both groups actively propagandise. And, as we are arguing here, both feed on mainstream criticism, which only provides proof of their enemies and new content to caricature.

What this suggests is that the *form* of such groups may be as significant as their content (see Topinka, forthcoming). The sociologist Georg Simmel (1909: 302) uses the term "forms of association" to describe the material formal structures through which "human beings arrange themselves in association." For extreme groups such as the alt-right and QAnon, these "forms of association" are linked with what media scholars call "affordances," the properties of websites, platforms, interfaces, and other digital media that make certain kinds of action possible (and others harder or impossible). We suggest that scholarly attention to extreme politics online ought to focus more on this overall form, the ecology, of which they are a singular manifestation. Such analysis of the "form" of communicative intervention necessitates qualitative interpretation informed by a theoretical understanding of how ideologies—and those of the right and far-right in particular—work so that we can make sense of how the standard argumentational patterns of such ideologies interact with the digital system.

Consider, for instance, the idea of the "echo chamber"—that digital media intensify partisan belonging because people are exposed only to material from within their ideological universe. The reality is somewhat different. Partisan online sites draw on, repost, and address material from outside their "echo chamber." But they treat it as primary evidence of the lies, deceptions, and conspiracies against which participants are organised. They compete to find examples and to demonstrate their capacity at interpreting and explaining what it "really" means. In this way, they are themselves engaging in a conflation of surveillance-as-method with surveillance-as-critique. They are ideal participants within digital technoculture, whom Jodi Dean (2001: 625) describes as "searching, suspicious subjects ever clicking for more information, ever drawn to uncover the secret and find out for themselves." Paradoxically, this is a politics that is both extremist and entirely normal for this culture, these platforms, and their affordances: we surveil the other side, bringing our findings back to our own side where we measure how far beyond the pale they are. To understand a

[1] As in "centipede"—the moniker adopted by Trump fans on Reddit, indicating their "nimble navigation" of online news and information in curating pro-Trump discourse.

[2] Shortened from cuckold as a pejorative directed at liberals and Trump opponents.

[3] Referring to the obscure hints at a liberal conspiracy offered by "Q," the alleged Washington insider posting on 4chan and later 8kun.

[4] The term QAnon followers use to describe their work interpreting the "breadcrumbs" or obscure hints.

politics today, as well as mapping, measuring, and interpreting its utterances, we must locate it in relation to the digital culture of which it is a part and explain how the ideological propositions making up its content are made possible, modified, and circulated by the form to which they belong.

Conclusion

Online, political activists surveil each other. They monitor each other's traffic, establish each other's identity, and expose the "agenda" to which each is working. In noting this, we do not for a moment intend to suggest that the two sides are the same, or that, as Trump might put it, there are bad people on both sides. Our point is that this situation is one part of a radically transformed environment within which political ideas are formed, articulated, and circulated. If we do not understand that, we do not understand what is happening.

As noted above, there has been a tendency on the part of security forces to underplay the extent of ideologically organised and motivated domestic terrorism in contrast to Islamist political violence. As Ganesh (2021) shows, while Jihadi propaganda is banned and deplatformed the rhetoric of the far right remains online, their presence justified in the language of "free speech protection." This is indicative of the fact that what they say is precisely *not* beyond the pale or guaranteed to be seen as unacceptable once exposed for what it is. On the contrary, theirs is a rhetoric that overlaps with, draws from, and feeds into a wider ecosystem. In this context, analysis cannot only count and describe what is there, and it can't simply securitise what it finds. It must put things properly in their place.

Acknowledgments

Supported by the AHRC grant-funded project "Political Ideology, Rhetoric and Aesthetics in the Twenty-First Century: The Case of the 'Alt-Right,'" accessible here: https://gtr.ukri.org/projects?ref=AH%2FR001197%2F1.

References

Agre, Philip E. 1994. Surveillance and Capture: Two Models of Privacy. *The Information Society* 10 (2): 101–127.

