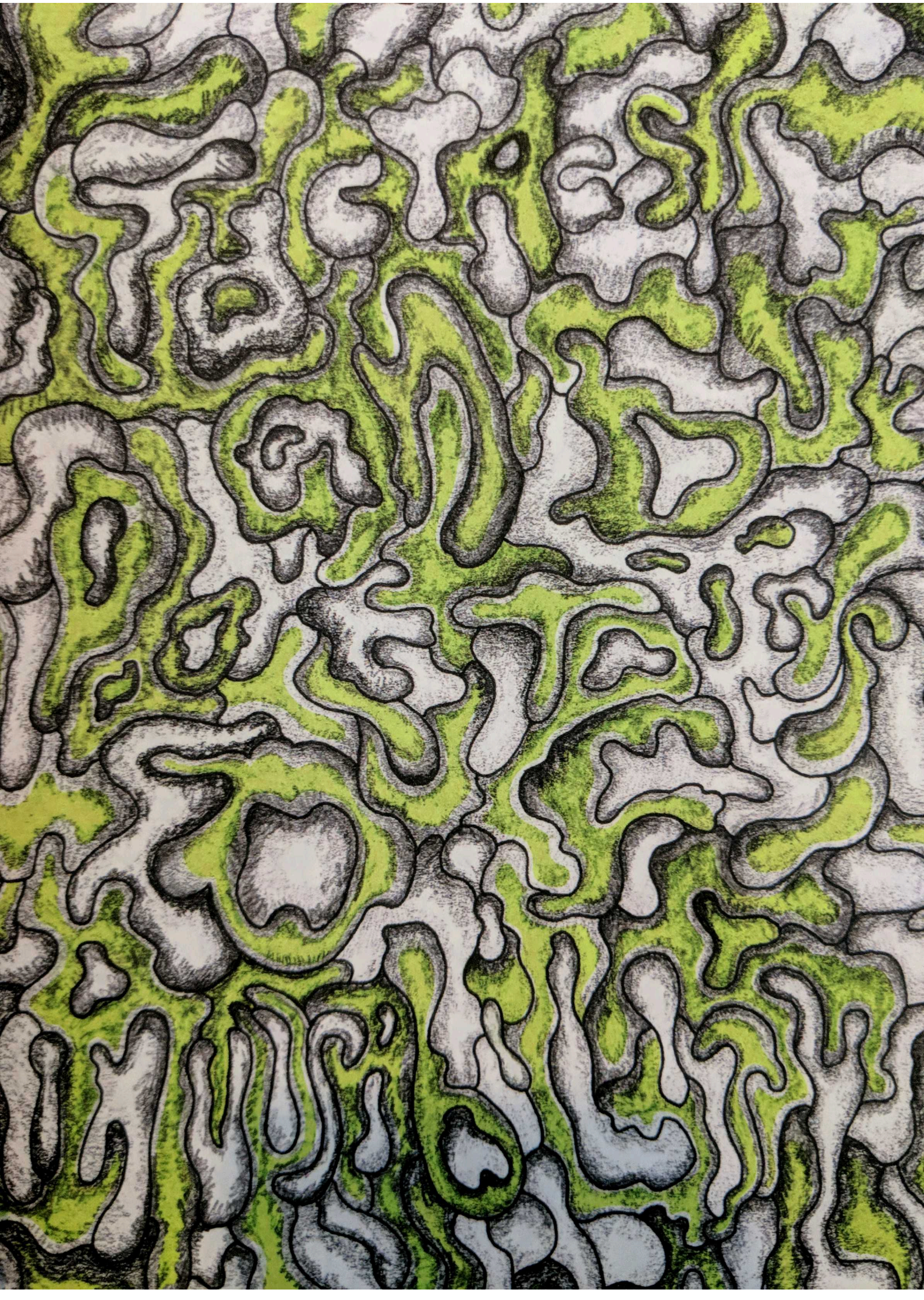
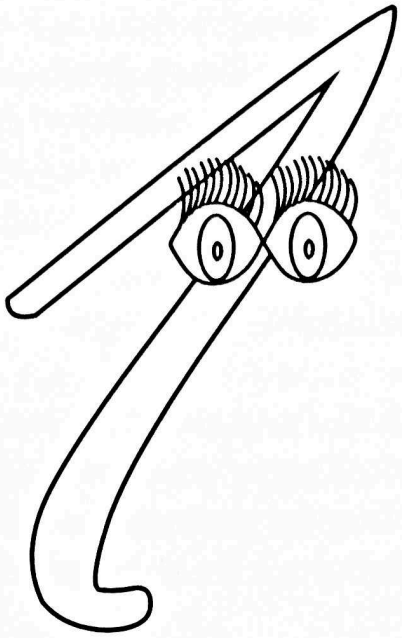
A Lookbook of Invisible Writing

Amy Suo Wu





If late twentieth-century preoccupations with power were atomic and ballistic, those of the twenty-first century are increasingly informatic.[1] Mark Andrejevic

White Spots is a mobile phone app that was featured in the 2016 Dutch TV documentary titled *Offline als Luxe*.[2] The app visually represents online connectivity around the world. Black spots indicate places with digital access, and white spots indicate the offline world, including places that are yet to be connected. The title of the documentary, which translates to 'Offline is the New Luxury', suggests that as offline spaces increasingly come into demand, they will be accessible only to those who can afford the new luxury. If one examines their map, one might conclude that the entire world will soon be blanketed in blackness. Tech giants such as Google, Facebook and Amazon will continue their digital colonisation of the globe, enmeshing it in technologies that soak up information and report it back to their data centres for as long as they can keep them running. In the face of this unprecedented industrial-scale mining of our behavioural and personal data, off-the-grid communication becomes an important alternative for facilitating political autonomy, individual will, collective organisation and creative expression. It was 1968 when Andy Warhol was quoted as saying that in the future everyone would be famous for fifteen minutes. In 2006, Banksy updated the statement in an installation piece bearing the sentence, 'In the future, everyone will be anonymous for 15 minutes'.[3]

1. Mark Andrejevic, 'Foreword', *Feminist Surveillance Studies*, eds. Rachel E Dubrofsky and Shoshana Amielle Magnet (Durham: Duke University Press, 2015) p. x.

2. 'Offline als luxe: VPRO Tegenlicht', *VPRO*, 8 May 2016, accessed 19 March 2018, https://www.vpro.nl/programmas/tegenlicht/kijk/afleveringen/2015-2016/offline-als-luxe.html.

3. Banksy, *Barely Legal* (exhibition), Los Angeles, 2006.

Online information is by its very nature vulnerable: the personal data of civilians is collected, mined and analysed in order to map online behaviour and subsequently develop measures and methods of targeted marketing, governing and policing. Media critics Howard Rheingold and Eric Kluitenberg have argued that the internet, which once promised freedom and democracy, is in fact built on technologies that enable authoritarian control and fascism.[4] Previously applied for military and political advantage in times of war (including the Cold War), surveillance technologies are now being used in times of peace.

