Note

E-Fears, E-Risks and Citizen-Intelligence: The Impacts of Surveillance on Resistance and Research

Patricia Widener

Florida Atlantic University, US.
pwidener@fau.edu

Introduction

Digital communications support public campaigns by enabling greater online participation, public organizing, information and face-to-face exchanges, and by increasing a sense of national and international solidarity. Online engagement also allows the public to post and comment on others' opinions, and continue online exchanges at convenient times and locations. Though such exchanges may be fairly constant, their volume may escalate during times of contentious local issues or peak social movement activities. It is at these times of increased mobilization that electronic fears, or e-fears, of citizen privacy protections and more general concerns over electronic risks, or e-risks, are raised. Meanwhile, the impact of cyber-surveillance and citizen surveillance fears on the social science research process is even less understood.

The primary intent of this research note is to begin a conversation on how the perception of online surveillance impacts citizen organizing and the research process. In particular, this research note recognizes the inability of researchers to guarantee confidentiality and identity protections to research participants. These comments are based on the e-fears and risks identified by some citizen-activists and non-governmental organizations (NGOs) in Aotearoa New Zealand mobilizing against new oil extraction proposals. One campaign formed to resist deep offshore seismic testing, exploration and drilling; another focused on onshore hydraulic fracturing.

This research included 66 qualitative interviews, participant observation, and attendance at 44 events from 2013 to 2014 in 23 towns or cities. To protect participant identities, I doubled the number of interviews from 66 to 132, and then randomly assigned each interview two different numbers, using an online source (www.random.org). This research note is not based on the original intent of my research (to study oil resistance in a time of climate change and oil disasters), but on the unexpected comments expressed by some participants, which then led to more targeted questioning toward the end of my fieldwork. To be clear, only a small proportion of participants identified surveillance as a concern.

The Impact of Suspicion

The suspicion of online surveillance may be making some community advocates and potential research participants alter their online activities and relationships to protect themselves and their organizations and

to maintain a sense of privacy and control over their cyber-presence. This case study indicates that the presence of oil advocacy (by state and industry) and resistance (by citizens and NGOs) may create a loop of observation and mistrust. So for the uninterrupted access and extraction of oil, corporations or states may covertly observe, document and store the online activities and comments of citizen-activists. Likewise, citizen-activists are explicitly observing the state and corporations (or gathering “citizen-intelligence”). If the researcher is known or has been identified by the state and corporations, they may be observing the online activities of the researcher, who is trying to openly observe the state, corporations and citizen-activists, the latter of whom may be observing and gathering citizen-intelligence about the researcher. I am not saying that data were collected on me, but that justifiable unease about the possibility of physical and online surveillance becomes one contemporary hindrance when questioning, resisting or researching state-supported, petroleum projects.

Two points are important. First, online surveillance is a way a political system supports private industry through the exchange or access of intelligence at the expense of citizens. This suggestion supports Eveline Lubbers’ (2015: 338) work in identifying the “close cooperation” between states and corporations “in collecting intelligence on campaigners.” Second, the presence of a researcher studying activism may heighten an individual’s e-fears or e-risks. Though activists interviewed could not prove cyber-surveillance or corporate or state-level data gathering, they expressed a cautious disquiet that it was or could be happening, which instilled enough doubt as to alter their online activities. According to one research participant:

The fear that it could happen is real. It tends to make you think twice about hitting the send button definitely. Makes you stop and not necessarily express that feeling you have on Facebook or in an email or on the phone. It does. People are on guard. You say a word, and they say, ‘Oh, don’t say that word.’¹

By establishing a physical and online campaign of resistance, citizen-activists suggest data about them may be collected for unknowable uses now or in the future. Citizen misgivings of the loss of their privacy due to electronic surveillance or the online publication of their activities infused trepidation and disrupted individual and group activities—even if those risks were not proven or real. To better understand the impacts of surveillance, this research note will first illustrate three past events that gave rise to this unease, before describing citizen concerns over controlling their online images. Next, this note will present how potential participants question and investigate the authenticity of the researcher and how the researcher may be constrained in protecting participant confidentiality and anonymity.