Anderson, Chris. 2008. The End of Theory: The Data Deluge Makes the Scientific Method Obsolete. *Wired*, June 23. https://www.wired.com/2008/06/pb-theory/ [accessed August 20, 2021].

Aradau, Claudia, and Tobias Blanke. 2015. The (Big) Data-Security Assemblage: Knowledge and Critique. *Big Data & Society* 2 (2). https://doi.org/10.1177/2053951715609066.

Beran, Dale. 2019. *It Came from Something Awful*. New York: All Points Books.

Bloom, Mia, and Sophia Moskalenko. 2021. *Pastels and Pedophiles: Inside the Mind of QAnon*. Stanford, CA: Stanford University Press.

Brunton, Finn, and Helen Nissenbaum. 2011. Vernacular Resistance to Data Collection and Analysis: A Political Theory of Obfuscation. *First Monday* 16 (5). https://doi.org/10.5210/fm.v16i5.3493.

Crosby, Andrew. 2021. Policing Right-Wing Extremism in Canada: Threat Frames, Ideological Motivation, and Societal Implications. *Surveillance & Society* 19 (3): 359–363.

Dean, Jodi. 2001. Publicity's Secret. *Political Theory* 29 (5): 624–650.

Daniels, Jessie. 2018 The Algorithmic Rise of the "Alt-Right." *Contexts* 17 (1): 60–65.

Fielitz, Maik, and Nick Thurston. 2018. *Post-Digital Cultures of the Far Right: Online Actions and Offline Consequences in Europe and the US*. New York: Columbia University Press.

Finlayson, Alan. 2020. YouTube and Political Ideologies: Technology, Populism and Rhetorical Form. *Political Studies*. https://doi.org/10.1177/0032321720934630.

Ganesh, Bharath. 2021. How to Counter White Supremacist Extremists Online. *Foreign Policy*, January 28. https://foreignpolicy.com/2021/01/28/how-to-counter-white-supremacist-extremists-online/ [accessed August 20, 2021].

Hawley, George. 2017. *Making Sense of the Alt-Right*. New York: Columbia University Press.

Kazansky, Becky. 2021. "It Depends on Your Threat Model": The Anticipatory Dimensions of Resistance to Data-Driven Surveillance. *Big Data & Society* 8 (1). https://doi.org/10.1177/2053951720985557.

Phillips, Whitney. 2018. The Oxygen of Amplification. *Data & Society*, May 22. https://datasociety.net/library/oxygen-of-amplification/ [accessed August 20 2021].

Phillips, Whitney, and Ryan M Milner. 2017. *The Ambivalent Internet: Mischief, Oddity, and Antagonism Online*. Cambridge, UK: Polity Press.

Pink, Sarah, Debora Lanzeni, and Heather Horst. 2018. Data Anxieties: Finding Trust in Everyday Digital Mess. *Big Data & Society* 5 (1). https://doi.org/10.1177/2053951718756685.

Reigeluth, Tyler Butler. 2014. Why Data Is Not Enough: Digital Traces as Control of Self and Self-Control. *Surveillance & Society* 12 (2): 243–254.

Rostami, Amir, and Tina Askanius. 2021. State Surveillance of Violent Extremism and Threats of White Supremacist Violence in Sweden. *Surveillance & Society* 19 (3): 369–373.

Simmel, Georg. 1909. The Problem of Sociology. *The American Journal of Sociology* 25 (3): 289–320.

Topinka, Robert. Forthcoming. The Politics of Anti-Discourse: Copypasta, the Alt-Right, and the Rhetoric of Form. *Theory & Event*.

van Dijck, José. 2014. Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology. *Surveillance & Society* 12 (2): 197–208.

Zeeuw, Daniël de, and Marc Tuters. 2020. Teh Internet Is Serious Business: On the Deep Vernacular Web and Its Discontents. *Cultural Politics* 16 (2): 214–232.