In March 2018, *The New York Times* and *The Observer* reported that the British political consultancy firm Cambridge Analytica had been harvesting and analysing the personal data of millions of Facebook users in order to influence the outcome of elections, notably the 2016 US presidential election and the UK Brexit referendum in the same year.[5] Established in 2013, the now-defunct Cambridge Analytica deployed a wide variety of seemingly harmless and playful quizzes, which had been designed to extract data from Facebook users and their circles of friends. The data was then analysed to target people's profiles with personalised political advertisements intended to influence opinion.[6] According to Christopher Wylie, whistleblower and former employee of Cambridge Analytica, the company served as 'a full-service propaganda machine'.[7] Wylie's comment points to how the company operated as an unethical tool in psychological and cultural warfare.

Using the analogy of the horizontal root system of certain plants, the French philosophers Gilles Deleuze and Félix Guattari have applied the term *rhizomatic* to describe a network of non-hierarchical nodes. They place this against the arborescent model, a hierarchical, vertical root system of a tree used to describe a centralised system.[8] The media scholar and artist Henry Warwick, author of *Radical Tactics of the Offline Library*, has expanded this concept. Warwick claims that the once decentralised, rhizomatic structure of the internet has become increasingly centralised or arborescent. The internet landscape has transformed into a top-down system led by economic and juridical powers acting in the interests of capital and propertarianism – driven by the desire to possess, own or hold exclusive rights to it.[9] Evgeny Morozov expressed a similar perspective in his 2011 book on internet freedom, *The Net Delusion*. Morozov points out how contrary to the populist cyber-utopian belief that technology will empower the oppressed, dictators have instead learned to wield technology for

4. Howard Rheingold and Eric Kluitenberg, 'Mindful Disconnection', *Open: Cahier on Art & the Public Domain*, 1 November 2006, accessed 1 March 2018, https://www.onlineopen.org/mindful-disconnection.

5. Emma Graham-Harrison and Carole Cadwalladr, 'Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach', *The Guardian*, accessed 17 March 2018, http://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election; Alex Hern, 'Number of Facebook Users Whose Data Was Compromised "Far More than 87m", MPs Told', *The Guardian*, accessed 17 April 2018, http://www.theguardian.com/uk-news/2018/apr/17/facebook-users-data-compromised-far-more-than-87m-mps-told-cambridge-analytica.

6. 'Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach'.

7. 'What is Cambridge Analytica? The firm at the centre of Facebook's data breach', *The Guardian*, accessed 23 November 2018, https://www.theguardian.com/news/2018/mar/18/what-is-cambridge-analytica-firm-at-centre-of-facebook-data-breach.

8. Gilles Deleuze and Felix Guattari, *A Thousand Plateaus: Capitalism and Schizophrenia* (Minneapolis: University of Minnesota, 1987) p. 7.

9. Henry Warwick, *Radical Tactics of the Offline Library* (Amsterdam: Institute of Network Cultures, 2014).

propaganda purposes – instrumentalising it for sophisticated systems of surveillance and censorship.[10] Like their cyber-utopian comrades, the cyber-feminists of the 1990s saw the internet as inherently revolutionary, with the capacity to sabotage existing power structures and central control, which they regarded as inherently male.[11]

In the early years of the internet, there was in fact a great deal of optimism about this decentralised, non-linear technology. It was seen as a platform that might provide women and other marginalised groups with the means to radically counter gender inequality and become empowered through self-organisation. However, over the course of two decades, old modes of power relations and hierarchies have been reinstalled as a consequence of the commercialisation of the internet.

Surveillance as discrimination

Tabita Rezaire once said, 'The Internet is exploitative, exclusionary, classist, patriarchal, racist, homophobic, transphobic, fatphobic, coercive and manipulative.'[12] The words of the Danish–French Guyanese video artist are hardly surprising, considering the fact that the internet was built upon existing structures that already exhibited such characteristics. To understand the notion of surveillance as discrimination, the feminist scholars Rachel E Dubrofsky and Shoshana Amielle Magnet expanded on the 'white supremacist capitalist heteropatriarchy' proposed by the American author and activist bell hooks, and instead suggest the term 'white supremacist capitalist heteropatriarchal surveillance'. This term captures 'the use of surveillance practices and technologies' and how they 'normalize and maintain whiteness, able-bodiedness, capitalism, and heterosexuality, [which are] practices integral to the foundation of the modern state'.[13]

Surveillance can be seen as the coupling of information collection and the use of power. In *Surveillance as Social Sorting*, David Lyon writes that 'surveillance is not itself sinister any more than discrimination is itself damaging. However, [he states] that there are dangers inherent in surveillance systems whose crucial coding mechanisms involve categories derived from stereotypical or prejudicial sources.'[14] He argues that digital surveillance is not only a matter of personal privacy but of social justice. Discrimination happens when people are sorted into groups, with their worth or risk assigned in ways that have real-life consequences on the opportunities one receives. Can the act of record-keeping ever be neu-

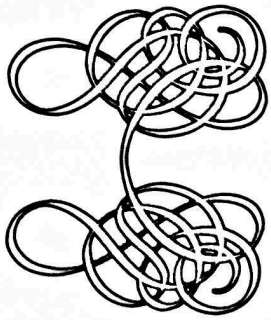
10. Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (New York: PublicAffairs, 2012) p. xiv; Laurier Rochon, 'The Dictator's Practical Internet Guide to Power Retention', accessed 1 March 2018, http://assets.pwd.io/pwd/media/The_Dictator_s_Practical_Internet_Guide_Laurier_Rochon.pdf.

11. 'VNS Matrix / Cyberfeminist Manifesto', *Sterneck.net*, accessed 1 March 2018, http://www.sterneck.net/cyber/vns-matrix/index.php.

12. '"We've Become Cyber Slaves!": "Web Warrior" Tabita Rezaire Wants The Internet To Be Safe Of E-Colonialism', *OkayAfrica*, accessed 4 January 2016, http://www.okayafrica.com/tabita-rezaire-cyber-warrior-e-colonialism/.

13. Rachel E Dubrofsky and Shoshana Amielle Magnet, 'Introduction', *Feminist Surveillance Studies*, eds. Dubrofsky and Magnet (Durham: Duke University Press, 2015) p. 7.

14. David Lyon, *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, (London: Routledge, 2003) p. 2.



tral? What is the imperative behind data collection, whose interests are served by the data, and what are the consequences?

In *Discipline and Punish*, the French philosopher Michel Foucault described surveillance as an instrument of control for disciplinarian measures derived from a traditional focus on Western criminology.[15] But the problem of *digital* surveillance transcends this. It also concerns the alleged neutrality of the algorithm that obscures the forms of gendered, raced and classed surveillance practices that are perpetuated in the name of general interest and national security.[16]

The US-led 'war on terrorism' has paved the way for surveillance practices and pre-emptive security measures that disproportionately target people with a Middle Eastern name or appearance. In 2016, a man living in the Dutch city Roosendaal and identified only as 'Samir O' was wrongfully arrested on suspicion of being a terrorist and for possessing explosives, which turned out to be shawarma spices.[17] In 2015, a fourteen-year-old student by the name of Ahmed Mohamed made a clock for a high school assignment in the US city of Irving, Texas. His teachers mistook it for a bomb, and he was removed from school in handcuffs.[18] That same year, *Al Jazeera*'s Islamabad bureau chief, Ahmad Zaidan, was misidentified by the NSA as a member of al-Qaeda and the Muslim Brotherhood, because his meta-data 'matched' their travelling patterns. This misidentification put his life in 'clear and immediate danger'; many before him have lost their lives due to the release of such fake information.[19] With the emergence of technologies such as predictive policing algorithms that extend nation states' surveillance capabilities, it is no surprise that our prejudices, biases and preconceptions migrate into these algorithms. Mark Andrejevic has described this migration as an 'autonomatization of our preconceptions and prejudices'.[20] Here we see how technology mirrors and advances a system in which power is already asymmetrical.