A History of Infiltration and Surveillance

In Aotearoa New Zealand, citizen-activists resisting extractive projects based concerns of state or industry surveillance on three national events: the 2002 Terrorism Suppression Act; the 1999 publication of *Secrets & Lies* by Nicky Hager and Bob Burton; and the 1985 infiltration and bombing of Greenpeace’s *Rainbow Warrior*. Each a project of their time, the first act indicated a globally integrated surveillance scheme (operating for both public and private interests); the second revealed a state’s determination to influence and control public land use; and the third exposed another nation-state’s on-site involvement or infiltration in the operations of citizen-activists organizing in their own sovereign state. Overall, and for the past three decades, grassroots and professional activist communities had experienced external threats to their operations or campaigns. From these experiences, some reasoned similar efforts (excluding the bombing)

¹ Interview #122. To mitigate e-risks the place of interviews is not provided as the communities are quite small in a nation of 4.4 million people and many local citizen-activists are known by name given a community’s size. The date is not provided as my schedule and movement in the country could be determined by the public talks that I gave and public events I attended, which would then indicate the small pool of people whom I could have interviewed.

could be launched to weaken their resistance against the new wave of offshore and onshore oil permits and proposals. Each is discussed below.

The first and more recent event that predisposed citizen and environmental advocates toward fearing state-controlled cyber-surveillance was the Terrorism Suppression Act of 2002. Using that Act in 2007, the police raided numerous homes and arrested 17 people. The sweep included people who identified as Māori activists, environmentalists, peace activists, union organizers, animal rights campaigners, and at least one veteran (see Morse 2010a). The state indicated the arrests were due to firearm and paramilitary style training occurring in or near the Te Urewera National Park, and the sovereignty claims of the Māori Ngai Tuhoe community over land loss in the Te Urewera area. At the time, Valerie Morse (2010b: 17), identified her arrest as part of a trend which indicated “the unproblematic linking of activism with terrorism.” Morse speculated that the raids were enacted to demonstrate commitment to the U.S.; to advance resistance to ongoing calls for sovereignty among one Māori leader; to use the surveillance equipment purchased after 9/11; and to silence dissent on a range of issues. Russell Lee, another person arrested suggested that it was a “signaling of a preparedness and willingness to use those tactics domestically” (Lee 2010: 57). The police file included approximately 18 months of intercepted communication via text, phone, and emails. Many of the anti-drilling activists knew of this case, which generated media attention due to the arrests and subsequent trials, detentions, protests, eventual release, and at least one book (*The Day the Raid Came*), and one documentary (*Operation 8*). One research participant, uninvolved in those raids, cited them as “a really good way of demoralizing any activists in the country.”²

In the U.S., surveillance and arrests of environmental activists after 9/11 have also been documented by Will Potter (2011). He argued that those groups tasked with investigating domestic “terrorism” focused on environmentalists and animal rights groups that targeted corporate interests rather than anti-government or domestic militia groups that targeted federal agencies or public interests. Dana Priest and William Arkin (2011: 71), writing in *Top Secret America*, were also concerned—not about the environmentalists—but about the “terrorism-industrial complex” and the scale of institutional secrecy, extensions, expenditures, facilities within facilities, and public agencies within public agencies employing public personnel and private companies, without the demonstration of increased domestic security. A tremendous amount of data is being collected, Priest and Arkin argued, without public understanding or consent or adequate indication that the nation is safer. Each of these accounts seem to indicate a twofold intent: to protect the state from known or unknown threats and to discourage citizens from participating in civic life and public engagements that may question the existing or future political and/or economic arrangements.

In the second account, Hager and Burton (1999), through insider access to photocopied reports and communications, documented how the public relations campaign of a state-owned timber company infiltrated and monitored activist groups, whom were trying to protect a native forest. Given Hager and Burton’s findings, efforts to protect one’s online documents and correspondence would seem prudent. Given the global reach of transnational corporations (TNCs) today, especially in the petroleum sector, even more prudence seems warranted. Some activists interviewed between 2013 and 2014 knew of this work and its possible implications for their own campaigns. Perhaps underscoring citizen awareness and concern, Hager spoke on “Surveillance and Privacy in the Snowden Era,” at a University of Otago conference in 2014.

The third event in New Zealand, not identified by the younger activists, occurred in 1985 when Greenpeace’s *Rainbow Warrior* vessel was bombed as it was preparing to block a French nuclear detonation test in the South Pacific. One person was killed. At the time, Greenpeace’s Auckland office had

² Interview #52.

been infiltrated and campaigners were befriended by a French agent, who was one of several French cells operating in the country to disrupt Greenpeace's efforts to stop nuclear testing (King 1986).

