Whistleblowing and Digital Technologies: An Interview With Suelette Dreyfus

Luke Heemsbergen, The University of Melbourne, Australia

Luke Heemsbergen: Suelette, you've held a long interest in whistleblowing and digital technologies. There seems to be a building renaissance for 'digital whistleblowing' as automated, digital knowledge-gathering technologies proliferate new possibilities of control and disclosure. First, do you see the current leak-scape as a technologically determined moment, and a product of its time? And second, are these leaks necessary and are they sufficient to find autonomy/freedom in what seem to be increasingly automated systems of control?

Suelette Dreyfus: The current whistleblowing landscape is a convergence of a number of things: technology, war and public distrust of institutions such as government, politicians, the Catholic Church, some large corporations. The technology involved is more than just the technology used in whistleblowing systems, it's also online publishing technology, security and privacy technologies and, of course, mass eavesdropping technologies.

I study both the technology *and* the humans - and how they interface - in order to understand this. It is not technologically determined and a product of its time, so much as human determined, as humans are a product of *their* time. Human ingenuity and resilience are terrific renewable resources. Both have played a role in changing this landscape. For instance, the US is quite amazing. Here, on the one hand, is a very well resourced army of military and intelligence apparatuses running a surveillance state. More than a million and a half people have security clearances - there are more people with top secret clearances than there are citizens of Washington DC. And on the other hand, there is a growing cabal of remarkable citizens who have just said ENOUGH. These citizens have few resources other than *voice* but they do have a good ability to ask rational questions and organize using online technologies.

These are the people who are, for example, behind recent campaigns such as 'Restore the Fourth' on the 4th of July. They want to restore the Fourth Amendment of the US Constitution, which they say has been cast aside as a result of the rise in the surveillance state. These are the thousands of Americans on Twitter, essentially saying "stop spying on us and treating us as criminals."

That is paraphrased of course, but the sentiment is about right. They are moving to-

To cite this article: Heemsbergen, L (2013) 'Whistleblowing and Digital Technologies: An Interview With Suelette Dreyfus', PLATFORM: Journal of Media and Communication 5(1) (October): 67–71. ISSN: 18365132 Online © Creative Commons 2.5 Australia licence

ward a tipping point.

The irony of the situation was recently splashed across the front page of the *Washington Post*. One lead story disclosed more on the revelations of the surveillance state, while a second story described how American children are going hungry. In places like rural Tennessee, more than one in four children need government food assistance, a record level according to the *Post*. School buses are running during holiday periods to deliver food to families that just don't have enough money to eat. The holiday deliveries fill in the gap - because there is no school, there is no lunch provided to the children. So they go without food. In the United States, adults come out to greet the school bus asking if there are leftovers.

One story (vast surveillance projects steeped in secrecy and the military state that is attached to this) represents a contributing cause of the second story (visible hunger in the streets of the United States). States need security. However, if a state spends huge amounts of money spying on its citizens and waging a 'war on terror' more generally, there often isn't enough left over to do things like providing jobs programs to get people back to work, or providing good, free education to increase the likelihood of getting a job, or balancing the budget so cities and states don't have to lay off employees or declare bankruptcy. Children may go hungry. That is the trade-off.

The importance of whistleblowing in this context is that it reveals when and where this alternative, secret world produces illegal, immoral or wasteful behaviour. The secrecy means that it is possible to hide very substantial wrongdoing and corruption before it may burst, like a boil, into the public arena. Whistleblowing may yet save the patient and restore them to good health.

LH: Edward Snowden was working for the contractor, Booz Allen Hamilton, which in a statement concerning his leaking activities wrote, "If accurate, this action represents a grave violation of the code of conduct and core values of our firm." This is a remarkable quote that begs the question, what are the core values of such firms? Looking at what Dana Priest and William M. Arkin have described as the 'Top Secret' industrial complex as a cybernetic system, what are we to make of this network of retrenchment that seemingly perverts ideas of national interests into the norms of secrecy?

SD: Based on the Priest-Arkin story, it seems no one in the US even actually knows how many tentacles this octopus of a secret state has. Public interest organisations like the Government Accountability Project (GAP) in the US cannot determine or find out simple things like "what is the total budget for the NSA and the rest of the surveillance state?" We don't really know what they do and we don't know what they cost. It's all secret. These things need to be public so that the public can decide if this is how it wants its money spent. This seems an obvious, if missing, feedback system for democracy.