Since the 2013 Snowden leaks, national intelligence agencies' data collection practices and the right to privacy of citizens have become topics of international debate.

In the US, journalists Glenn Greenwald and Murtaza Hussain revealed in 2014 that a number of the NSA's targets of surveillance had been prominent Muslim Americans, and not one of these Americans had been charged with any crime.[21] This news garnered less media attention than the NSA's unauthorised snooping of US citizens and foreign nationals' telecommunication. Arun Kundnani and Deepa Kumar highlight the double standards in their online article 'Race, Surveillance, and Empire'. While many people take issue with NSA's secret mining of private data on 'ordinary' citizens, this is not extended to Muslim

15. Michel Foucault, *Discipline and Punish*, trans. Alan Sheridan (New York: Vintage Books, 1995).

16. Andrejevic, 'Foreword', p. xii.

17. Hans de Zwart, 'Draconian Anti-Terrorism Measures Turn Us into Scared and Isolated People', *Bits of Freedom*, accessed 1 March 2018, https://www.bof.nl/2017/07/31/draconian-anti-terrorism-measures-turn-us-into-scared-and-isolated-people/.

18. 'Ahmed Mohamed: "Clock Boy" Seeks $15m Redress', *BBC News*, accessed 1 March 2018, http://www.bbc.com/news/world-us-canada-34904226.

19. Ahmad Zaidan, 'Al Jazeera's A. Zaidan: I am a Journalist not Terrorist', *Al Jazeera*, accessed 1 March 2018, https://www.aljazeera.com/indepth/opinion/2015/05/al-jazeera-zaidan-journalist-terrorist-150515162609293.html.

20. Andrejevic, 'Foreword', p. xv.

21. Glenn Greenwald and Murtaza Hussain, 'Meet the Muslim-American leaders the FBI and NSA have been spying on', *The Intercept*, accessed 23 November 2018, https://theintercept.com/2014/07/09/under-surveillance/.

citizens who are seen to be reasonable targets of suspicion.[22] All this begs the question, who fits into the category of an 'ordinary' person and who gets to decide? What is coming to the surface through all of this is that some bodies are deemed worthy of protection while other bodies are not. Racist ideas are the bedrock of the national security surveillance in the US, as they're deeply intertwined with colonialism and empire. Recalling Dubrofsky and Magnet, this example illustrates 'white supremacist capitalist heteropatriarchal surveillance'. Taking a feminist perspective, my feeling is that general discussions about the right to privacy often neglect the general lack of a right to privacy as well as the infringements upon this right for marginalised groups. Law professor Khiara M Bridges' argues in her book *The Poverty of Privacy Rights* that poor women in America do not have the privilege of privacy rights that others enjoy. They are subject to routine intrusions of their private spaces where they raise their children and have no say in the government's collection of their private information about reproductive and sexual choices.[23] The issue at hand in this text is how the poor are being policed and monitored. Rather than applying its resources toward addressing structural deficiencies, the US state has been instead seen to coerce poor women out of motherhood – where even the values that women impart to their children are being monitored.[24] Such surveillance measures are based on an understanding of poverty as an individual failure of the person, rather than as a structural failure of the system. In their book *Feminist Surveillance Studies*, the editors Dubrofsky and Magnet raise the following questions:

> *Who is considered to have a right to privacy? Whose privacy is not a concern and why? And importantly, how might a focus on these questions shape the field of surveillance studies? For instance, many communities – including prisoners, those receiving certain forms of welfare from the state, people with disabilities living in institutional care, as well as immigrants and refugees – have historically had, and continue to have, their bodily privacy invaded, but there is almost no public discussion about the infringement of their rights to privacy.* [25]

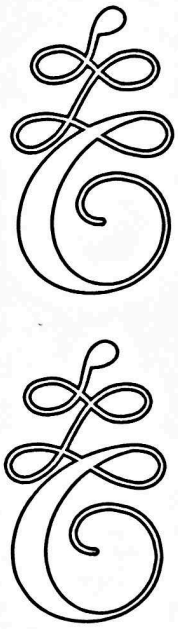
Following this line of thought, Dubrofsky and Magnet reflect upon Rachel Hall's contribution to the book, in which she suggests that the feminist intervention to surveillance is to move critical surveillance studies away from subjects concerned with privacy and security and instead address the ethical problems arising in light of new forms of discrimination-related privilege, access and risk. In other words, what happens to those who have

22. Arun Kundnani and Deepa Kumar, 'Race Surveillance and Empire', *International Socialist Review*, accessed 23 November 2018, https://isreview.org/issue/96/race-surveillance-and-empire.

23. Khiara M Bridges, cited in Tanvi Misra, 'Privacy Is Reserved for Women of Means', *CityLab*, accessed 19 April 2018, https://www.citylab.com/equity/2017/07/do-poor-women-have-privacy-rights/534423/.

24. Ibid.

25. Dubrofsky and Magnet, 'Introduction', p. 4.



no access to privacy rights and what are they at risk of?

The project *Facial Weaponization Suite* (2011–14) by the artist Zach Blas exemplifies how discourse around surveillance technologies collides with the social inequalities they propagate. In the project, Blas develops four masks in order to problematise biometric facial recognition technology. Biometrics is the measurement of unique body characteristics. Perhaps the most iconic piece to have come out of the project is *Fag Face Mask*, a work that responds to the linking of sexual orientation to facial features. Another mask explores the inability of biometric technologies to correctly perceive dark skin. A third mask engages with face-veil legislation in France, considering how the state's demand for facial visibility operates as an oppressive force, while the fourth mask considers the relationship between nationalist violence and biometrics in the context of security technology at the Mexico–US border. Each mask makes visible how digital surveillance technologies perpetuate discrimination in different ways. At the same time, they conceal the human face from these very technologies to subvert and resist categorisation and profiling.

26. Michel Foucault, *Discipline and Punish*, trans. Alan Sheridan (New York: Vintage Books, 1995) p. 201.

27. Martha Kaplan, 'Panoptican in Poona: An Essay on Foucault and Colonialism', *Cultural Anthropology*, vol. 10, no. 1 (February 1995) p. 85 - 98.