These documented occurrences underscore the concerns among anti-drilling activists of being infiltrated or spied upon (through physical or cyber-surveillance) by public or private entities for political or economic gain. In the past, activists anywhere in the world may have believed their telephones were tapped, their cars were tampered with, their groups infiltrated, their homes observed, and their actions monitored (see Widener 2011 for examples in Ecuador when contesting an oil project). However more recently, and as indicated in this 2013-2014 study, those resisting state support of oil projects were confessing to an e-fear, of what is perceived to be the chronic yet indeterminable risk of online surveillance and the manipulation of online images.

There are other anecdotal stories of surveillance. When I presented two talks on the impacts of surveillance on research in 2014,³ at least two in the audience mentioned an incident that would cause one to pause and check their own activities. A student, who was using a telephoto lens to photograph a refinery site in the U.S.,—not from an activist's position but for the gritty, industrial art images—was contacted by the FBI and interviewed about their activities after a neighbor had observed the student-photographer and called the FBI. Another identified that an organization they had previously worked for had been broken into and that the group believed the computers were stolen for the information stored on them. These two anecdotes are presented here as harbingers: when people attempt to engage in social life and to be members of civil society, they may risk suspicion, surveillance, and disruption.

Fearing Surveillance or an Oil Disaster

People who hold strong views against state-endorsed, private oil projects may not want to make their opposition publicly known or have it displayed online, if they believe the state will respond. According to another citizen-activist, it is best to talk to people in person: "It's all tapped. ... [This one group] has already had the police around, just to enquire, 'You're not going to do anything at sea?' And they said, 'No, of course not.' ... So it's not so easy [to organize anymore]."⁴ This citizen-activist believed that private information conveyed through various means of telecommunication could be used against an individual or community group if it appeared they were conspiring to commit a crime (against state interests) as identified in the Terrorism Suppression Act.

In contrast, engagement in public discourse or displays to contest or question seismic testing or exploratory drilling, to protect human and marine life, or to reduce global greenhouse gas emissions could be viewed as the right and responsibility of citizens to be informed of and participate in issues of national and global importance. "Citizen-intelligence," or what I am calling the agency of citizen-activists to collect and share data for mobilized resistance against state or corporate projects—as in the spirit of Habermas' (1985) "communicative action"—may be challenged and disrupted reactively (once mobilized) and proactively (before mobilized) by state and corporate interests. Citizen-intelligence is the counter to Lubbers' (2015) "activist intelligence" or the increasingly proactive intelligence and surveillance of activist groups gathered by company sleuths, employed by TNCs, including petroleum and agricultural corporations. These corporate agents collect online data on anti-corporate activists and promote favorable public understandings of corporate products or activities. To Lubbers' work, I add the importance of understanding "citizen-intelligence," including the data collection of citizen-activists on the state and

³ This research note is based on these two talks in 2014, one at the American Sociological Association annual meeting ("Learning in the Field: Ethical Differences, Time Banking, & Online Privacy Protections"), and one at Society for the Study of Social Problems annual meeting ("Technological Impacts on Environmental & Community Advocacy: Electronic Surveillance & Public Participation").

⁴ Interview #76.

TNCs, as well as the ability and interest of potential research participants in gathering data about the researcher.

After I had completed my interviews, the worried citizen-activists and NGOs received confirmation that their online communication could be collected, validating some of their suspicions. As reported in the *New Zealand Herald*, Edward Snowden, the former U.S. National Security Agency (NSA) systems analyst, who leaked American documents and was residing in protection in Russia at the time, spoke via an online video connection to a town hall meeting in Auckland. Snowden told the audience that the Government Communications Security Bureau (GCSB) was collecting data on New Zealanders for the U.S. This information, they were told, could be accessible by their own government (Bennett, Quilliam and Cheng 2014; see also Lyon 2015).

