Selected Papers of #AoIR2023:
The 24th Annual Conference of the
Association of Internet Researchers
Philadelphia, PA, USA / 18-21 Oct 2023

REVOLUTIONARY TACTICS: ABOLISH PRIVACY

This paper addresses internet scholars who promote online privacy. This paper rejects privacy as a neoliberal agenda.

1. Privacy is not Social Justice

Corporate online platforms are built on racial capitalism, to quote Cedric Robinson, designed to make profit by marginalizing Blackness. Black, working class, Indigenous, refugee, disabled communities are further marginalized by automated health care (Cruz 2022), policing (Brayne 2020), welfare qualifications, refugee status (Molnar and Gill, 2018), democratic voting rights (Noble 2018), and access to information seen in Meta's current restrictions on documenting Palestinian casualties.

Privacy will not protect us from these harms. However many excellent alternatives have been proposed, for example in a study of predictive policing (Dixon-Roman, Nyame-Mensah, Allison Russell 2019): First, they call for the decriminalization of poverty and self-defense, and instead, a focus on the far more socially expensive problem of white collar crime. Second, they call for data audits, so that individuals can object to attributes generated by racist training data. Third, they call for a turn of the predictive gaze instead onto the perpetrators by training AI to forecast excessive violence by the police and military. Fourth, they ambitiously but crucially call for the dismantling of the category of human, which excludes Black people and demotes Indigenous, disabled and queer people not by mistake but by design.

These authors invoke the Black Radical tradition, Robinson's thesis that the reduction of Black people to private property is the basis of capitalism. In his urgent 2020 political pamphlet *On Property*, Rinaldo Walcott argues that private property justifies carceral systems and the un-privacy of a caged class (Walcott, 2020; Hill 2016). In *Dark Matters*, Simone Browne shows how surveillance is born out of the selective deprivation of Black privacy and the desire to claim Blackness as the private property of whiteness. Whiteness as Cheryl Harris reminds us, is the only basis of private ownership. Unprivacy is fundamental to able bodied supremacy, as Crip theorist Mia Mingus (2017) writes, forcing disabled people into intimate disclosures on a daily basis as a requirement for basic needs and access. Queer theorist Laurent Berlant argues that

Suggested Citation (APA): Lim, E. (2023). "Abolish privacy." Panel presented at AoIR 2023: The 24th Annual Conference of the Association of Internet Researchers. Philadelphia: AoIR. Retrieved from http://spir.aoir.org.

constitutional American “personhood” is historically defined by the ownership of slaves within a private realm; privacy that protects nobody from the abuse of white men (p. 18). Critical race, feminists, queer and crip theory relentlessly problematizes privacy as an ideology.

Activists must not invoke the specter of privacy in our efforts to shield and care for each other. Our resistance movements have always called for its opposite: interdependence and collective solidarity, or to quote Wendy Chun (2014), the right to be vulnerable online. She cites the Toronto slutwalk, as well as South Asian feminist activists fighting gender-based violence. These women call for the right of marginalized communities to take risks in public without facing violence. To Quote Chun, “rather than fight for privacy—for hermeneutic bubbles of protection—we need to fight for the right to loiter.”

2. Privacy is inextricable from private property.

One might argue that calls for online privacy are not the same as calls for private property, but in the discourse surrounding online privacy, this distinction is not made. This is the result of several critical discourse analyses of mainstream privacy rhetoric concluding that privacy narratives focus on customer rights, government and corporate transparency, and threats to democracy (Connor and Doan, 2021). McDonald and Forte complement these findings with a discourse analysis of blog posts written by the newsrooms of Meta and Snapchat, which strive to shape media privacy rhetoric towards a focus on personal authenticity, safety and data impermanence; in other words the assertion and expansion of private property.

David Carroll’s words especially alarmed broad audiences in his opening lines of Netflix documentary *The Great Hack,* “All of my interactions… all collected in real time and attached to my identity, giving any buyer direct access to my emotional pulse” (The Great Hack, 2019). *Wired Magazine* called the documentary a “horror movie” that “brings our data nightmare to life” (Dreyfuss, 2019). However in media appearances that year, Carroll made a concerted effort to temper those words, and in fact, critique the documentary’s overall message (Fischer, 2019), “My pursuit [in the film] is a highly individualized narrative, which obscures the reality that it's a story about all of us…it does require a collective response. Data protection is a structural problem” (Fischer, 2019). Carroll emphasizes that data infractions are not about *individual* privacy. Nevertheless, the film spread a contagious nightmare of defenseless personal property online.

This moment inaugurated Facebook’s grandiose pivot to privacy, when Mark Zuckerberg happily announced at F8 conference that year, that “the future is private,” touting new Facebook resources like “Control Who Can Find You,” “Abuse Resources” and other frightening titles that serve to raise fears of dangerous invaders that only Meta can stop through securitization and corporate biometrics. Even though at the same time research shows that increased corporate securitization does not work (Wolff, 2019), surveys found that these privacy settings made people feel secure (Torres & O’Brien, 2012) in a deliberately provoked atmosphere of danger.