A brief history of surveillance technology

Developed in the late eighteenth century by the English philosopher Jeremy Bentham, the panopticon is an architectural system for a prison in which the inmates' cells are arranged in a circular fashion around a central watchtower. The layout allows for observation, by a single watchman, without any particular inmate knowing whether they are being watched or not, thus inducing what Foucault referred to as a 'state of conscious and permanent visibility that assures the automatic functioning of power'.[26] At the time, the panopticon was a technical innovation in the field of surveillance that reduced labour expenses while increasing the productivity of control through means of self-policing and preventive measures. Foucault used the panopticon as a metaphor for a critical analysis of institutions of power in the West. In fact, as noted by the anthropologist Martha Kaplan, early panoptical prisons with Bentham's design were not built in Britain, but in the beginning of nineteenth-century India under British colonial rule.[27] What this goes to show is how surveillance was inseparable and essential to colonisation. In *Post-Colonial Studies*, the three authors write the following:

> *One of the most powerful strategies of imperial dominance is that of surveillance, or observation, because it implies a viewer with an elevated vantage point, it suggests the power to process and understand that which is seen, and it*

objectifies and interpellates the colonized subject in a way that fixes its identity in relation to the surveyor. [28]

European nations used their colonies as laboratories to test surveillance technologies for home use, according to the sociologist Elia Zureik in his 2013 essay on domestic spying and imperial histories:

It is significant that the basic tools of surveillance as we know them today (i.e., fingerprinting, census taking, mapmaking and profiling), which include the forerunners of present day biometrics, were refined and implemented in colonial settings, notably by the Dutch in Southeast Asia, the French in Africa, and the British in India and North America. [29]

Feminist activist and academic Andrea Smith has argued that the colonial gaze is based on a logic of *not-seeing*.[30] It was precisely this not-seeing that allowed for colonial takeover in the first place – as exemplified by the British declaration that Australia was *terra nullius* ('nobody's land') at the time of settlement.[31] As is becoming clearer, the European colonial project traces directly to white supremacism. Indigenous societies and other non-Europeans such as immigrants and the enslaved only became visible to the colonising state when they were regarded as threats to the project of colonial domination and state security.[32] Thus, as Zureik argues, 'colonialism and imperialism provided the impetus for developing modern surveillance technologies'.[33]

Many scholars of surveillance have shown that its origins are inextricably linked with imperial dominance over colonised 'others', and this link continues to shape modern surveillance practices of radicalised and marginalised populations as well as political dissenters.[34]

Today, passport photographs are a standardised technique for connecting individual identity with the body and its representation. However, in the United States for example, the earliest implementation of the medium of photography for passports was tested on marginalised groups such as immigrants – beginning with Chinese women. According to the gender and women's studies scholar Eithne Luibhéid in her book *Entry Denied*, the sexuality of immigrant women was seen as a danger to the nation's security, a threat that elicited containment through strict border control.[35]

28. Bill Ashcroft, Gareth Griffiths and Helen Tiffin, *Post-Colonial Studies: The Key Concepts* (London: Routledge, 2007) p. 207.

29. Elia Zureik, 'Colonial Oversight', *Red Pepper*, accessed 1 March 2018, https://www.redpepper.org.uk/colonial-oversight/.

30. Andrea Smith, 'Not-Seeing: State Surveillance, Settler Colonialism, and Gender Violence', *Feminist Surveillance Studies*, eds. Dubrofsky and Magnet (Durham: Duke University Press, 2015) p. 26.

31. Smith, 'Not-Seeing: State Surveillance, Settler Colonialism, and Gender Violence', p. 26.

32. Ibid., p. 27.

33. 'Colonial Oversight'.

34. Simone Browne, *Dark Matters: On the Surveillance of Blackness* (Durham: Duke University Press, 2015); Dubrofsky and Magnet, eds., *Feminist Surveillance Studies*; Arun Kundnani and Deepa Kumar, 'Race, Surveillance, and Empire', *International Socialist Review*, accessed 1 March 2018, /issue/96/race-surveillance-and-empire; Christian Parenti, *The Soft Cage: Surveillance in America from Slavery to the War on Terror* (New York: Basic Books, 2004); Elia Zureik, 'Colonial Oversight', *Red Pepper*, accessed 1 March 2018, https://www.redpepper.org.uk/colonial-oversight/.

35. Eithne Luibhéid, *Entry Denied: Controlling Sexuality at the Border* (Minneapolis: University of Minnesota Press, 2015).

The Page Act of 1875 and the Chinese Exclusion Act of 1882 were some of the earliest examples of laws limiting the entry of immigrants to the US from Asia.[36] Photography, with its ability to record the uniqueness of individual bodies, proved to be a technology that could control an individual's mobility. Eithne Luibhéid again:

> *A photograph was attached to each woman's consular clearance, and another photograph was sent in advance of the ship, so that when the ship arrived, officials already had in their possession photographs of the women who had been approved for migration. Women who arrived without photographs, or who did not match the photographs that had been sent in advance, were detained and returned to Hong Kong.*[37]

These laws helped mould a system of border controls in the United States. They created categories of illegal immigration and 'aliens ineligible for citizenship', which in turn were used to deny voting rights and property ownership.[38] They also established principles of race-based immigration that the US Congress enforced through subsequent laws, such as the Trump administration's 2018 efforts to ban immigration from Muslim-majority countries.

In her book *Dark Matters: On the Surveillance of Blackness*, Simone Browne introduces the term 'racializing surveillance' as a way to frame surveillance as a technology of social control that produces norms related to race that define what is in or out of place.[39] Browne points out that these practices stem from plantation societies, repressive societies and anti-Black spaces. For instance, one of the earliest identification and surveillance systems in the United States was the 'slave pass'. Designed to monitor slaves and prevent them from escaping to freedom, the slave pass can be seen as an early example in the development of modern-day identification systems such as biometrics.

In *The Soft Cage*, the journalist Christian Parenti highlights how, although the intention of pass laws was to control the mobility of poor whites and Native Americans in the seventeenth century, the first pass law enacted in Virginia in 1680 exclusively targeted African slaves.[40] In 1687, it became illegal in South Carolina for slaves to travel without a note from their master.[41] These notes or passes, which are early examples of identification, were written by plantation owners giving permission to slaves to travel beyond the plantation to which they belonged. Parenti describes the loopholes of the early passes: since they only recorded the times at which they could travel and not their physical characteristics, slaves who learned how to read and write could forge passes and manoeuvre around systems of control in order to gain freedom. In a time when black illiteracy was the rule, enforced as a measure of control, literate slaves were able to tactically evade the pass

36. 'The Page Act of 1875', *Wikipedia*, accessed 1 June 2017, https://en.wikipedia.org/wiki/Page_Act_of_1875; 'The Chinese Exclusion Act', *Wikipedia*, accessed 1 June 2017, https://en.wikipedia.org/wiki/Chinese_Exclusion_Act.

37. Luibhéid, *Entry Denied*, p. 45.

38. 'Alien land laws', *Densho Encyclopedia*, accessed 19 July 2017, http://encyclopedia.densho.org/Alien_land_laws/.

39. Simone Browne, *Dark Matters: On the Surveillance of Blackness* (Durham: Duke University Press, 2015) p.16.

40. Christian Parenti, *The Soft Cage, Surveillance in America, From Slavery to the War on Terror* (New York: Basic Books, 2003) ebook, p. 20.