Before this town hall meeting, several activists believed their emails could be obtained so as to monitor their activities or campaigns. Though they could never verify it, the hardship on the individual, family and campaign is the idea that this systematic monitoring could be happening. The town hall meeting would have heightened their belief of the possibility, further threatening their civic desire to speak, share information, or organize online. For some, the risk of an oil disaster appeared to be a greater problem than the risk of surveillance; but that may not be the case for everyone. For the researcher, it is a struggle to identify, meet or interview this pool of citizens who may desire a more active role in civic life but elect not to because of these fears.

Control over One's Digital Images

Another concern is how grassroots campaigns have been affected by the ease and speed of distributing photographs and videos online. The paradox is in the need for citizen campaigns to have an online presence while being unable to control how others present online images of one's actions. Professional and grassroots groups often need a publicly accessible online profile to attract new supporters, to announce events, and to be engaged in a public and transparent manner—a practice they request of the state and corporate oil interests. Yet while event organizers want public and media attention and the perpetual online image of their campaign, individual members may be wary of their own image associated with the campaign, especially on websites they do not control.

At one public rally, a person held a provocative sign when hidden in the middle of a group, but hid the sign when I tried to photograph them individually. It appeared that some people are comfortable with some public display, but are uncomfortable with how those images could be manipulated by others at a later date and in a different context. At this coastline demonstration for example, a pro-oil and gas counter-group had a supporter taking photos of the event, and then posting them online in a manner that mocked the anti-drilling activists for driving cars and using petroleum-based plastic raingear and kayaks.

Given this pro-oil tactic, private people who may want to act publicly on their convictions or join grassroots campaigns or public demonstrations may not do so for fear of losing a sense of privacy and control over their own online images. On controversial issues, manipulated or misrepresented images could harm a person's current or future employment, neighbor relations, or lives of their families. Through the open displays of such surveillance (public online mocking or shaming tactics), citizens may interrupt their own engagement to protect their economic or social well-being.

At a public talk I gave on "Oil & Society," the audience was a mix of academics, students, community members, and those with a general interest in the subject, including a media photographer.⁵ During my presentation, a person in the audience complained about the photographs being taken. The photographer

⁵ Public presentation, "Oil & Society," at the Centre of Sustainability CSAFE, University of Otago, Dunedin, 4 February 2014.

identified themselves, and asked the audience for permission to continue photographing the free public event. Although others agreed, the person who complained rejected the request, citing public privacy concerns and the potential of others (not the photographer) to use the photograph in a manner that could be harmful or damaging to them in unexpected ways in the unforeseeable future. The audience member had attended the surveillance conference the previous month. Even now, I worry that my comment here is an invasion of a person's right to speak freely at a public event. With the ease of tracking, misusing and misappropriating online public talks and broad audience panoramas, it is important to acknowledge these public concerns. It is especially crucial to recognize the risks perceived by individual citizens, who are unprotected by professional institutions or organizations.

Even more troubling for civil society and civic engagement is that others may avoid public gatherings organized to raise awareness or exchange information. If they perceive their activities or presence will be monitored, documented and distributed overtly or covertly in a manner they cannot control, and in a manner that could jeopardize their employment or sense of safety, they may stay home. Moreover, online media surveys or public submissions to local, regional or state queries over a debated project (all tools that I use in my research) may pose unintended risks if identity markers are required or traceable, especially for the more vulnerable grassroots citizen-activists. Much like attendance at public demonstrations or talks, citizens may reduce their online submissions or dilute their messages if they believe a cyber-fingerprint links them to the comment or if such associations will be used against them in the future. For the researcher, it is challenging to assess the one who stays home or fears making one's private thoughts public. We know these actions as a chilling effect, and they have occurred perhaps since the formation of nation-states and their protected and legal use of force. Nevertheless, the fear of online surveillance, collection and data storage elevates and extends the sense of risk for individual citizens who may want to question or contest a state-permitted or large-scale project of global interest.

Knowing the Unknown yet Knowable Researcher

Suspensions of cyber-surveillance may also increase the distrust among citizen-activists regarding unknown researchers, social scientists, or journalists. In this case, activists photographed me taking photographs of them at public actions. It seemed that some of them were documenting my presence as an unknown photographer or unknown "researcher." Researcher-in-quotes reflects that some of them knew me as having presented myself as an academic and researcher (some I had interviewed). But if they believe they are organizing under an unknown degree of surveillance, who can know for certain the alliance or affiliation of the researcher? For some, my presence at public meetings or events was unclear. I could have been employed by a corporation, state agency, or industry association to gather information, or brought into the community to build industry support or form an "astro-turf" organization or campaign. ["Astro-turf" is used to depict a non-local, industry-supported counter group, which has been developed to support industry interest in contrast to a local, grassroots, community-based campaign.] The layers of concerns over photographic documentation, image control, and online displays intrude on community events and introduce increased degrees of distrust and misgiving among people trying to build a community response to what they believed to be an external threat: the transnational oil and gas industry.