It is no coincidence that these securitization measures further marginalize vulnerable communities. For example two-factor authentication that requires two fully charged, updated, working devices with fully paid off monthly bills; or byzantine platforms whose complicated permissions exclude users due to language or neurological barriers. As these security measures are expanded throughout privatized platforms in health services, rental agencies, welfare, social media platforms and more, they claim to efficiently reduce organization workload by in fact locking out significant numbers of vulnerable stakeholders, as Shoshana Magnet has shown.

3.Online “privacy” is a myth.

Online privacy is neither possible nor desirable. In her book *Updating to Remain the Same* Wendy Chun points out that the nature of the internet is computers that are “engaged in constant, incessant, and promiscuous exchanges of information” (2016, p. 107). Meta's security claims are fruitless defenses against the promiscuous circulation of marketing, cyberbullying, violence, and as Maggie McDonald shows, CSAM or Child and Sexual Abuse material that happens inside closed networks of so-called “friends.”

Social media is not really social, it is a decision support system for flagging market trends. Activist academics like Zeynep Tufecki (2018) repeatedly show how misinformation is spread between like-minded networks. Social media privacy measures will never interfere with marketing, and hate is abundantly marketable.

4.“Privacy” is a historic device for designating morally upright sex and policing and punishing its deviations.

Privacy is a colonial legacy that produces, polices and enforces the limits of heteronormative decency. Today, contemporary U.S. notions of broader cis-heterosexual “privacy” entitlements expose transgender communities to danger: required to frequent bathrooms in accord with their sex assigned at birth and subject to mandatory disclosure in order to access healthcare services and obtain government services including government-issued identification (Ringrose, 2020).

Privacy is not social justice, neither for consumer protection, which is disingenuous, nor for marginalized communities, whose problems are systemic. When we call for privacy, we reinforce the logics of liberal property entitlements, gatekeeping and policing. As Walcott argues, oppression and violence are rationalized through, quote, “the faith and enduring belief that something wrong might happen to us” (Walcott 2020, p. 37).

References

Brandom, R. (2017). Two-factor authentication is a mess. *The Verge*, July 10. https://www.theverge.com/2017/7/10/15946642/two-factor-authentication-online-security-mess

Benjamin, R. (2019). *Race after technology: Abolitionist tools for the new jim code.* Social Forces.

Cruz, T. M. (2022). The social life of biomedical data: Capturing, obscuring, and envisioning care in the digital safety-net. *Social Science & Medicine,* 294, 114670.

Clough, P. (2009). The new empiricism: Affect and sociological method. *European journal of social theory,* 12(1), 43-61.

Daniels, J. (2009). *Cyber racism: White supremacy online and the new attack on civil rights.* Rowman & Littlefield Publishers.

Dreyfuss E. (2019). Netflix's The Great Hack Brings Our Data Nightmare to Life. *Wired Magazine*. Retrieved from: https://www.wired.com/story/the-great-hack-documentary/

Fischer, W. (2019). We talked to the professor who fought Cambridge Analytica to get his data back in Netflix's 'The Great Hack' about why privacy rights in the US are lagging behind the rest of the world. *Business Insider*. Retrieved from: https://www.businessinsider.com/netflix-great-hack-david-carroll-interview-data-rights-cambridge-analytica-2019-8

Lapowsky, I. (2019). One Man's Obsessive Fight to Reclaim His Cambridge Analytica Data. *Wired Magazine*. Retrieved from: https://www.wired.com/story/one-mans-obsessive-fight-to-reclaim-his-cambridge-analytica-data/

Massumi, B. (2015). *Ontopower: War, powers, and the state of perception.* Duke University Press.

McMillan Cottom, T. (2020). Where platform capitalism and racial capitalism meet: The sociology of race and racism in the digital society. *Sociology of Race and Ethnicity,* 6(4), 441-449.

Molnar, P. and Lex Gill. "Bots at the Gate: A Human Rights Analysis of Automated Decision-Making in Canada's Immigration and Refugee System," Citizen Lab and International Human Rights Program (Faculty of Law, University of Toronto) Research Report No. 114, University of Toronto, September 2018.

Noble, S. U. (2018). *Algorithms of oppression*. New York University Press.

Robinson, C. (2023). Black marxism. In Social Theory Re-Wired (pp. 156-164). Routledge.

Torres, A. M., & O'Brien, D. (2012). Social networking and online privacy: Facebook users' perceptions. *Irish Journal of Management.*

The Great Hack (documentary film). Produced and directed by Karim Amer and Jehane Noujaim. Netflix, 2019. 1 hour 54 minutes

"United States Senate Committee on the Judiciary". www.judiciary.senate.gov. Archived from the original on June 8, 2020. Retrieved Feb 6, 2023.

Walcott, R. (2021). *On Property*. Biblioasis: Windsor.

Wolff, J. (2019). Two-Factor Authentication Might Not Keep You Safe. *The New York Times,* January 27. https://www.nytimes.com/2019/01/27/opinion/2fa-cyberattacks-security.html