41. Ibid.

system and escape while also enabling the liberation of others – notably the social reformer and former slave, Frederick Douglass.[42]

As slaves found ways to resist and counter surveillance-mechanisms instated to curb any possibility of their freedom of movement, colonial overseers further developed surveillance strategies to gain back control. For example, paper passes were eventually replaced by metal tags that were more resistant to tampering and forgery.[43] Colonial overseers also improved identification and biometrics through the use of the wanted poster, describing specific body measurements and other physical indicators. For example:

> *Negro man Slave named Bob,*
> *Copper color, high cheek bones, 5 11 inches high, weighs about 150 pounds, 22 years old very white teeth and a space between the center of the upper teeth. Had a blue blanket sack coat with red striped linsey lining.*[44]

To quote Kundnani and Kumar again:

> *This is as true today as it has been historically: race and state surveillance are intertwined in the history of US capitalism. Likewise, we argue that the history of national security surveillance in the United States is inseparable from the history of US colonialism and empire.*[45]

Returning to the present day, the sociologist David Lyon points out how surveillance in the West has gradually evolved from the top-down panoptic model to a model that envelops us as we actively engage and participate in it on a daily basis. Together with Zygmunt Bauman, in 2012 Lyon coined the term 'liquid surveillance' to describe how surveillance flows within and between organisations, fluidly encompassing our technologies, the means of social control and our culture at large.[46] By extension, liquid surveillance means that we watch our friends, colleagues and family on social media. We give away personal data to commercial companies such as Facebook, Twitter and YouTube, which then flows through data brokers that might end up being used for government or policing purposes.

Against the backdrop of advances in digital technology, the cat-and-mouse game of surveillance and counter-surveillance has become increasingly blurred and complicated. This relatively new concept of liquid surveillance means that traditional power relationships between

42. Ibid., p. 22.

43. bid., p. 24.

44. 'Broadside Offering Reward of $2,500 for Return of Three Runaway Negroes, August 23, 1852', *Missouri History Museum*, accessed 13 November 2017, http://collections.mohistory.org/resource/216610.

45. Kundnani and Kumar, 'Race, Surveillance, and Empire'.

46. Zygmunt Bauman and David Lyon, *Liquid Surveillance: A Conversation* (Cambridge: Polity, 2012).

watcher and watched, oppressor and oppressed are collapsing and need to be reassessed.

47. Michel de Certeau, *The Practice of Everyday Life*, trans. Steven F. Rendall (Berkeley: University of California Press, 2011).

48. Geert Lovink and David Garcia, 'The ABC of Tactical Media', *Nettime*, accessed 1 March 2017, http://www.nettime.org/Lists-Archives/nettime-l-9705/msg00096.html.

Sousveillance: invisibility as a tactic

Given what we know about liquid surveillance, is it still possible to subvert and deflect surveillance in a world that is totally submerged in it?

The term *sousveillance*, coined by the media researcher Steve Mann, is based on the idea of watching those who are watching us. Similar to the word surveillance, which means 'watching from above' in French, sousveillance means 'watching from below', implying an effort by citizens to disrupt asymmetries of power. The split between surveillance and sousveillance echoes the dichotomy of the watchers and the watched, the strong and the weak, the powerful and the powerless.

The cultural theorist Michel de Certeau described a theoretical framework for understanding how the 'powerless' may appropriate, subvert and reclaim meaning from the 'powerful'.[47] In de Certeau's original formulation, written in 1980, *strategies* are seen as the weapons of the strong, accessible only to those who are in a position to define the environment and the conditions of the playing field – such as governments, corporations, the media, schools and the church. In contrast, *tactics* are the weapons of the weak. De Certeau identifies tactics with the creative consumer and rebellious participants, or rebellious 'users', who are able to take advantage of the strong. De Certeau's terminology provided the theoretical groundwork for the 'tactical media' practice of the 1990s. The people who took up this practice defined its identity against dominant structures and its actions challenged mainstream culture through subversive, grassroots and DIY production and distribution of media. In their seminal media theory essay from 1997, 'The ABC of Tactical Media', Geert Lovink and David Garcia reflect on de Certeau's writing:

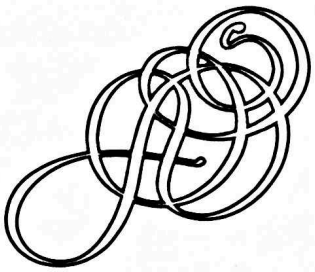
> *Setting up this dichotomy allowed [de Certeau] to produce a vocabulary of tactics rich and complex enough to amount to a distinctive and recognizable aesthetic. An existential aesthetic. An aesthetic of poaching, tricking, reading, speaking, strolling, shopping, desiring. Clever tricks, the hunter's cunning, maneuvers, polymorphic situations, joyful discoveries, poetic as well as warlike.*[48]

For media activists and artists such as the Critical Art Ensemble, the Yes Men, and Eva and Franco Mattes of 0100101110101101.org, de Certeau's framework has been hugely influential.

In the present day media landscape, however, the strategies–tactics dichotomy has become inadequate. De Certeau's text also, of course, is unable to critically address the recent rise of the alt-right, in particular its online activity. As an extreme, neo-fascist group, the alt-right has weaponised internet meme-making and online trolling as a means

for spreading white nationalism, misogyny, homophobia, right-wing populism, racism and hate speech. Many of the methods practiced by tactical media activists have been absorbed by radical right-wing subcultures. For example the use of multiple-use names or anonymity pseudonyms, which are names used by many people so that they can remain anonymous. The names 'Luther Blisset' and 'Wu-ming', for example, were used by cultural activists and media pranksters in the 1990s for projects that wanted to challenge and experiment with forms of collective authorship and identity. A decade later, the Anonymous group, an online community of amorphous hackers, emerged on 4chan, an internet forum whose original function was to simply allow users to post images. 4chan has been the birthplace of many internet memes, and its participants are usually anonymous, owing to the fact that one doesn't need to register in order to post. And thus the Anonymous group adopted its name based upon this feature of anonymity.

4chan has been central to the rise of the alt-right. What was once a space for generally left-wing, anarchic rhetoric gradually shifted into one of militant, fascist, right-wing rhetoric. The uncomfortable uncertainty is whether or not the shift was a gradual evolution or a conscious takeover. In other words, are they the same people or different people? In part due to user anonymity and lack of accountability, the site provided a breeding ground for would-be trolls potentially harbouring neo-Nazi ideologies.



The reality is that the alt-right subculture and movement also operates under the libertarian premises of less surveillance, more privacy and freedom of expression. How do we reconcile the desire for freedom of expression with the neo-Nazi desire for freedom of expression to spread hate and advocate for white supremacy? Returning to de Certeau's notion of tactics as the weapons of the weak and strategies as the weapons of the strong, perhaps this binary has in fact depoliticised the issues at hand. Considering this possibility, I have taken to using the term 'tactical invisibility' to support and highlight the subversive practices of marginalised gender, ethnic and sexual cultures.[49]

To understand surveillance from an Afro-American perspective, Simone Browne introduced the concept of 'dark sousveillance' to describe 'tactics used to render one's self out of sight'.[50] Building upon Steve Mann's idea of sousveillance as watching those who are watching us, Browne's 'dark' modifier comes from a place of critique but does so while also acknowledging the usefulness of the original term.[51] Dark sousveillance is used to look at the ways that people living in anti-Black spaces might 'challenge repressive practices through their own experiences of counter-veillance and surveillance'.[52] Such experiences in turn produce a

49. This term was my own coinage. During my research for this book, I found that the term has precedents in the following publications: Karin L. Tamerius, 'Sex, Gender, and Leadership in the Representation of Women', in Mona Krook and Sarah Childs, *Women, Gender, and Politics: A Reader* (Oxford: Oxford University Press, 2010) p. 250.