Citizen-activists who engage in citizen-intelligence or online data gathering are also empowered to investigate the researcher. Alongside the uncertainty is the online opportunity to establish "trust of identity" or "validation of authenticity" of the researcher. Although online technology may have compromised a citizen-activist's sense of safety and privacy, online technology also lent control and agency to them, which is a positive step forward in the research interchange. In a first page search, participants could access my employment, publications, presentations, teaching schedule, and student evaluations. These investigative endeavors in the name of citizen-intelligence also meant they could go into an interview influenced by what they read online, as researchers are influenced by their own online inquiries before meeting professional and grassroots organizers.

Protecting Participant Confidentiality

As a final point, online technology also affects qualitative fieldwork in terms of accessing and protecting the identity of potential participants. For example, if participants believe that their email accounts and online activities could be accessed (legally or illegally but without notification), then it may be possible that the researcher's email could be accessed, placing the research participants' privacy and confidentiality at risk, as well as the research project. Eventually, and importantly, to study activist campaigns and pass institutional and ethical review boards, the researcher may need to guarantee online protections, which we are unable to achieve.

There also exists an online-profile conundrum for the participant and researcher. Some potential participants were accustomed to being "found" or approached online, especially if they had been in the public eye and had expressed strong positions on certain local or national issues. Their understanding of their own online presence facilitated introductions, though apprehension may persist when the "researcher" is an inquisitive U.S. citizen and the activists are contesting a U.S. oil company.

During my fieldwork, others, particularly first-time citizen-activists, were shocked, puzzled, and disturbed by how their identities and contact information were found online. Even though they had taken a public position against a state and multinational project (and perhaps because it was their first time wading into anti-drilling activism), they had failed to understand the ease of identifying them and accessing their contact information. Some had failed to imagine that a public comment against oil may become permanently available online to anyone, including international researchers. In those instances, they would reply: "How do you know about me? How did you find my information?" The answer is an easy one: online.

Though I lack the skills to conduct anything but the most basic search, my email introductions and requests for an interview revealed to community advocates that an international audience was observing their online activities of resistance far beyond their fence-lines or coastlines. For some, this brief exchange initiated or added to their discomfort about the online world. In one email correspondence, one responded:

A concern that came to mind when I read your attachments was "could the information I give you in any way make more difficult our efforts?" I was thinking of who would read your material and would this help industry and government to know how to undermine or stop our efforts to gain and share information.... I am also wondering how you came across my name?

The people identified had been interviewed in the local media, had spoken at a public meeting, or had a publicly accessible online group or Facebook page that referenced citizen or environmental resistance against the state's efforts to begin oil exploration in new blocks; against the state's bidding process and lack of citizen consent or notification; and against the arrival of multinationals. Even though they had an online presence on this polemical issue, some had not considered its full meaning until I contacted them online.

The email reply also captures the anxiety that community activists bear about the perceived peril imposed upon them by government agencies, TNCs, and unknown researchers. Citizens with an opinion different from the state and researchers engaged in standard research practices should not feel apprehension in democratic and open societies, but we do when contesting, questioning or researching extractive industries with influence and resources that appear to be much greater than our own. As for this researcher, disquiet persists over the extra-burden placed on citizens (or potential research participants) by my presence and quest for an interview.

TNCs have hired social scientists to gain access to communities or to design community-bridging programs in places such as Ecuador (Widener 2011). As incongruent as it may seem, it may have been easier to conduct oil-related research in Ecuador more than a decade ago when the degree of online surveillance was less prevalent and the Ecuadorian government focused on the physical threats from laboring and Indigenous communities, who possess knowledge and access to block the flow of oil, rather than resistance from environmental groups. The established environmental groups negotiated with the industry, while the nature-based community groups, first-timers to the presence of oil, fractured or were slow to mobilize. At the time, I was more concerned about protecting my computer, rather than protecting online exchanges. For Adam Briggie (2015: 123-125), a philosophy professor and resident of an oil and gas state in the U.S., civic engagement and academic life collided when an FBI agent and a police representative visited his campus office unannounced to ask about his community involvement in questioning hydraulic fracturing, his classroom teachings, and a former student, who was an environmental activist.