50. Claudia Garcia-Rojas, 'The Surveillance of Blackness: From the Trans-Atlantic Slave Trade to Contemporary Surveillance Technologies', *Truthout*, accessed 14 March 2018, http://www.truth-out.org/news/item/35086-the-surveillance-of-blackness-from-the-slave-trade-to-the-police.

51. Ibid.

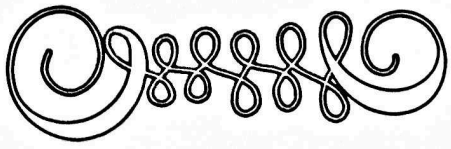
52. Ibid.

body of 'liberatory knowledge' in subversion, resistance and coping mechanisms for survival.[53]

Tactics of Black resistance trace a long way back. From the seventeenth century, African slaves who resisted and escaped slavery from European colonisers formed autonomous communities throughout the Americas. In regions of the US, Suriname and Jamaica, escaped slaves were known as Maroons and formed new settlements in inaccessible and inhospitable environments where they could hide and defend their communities from colonial forces.[54] Surviving beyond the sight and control of the colonial officers meant that they were able to practice and maintain aspects of their ancestral languages, cultures and religions.[55]

The Chinese phenomenon of *shanzhai*, meaning counterfeit consumer goods, may in a sense also be considered an invisibility tactic. The word *shanzhai* translates to 'mountain fortress' or 'mountain village' – referring to outlaws and bandits who lived remotely across China, beyond the reaches of official control. Inhabiting and operating in the blind spots of copyright protection of big multinational brands, *shanzhai* products are usually illegal and made in poor labour conditions. But the designs and the market evolve rapidly, giving life to unauthorised and strange electronic hybrid products such as Swiss Army–knife phones, shaver phones, lighter phones and pen phones. But *shanzhai* encompasses more than just phones. *Shanzhai* aesthetics usually mirror those of Western designs and products, such as fashion brands, European paintings, art exhibitions and entire villages made to look like European towns. Flying under the radar of global corporations, cheap knockoffs circulate the vast space of the 'grey market' – unofficial markets where goods are sold legally, but are unauthorised for sale by the official suppliers. Drawing from this cultural phenomenon, 'Second (Hand) Mountain (Fortress)' is a pirate publishing-project by Display Distribute, an artist-run publishing house based in Hong Kong. Channelling the energy of *shanzhai*, one of Display Distribute's publications is self-reflexively titled *Copycat*, and is an illegally reprinted chapter of *China in 10 Words* by the Chinese writer Yu Hua. The cover of the book depicts an enlarged text snippet from Yu Hua's book that describes the word copycat as having 'more of an anarchist spirit than any other word in the contemporary Chinese language'.[56]

Taking the cultural phenomenon of *shanzhai* as an example, how then to apply this to communication technology? Where are the invisible cracks and mountain fortresses of digital media? According to the media theorist Wendy Chun, digital media not only facilitates leaks by whistleblowers, but also, the technology is itself 'leaky'.[57] In the wake of the Snowden leaks, Chun writes the following:



53. Ibid.

54. 'The Obscured History of Jamaica's Maroon Societies', *Jstor Daily*, accessed 30 November 2018, https://daily.jstor.org/maroon-societies-in-jamaica/; Gloria Wekker, *The Politics of Passion: Women's Sexual Culture in the Afro-Surinamese Diaspora* (New York: Columbia University Press, 2006) p. 58.

55. 'The Obscured History of Jamaica's Maroon Societies'.

56. Yu Hua, 'Copycat', *China in Ten Words*, (Hong Kong: 'Second (Hand) Mountain (Fortress)', 2016).

57. Wendy Hui Kyong Chun and Sarah Friedland, 'Habits of Leaking: Of Sluts and Network Cards', *differences*, vol 26, Issue 2 (2015): p. 1–28.

Leaking information is framed paradoxically as both securing and compromising our privacy, personal and national. Thanks to these leaks, we now understand the extent to which we are under surveillance; because of these leaks, we are exposed. [58]

From a media theory perspective, Chun questions whether leaking information is an issue of personal human agency at all, and instead positions digital media's leakiness as a systematic vulnerability of networked technology. In the open waters of digital technology, communication is vulnerably 'visible' to potential human and non-human spies alike. As such, what constitutes invisible and leak-proof communication?

The option of going offline or off-the-grid is becoming increasingly relevant due to our digital vulnerability and unease generated around that reality. Such sentiments are mirrored by changes in consumer behaviour, such as demand for vintage communications devices. One local German publication reported that following the Snowden revelations, Bandermann and Olympia typewriter manufacturers were experiencing a customer surge.[59]

The relative security of paper is also touched upon in the final scene of *Citizen Four*, a documentary film on Edward Snowden. In this scene, the journalist Glenn Greenwald resorts to paper and pen to communicate with Snowden.

The Chinese artist-run zine collective called Fong Fo harnesses the tactical nature of printed DIY zines. Running out of a home-studio in Guangzhou, Fong Fo prints, binds and distributes its work on paper in a conscious effort to circumvent stringent censorship measures and publish more freely in the government-restricted Chinese media landscape.

In the United States, against the backdrop of online trolling by the alt-right, self-organised spaces are opting to go underground and offline in search of safer forms of communication. In December 2016, the DIY venue Ghost Ship burned down in Oakland, California, sparking a public debate on the safety and legal status of these spaces.[60] Alt-right groups subsequently jumped in on the conversation, calling artist-run DIY spaces 'open hotbeds of liberal radicalism and degeneracy'.[61] The contemporary art blog *Hyperallergic* reported:

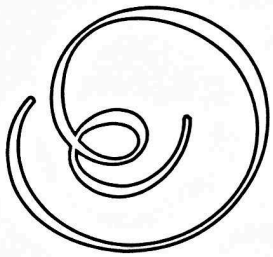
The troll campaign against DIY music venues and live/work artists' spaces [...] emerged from /pol/, a 4Chan message board [...]. The anonymous posters adopted

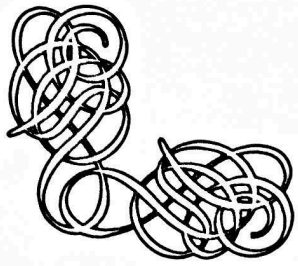
58. Ibid.

59. Felix Reimer, 'Typewriter Manufacturers See Boom in Sales', *The Local*, accessed 21 July 2014, https://www.thelocal.de/20140721/german-typewriter-manufacturers-see-sales-boom.