Today, state leaders and energy companies may perceive domestic threats against oil frontiers as an intellectual or cyber one. The threat is living among or being launched from a cadre of online information-sharing communities, researchers, and scholar-resident-activists. Citizen-activists, the state and corporations each engage in tactics of intellectual endeavor (knowledge collection and exchange) and physical struggle (action, arrests and warnings). On the physical side, for example, activists in Aotearoa New Zealand, were arrested when protesting at sea against Petrobras' exploring rig. Eventually, a judge ruled that the police had no jurisdiction beyond the 12 mile coastline limit. Certainly the social movement researcher is an observer or listener of protest; but in an atmosphere of surveillance, the researcher may become an unwilling participant in conjuring safety and privacy concerns for the observations and access we desire to make.

Implications for Research on Social Activism

In an atmosphere of cyber uncertainty, distrust and surveillance, researchers formulate research questions and initiate research projects, while deliberating over their inability to guarantee or secure privacy and confidentiality protections, and how their presence adds to the distress of some citizen-activists. This research note is an attempt to encourage discussion on how knowable and unknowable e-fears and e-risks impact community campaigns and the research process. Though a researcher's online presence may minimize participant concerns and serve as an authenticity voucher, an unknown (yet knowable) researcher may also contribute to citizen apprehension regarding the durability and misuse of their online comments or actions. From among us, suspected and observed surveillance schemes may quell (or launch) campaigns of resistance and research. Yet least identifiable are the citizens who avoid engaging in civic life or contesting a local project due to the fear of indeterminable repercussions. Their absence weakens the knowledge and potential of civil society, and it is an absence that demands to be studied as a complement to Lubbers' (2015) call for increased research on corporate activist intelligence. Finally, the subjective experiences and anecdotal comments featured in this research note also invite a greater discussion on when and how surveillance fears not only disrupt citizen activism but also impede social movement research.

References

- Bennett, Adam, Rebecca Quilliam and Derek Cheng. 2014. US Spies Have Two Bases in New Zealand: Snowden. *New Zealand Herald*, 16 September.
- Briggie, Adam. 2015. *A Field Philosopher's Guide to Fracking: How One Texas Town Stood Up to Big Oil and Gas*. New York: Liveright Publishing Corp.
- Habermas, Jurgen. 1985. *The Theory of Communicative Action, Volume 1*. Boston, MA: Beacon Press.
- Hager, Nicky and Bob Burton. 1999. *Secrets & Lies: The Anatomy of an Anti-Environmental PR Campaign*. Nelson, Aotearoa New Zealand: Craig Potton Publishing.
- King, Michael. 1986. *Death of the Rainbow Warrior*. Auckland, New Zealand: Penguin Books.

- Lee, Russell. 2010. Hamilton: Russell Lee. In: *The Day the Raids Came*, ed Valerie Morse, 47-57. Wellington, New Zealand: Rebel Press.
- Lubbers, Eveline. 2015. Undercover Research: Corporate and Police Spying on Activists. *Surveillance & Society* 13(3/4): 338-353.
- Lyon, David. 2015. The Snowden Stakes: Challenges for Understanding Surveillance Today. *Surveillance & Society* 13(2): 139-152.
- Morse, Valerie (ed). 2010a. *The Day the Raids Came: Stories of Survival and Resistance to the State Terror Raids*. Wellington, New Zealand: Rebel Press.
- Morse, Valerie. 2010b. Introduction. In: *The Day the Raids Came*, ed. Valerie Morse, 11-18. Wellington, New Zealand: Rebel Press.
- Potter, Will. 2011. *Green is the New Red: An Insider's Account of a Social Movement under Siege*. San Francisco: City Lights Books.
- Priest, Dana and William M. Arkin. 2011. *Top Secret America: The Rise of the New American Security State*. New York: Back Bay Books.
- Widener, Patricia. 2011. *Oil Injustice: Resisting and Conceding a Pipeline in Ecuador*. Lanham, MD: Rowman & Littlefield.