60. Benjamin Freed, '"Alt-Right" Trolls Are Targeting DC's DIY Music Houses', *Washingtonian*, accessed 28 November 2018, https://www.washingtonian.com/2016/12/19/alt-right-trolls-targeting-dcs-diy-music-houses/.

61. Gabrielle Canon, '4chan Users Launch Campaign to Shut Down DIY Venues in Aftermath of Oakland Fire.' *Vice*, accessed 1 March 2018, https://thump.vice.com/en_ca/article/d7jwdj/4chan-trolls-diy-spaces-oakland-fire.





the name 'Right Wing Safety Squad' – SS for short – and posted memes incorporating Nazi symbolism. They found lists online of DIY spaces across the country and scoured Facebook for venue names, addresses, and, in some cases, images of specific venues, using the information to call in anonymous complaints in an attempt to get spaces shut down over fire code violations and permitting issues.[62]

As a consequence, some underground spaces have gone back to announcing their shows through word-of-mouth rather than online.[63] The same sentiment is echoed by Henry Warwick in *Radical Tactics of the Offline Library* when he proposes to abandon 'the online for more secure offline transfer'.[64]

The fact that invisible ink recipes are now deemed obsolete and harmless makes these recipes steganography on top of steganography. Invisible ink is now overlooked, not only because the ink is invisible, but also because nobody expects this technique to still be used. From a media-archaeological perspective, invisible ink has been relegated to the status of 'dead media'.[65] Another way of looking at it is as 'zombie media', to borrow a term from media studies that explores the temporalities of media objects, planned obsolescence and electronic waste.[66] Analog steganography is a medium that I have attempted to resuscitated and reactivated. As such, it is my claim that invisible ink can be used tactically to oppose a commodity culture that focuses solely on the development of ever-newer media. It can push us backwards to explore forgotten-tech alternatives that have been underestimated, and are perfectly suitable for flying under the radar of detection. Another advantage of forgotten technology such as this is the fact that the modern equivalents have lost the ability to counter it.

This brings to mind a seemingly unrelated story about a thousand-year-old treatment for eye infection that was used to treat the notorious superbug Methicillin-resistant Staphylococcus aureus (MRSA).[67] In 2015, two scientists recreated a ninth-century Anglo-Saxon home remedy using garlic, onion, wine, cow bile and copper. To their surprise, the concoction wiped out ninety per cent of the MRSA bacteria in their sample test that at the time had developed a resistance to modern medicines. Because the bacteria had evolved over time, the scientists' hypothesis was that the bacteria had forgotten how to fight the Anglo-Saxon remedy since it had been so long out of circulation.

This anecdote challenges the narrative that human progress and innovation should always be looking toward the future. The past may also hold valuable answers for healing the present, potentially offsetting the 'arms race' between medicine and germs. In its own way, perhaps invisible ink may subvert the arms race of surveillance technologies.

62. Blair Murphy, 'From Texas to DC, Artists and DIY Spaces Struggle with Permits and Trolls,' *Hyperallergic*, accessed 1 March 2018, https://hyperallergic.com/355219/from-texas-to-dc-artists-and-diy-spaces-struggle-with-permits-and-trolls/.

63. '"Alt-Right" Trolls Are Targeting DC's DIY Music Houses'

64. Warwick, *Radical Tactics of the Offline Library*.

65. Bruce Sterling, 'A Modest Proposal and a Public Appeal', *Dead Media*, accessed 1 March 2018, http://www.deadmedia.org/modest-proposal.html.

66. Garnet Hertz and Jussi Parikka, 'Zombie Media: Circuit Bending Media Archaeology into an Art Method', *Leonardo*, vol. 45, no. 5 (5 July 2012) p. 424–30.

67. 'A Medieval Medical Marvel - Science Blog', *British Library*, accessed 1 March 2018, https://britishlibrary.typepad.co.uk/science/2015/04/a-medieval-medical-marvel.html.

The visibility paradox

The feminist project of making women and gender more visible within and across numerous disciplines and interdisciplinary studies is rendered especially contradictory when articulated in terms of a knowledge field that starts off from the problematization of visibility as a mode of subjection and regulation. Surveillance betrays and degrades the liberatory promise of visibility.[68] Laura Hyun Yi Kang

With temptation, if I can put it this way, we're crushed by twin pincers of nothingness. By not communicating, we're annihilated into the emptiness of an isolated life. By communicating we likewise risk being destroyed.[69] Roberto Esposito

Regimes of surveillance oppress with visibility, stripping naked their subjects and encroaching into societies' most intimate nooks and crannies. 'Glass is the enemy of secrets',wrote the philosopher Walter Benjamin who was himself persecuted by Nazi Germany.[70] To me, this conjures up a place where no one can hide or seek refuge. The term *gläserner Mensch* ('glass human' or 'transparent being') was used by West German privacy activists in the early 1980s during the Cold War and then retroactively applied to East German Ministry for State Security (Stasi) surveillance.[71] The Stasi had unlimited state access to all information on all citizens, including medical records, financial records, insurance policies and bank statements.

On the other hand, visibility can also be seen as generating evidence – for example, a person's visibility can work to legitimise invisible and undervalued work that has historically been ignored. Within a feminist framework, the act of voicing or making visible violence that traditionally happens behind closed doors – the private sphere being the primary site of oppression and violence for women – can be liberating, as demonstrated by the Me Too movement in 2017. Marginalised groups have a long history of fighting for public visibility as a means of then gaining recognition from the state. Their battles, however, are due to their erasure by the same state. An example is the representation of ethnic minorities within the mainstream media, which also concerns visibility as a legitimizing, inclusive and empowering force. What comes to mind are indigenous Australians, and their ongoing fight to overturn the national day of 'celebration', a date that marks the invasion of their

68. Laura Hyun Yi Kang, 'Surveillance and the Work of Antitrafficking', *Feminist Surveillance Studies*, eds. Dubrofsky and Magnet (Durham: Duke University Press, 2015) p. 40.

69. Roberto Esposito, *Communitas: The Origin and Destiny of Community*, trans. Timothy C. Campbell (Stanford: Stanford University Press, 2009) p. 146.

70. Walter Benjamin, 'Erfahrung und Armut', *Textlog*, accessed 1 June 2017, https://www.textlog.de/benjamin-erfahrung-armut.html.

71. 'Gläserner Mensch (Datenschutz)', *Wikipedia*, accessed 7 June 2018, https://de.wikipedia.org/w/index.php?title=Gl%C3%A4serner_Mensch_(Datenschutz)&oldid=178101975.

land. To go back to the East German regime, it's important to note that in the aftermath, citizens occupied Stasi buildings to prevent the destruction of their files, so that the state could be held accountable for injustice.

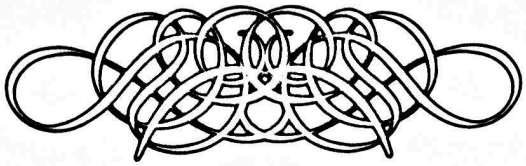
72. Felix Stalder, 'The Fight over Transparency: From a Hierachical to a Horizontal Organization', *Open: Cahier on Art & the Public Domain*, no. 22 (2011) p. 22.

To be visible is to be vulnerable to social control and surveillance. But visibility can facilitate public recognition, as well as cooperation, solidarity and community-building. This also applies to immigrants, prisoners and refugees who live simultaneously as hyper-visible to the monitoring gaze of the state, and yet remain socially invisible. How then do we negotiate the idea of visibility as a disciplinary and discriminatory measure and, at the same time, as a means of empowerment and accountability for those experiencing inequalities and discrimination?

In his essay 'The Fight over Transparency', the Swiss media theorist Felix Stalder describes visibility in today's neoliberal era as synonymous with institutional 'good practice'.[72] Stalder names 'bottom-up visibility' as the instance in which communities and people demand visibility to structures of power for accountability. In this context, transparency can be empowering, such as former East German citizens demanding access to their files. However, 'top-down visibility', in which the state demands visibility, is a disciplinary measure of control that leads to what Stalder calls 'information asymmetry'. The question is how to remain invisible, while still being visible to our peers. Stalder's answer is to suggest particular forms of visibility for social solidarity, in which people can come to see one another, and experience zones of mutuality. Without horizontal transparency, social solidarity cannot take place, as I will show in the next section, which looks at how queer languages protect members of a group from potential aggressors while not rendering them complete invisibility to each other. Perhaps the issue at hand shouldn't be framed as one of visibility versus invisibility, but rather as a matter of our individual autonomy and sovereignty regarding this visibility.

Steganography as social glue

Although the Chinese linguistic phenomenon of Nüshu cannot definitively be labelled as steganography, it is nevertheless an interesting and relevant example that elucidates the potential of secret writing as a means of tactical solidarity. Nüshu (女书), meaning 'woman's writing', is perhaps the only known written script developed and used exclusively by women. Far away from the densely populated cities, Nüshu originated in Jiangyong county in the Hunan province of China, reaching peak usage during the latter part of the Qing Dynasty (1644–1912). The script itself is one that represents the local dialect of Jiangyong, and therefore is a syllabic script, meaning that each symbol represents a syllable. This contrasts with the official Chinese writing system known as *hanzi* (汉字), which uses

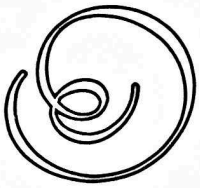


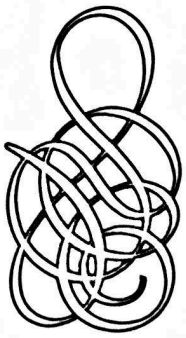
an extensive system of syllabic and logographic characters (with each symbol representing a word or phrase).

In this rural region isolated by mountains, traditional Confucian patriarchal ideals prevailed. As such, women were excluded at various levels of social interaction. Most significantly, their restricted access to formal education meant that women were usually illiterate in *hanzi* writing.

Interestingly, it has been said that Nüshu was forbidden during the Japanese occupation of much of China in the 1930s and 1940s, since the Japanese invaders feared that the Chinese could use it to send secret messages.[73] Although efforts have been made to preserve the script, the last writers who used it in their day-to-day lives died during the 1990s, leaving the legacy to only a very small number of scholars interested in the language. Indeed, much of the information detailed here was imparted to me in a conversation I had with Professor Liming Zhao, head of the Nüshu research project at Tsinghua University in Beijing, back in 2017.[74]

It is quite remarkable that a community of women in Hunan were able to co-author a written language that allowed them to express themselves. What emerged was Nüshu poetry, song lyrics and biographies recorded in embroidery and in booklets usually written with sharpened bamboo dipped in ink – lending the calligraphy a thin and wispy aesthetic quality unlike the traditional brushstrokes of *hanzi*. One of the primary uses of Nüshu was to enable communication between 'sworn sisters' (*jiebai zimei*, 结拜姊妹), who were not biologically related. This sisterhood required them to pledge commitment to each other and included activities such as attending festivals and making textile arts and crafts together. These relationships were often closer than those with one's biological sisters.[75]





In a male-dominated society, Nüshu helped to create a degree of social cohesion in which women could develop autonomous forms of belonging and a sense of community. Women developed an alternative script, not in order to undermine systems of oppression, but rather as a coping mechanism. In fact, Nüshu was never meant to be a secret or to explicitly exclude men. Rather, it was men in the community who were oblivious or indifferent to it. On a certain level Nüshu operated as steganography because, although it was there in plain sight, male onlookers were not aware or not interested. In this context, 'codes' or 'secrets' refer more so to a common understanding within a group and less to a deliberate withholding of information from outsiders. To quote Nüshu researcher Cathy Silber: 'When power is distrib-

73. 'Nüshu', *scriptsource.org*, accessed 3 September 2017, http://scriptsource.org/cms/scripts/page.php?item_id=script_detail&key=Nshu.

74. In typical Chinese fashion, I was invited to join Professor Liming Zhao for dinner afterwards as she had other visitors that day. Strangely enough, it turned out that one of her other dinner guests was the grandson of one of the last 'real' writers of Nüshu. He was in town for business related to his grandmother's use of Nüshu. During dinner, I learned how the culture around the script has become a commercial enterprise where the government and locals leverage it for tourism.

75. Orie Endo, 'Endangered System of Women's Writing from Hunan China', 1999, accessed 3 October 2017, http://nushu.world.coocan.jp/aas99.htm.

uted unequally in a social relation, the impact of exclusion depends on which side is exercising it.' [76]

Steganography relies on both invisibility and visibility, exclusion and inclusion. Like any other language, secret languages are social. Rules, conditions and systems need to be invented and established within a community. Steganography relies on the specificities of each community, and can thus be visual and tactile as well as linguistic. Secret languages manifest in myriad forms: from written scripts such as Nüshu to slang and colloquial language used to define and mark group identity; from argot, or a type of jargon, that is developed under scrutiny by groups who are oppressed or imprisoned, to non-secret yet specific vocabulary applied in specialised settings, such as professional jargon. What all of these in-group, collectively developed codes share is the function of strengthening community bonds, while also excluding outsiders or shielding members from oppression. An excellent example of this is the phenomenon called 'lavender linguistics', a strand of camouflaged vocabularies developed by queer communities to protect themselves from social persecution and judicial punishment: these include Kaliarda in Greece, Polari in England and Hijra Farsi in India.[77] Consider also the development of jargon codes in countries such as Syria and China, where the expression of political opposition can be extremely dangerous. What links Nüshu, Polari, Kaliarda, Hijra Farsi and other camouflaged languages is their shared function of facilitating and reinforcing social ties and relations. In Chapter 4, I will show how verbal and non-verbal forms of masked communication have been used as tools to mark identity, express political dissent, protect from incarceration, cope with oppression and even gain freedom. Steganography has the tactical potential to shield against surveillance and censorship, as well as the poetic potential to foster collective affinities.

76. Cathy Silber, 'Writing From the Useless Branch', *Cathy Silber* (blog), 2011, accessed 3 October 2017, https://cathysilber.wordpress.com/writing-from-the-useless-branch-chapter-1-introduction/.

77. Anna T., 'The Opacity of Queer Languages', *e-Flux*, no. 60 (December 2014) accessed 1 March 2018, http://www.e-flux.com/journal/60/61064/the-opacity-of-queer-languages/.