Running a functioning democracy when the people do not have oversight of how their money is spent on the massive surveillance and security state (in even in the most broad-brush way) calls into question the legitimacy of that government.

We're heading toward a positive public tipping point. One of the most worrying recent developments is the flip side to secrecy networks, namely the new powers of propaganda that are available to the government. With barely a peep issued by the US mainstream media, in the middle of 2013 the US Government began unleashing a large channel of propaganda inside the US. While the government has used propaganda effectively against other nations - notably in Europe during the Cold War - laws had prevented it from turning that formidable propaganda machine on its own people domestically. Congress recently removed that ban.

The result is deeply disturbing 'perfect storm'. The surveillance state no longer just spies on citizens, it now can quite legally tell them what they should be thinking as well. While existing government media outlets such as *Voice of America* may generate good reportage, these government media outlets were always intended to be used as a communication tool from the US government to the rest of the world, not a propaganda tool to sway the American people that things such as the 'War on Terror' are a 'good thing.' A big part of George Orwell's '*1984*' is not just about government watching the citizenry, it's about government brainwashing them. The blandly named ' *Smith-Mundt Modernization Act of 2012*', which Congress approved as part of the 2013 *National Defense Authorization Act*, has the potential to push the US much closer to Orwell's '*1984*' than most people realize. Yet few media carried this story in July 2013, when the changes came into effect.

LH: Julian Assange has suggested that as one's political-institutional power increases, so too should transparency into their affairs. That is to say the general online user should be able to remain anonymous while political representatives should be held to a more open standard. Is online anonymity, and transparency in power, a possible and beneficial way to live and govern digital life?

SD: This philosophy of institutional transparency and individual privacy is definitely doable and can be translated to the real world. All it takes is the political will to demand it, and then the will to do it. And it's certainly beneficial.

One of the key elements within a whistleblowing relationship is, invariably, power. The whistleblower is almost always lower down the totem pole than the powerful that he or she is blowing the whistle on. Further, when the institution tries to block and then blame the whistleblower (as often happens) the relationship changes to become the entire institution versus one person. That is a very disproportional relationship in terms of power and resources.

I suspect that the reason that Assange espouses that the more power/less privacy philosophy is important is that it rebalances the above power relationship. Things often work best when there is a tension in the wire, a peaceful balance based on a suitable level of tension. The level of that tension at the moment is out of whack, pushing some democracies toward a state of either dangling loosely or snapping. When there is a proper balanced tension in the wire, the cost of those in power being involved in wrongdoing is reasonably high. This creates a disincentive toward committing fraud or other serious wrongdoing, because it might easily be exposed in the public arena.

LH: Your research has also focused on 'hacking' culture and activities that are performed for autonomy, but use high levels of technological automation and surveillance. Clandestine and automated surveillance here is useful for whistleblowers, hackers and their counterparts trying to protect secrets and snoop on populations or catch digital intruders. It is a fascinating dynamic. What available modes of resistance are sustainable in this context of increased automated monitoring?

SD: First, cryptography. Strong cryptography for everyman. That ensures individual privacy. Presently, the learning curve is reasonably high for an average person but once you know how to use it, it is definitely sustainable.

Second, using open-source software where available. It's clear now that a number of tech companies have non-transparent and very close relationships with the US intelligence agencies. Are Apple products backdoored? Who knows? Snowden's revelations this year suggest that what was once in the realm of high-end computer security experts (inside knowledge), and conspiracy theorists (hypothesis) is now very much more in the realm of reality. It is quite reasonable to hypothesize that secret arrangements between government and entities like Microsoft and Apple may involve handing over any number of hacking backdoors to government. With open-source software this is harder to do since the code is transparent for all to see. So, where privacy for the citizen really counts, using open-source operating systems like Linux is sensible.

The Electronic Frontier Foundation (EFF) has an excellent free online resource called 'Surveillance Self-Defense'.

LH: I want to turn now to the culture that surrounds groups like Anonymous, and the tools that are preferred to crowdsource online attacks (e.g. The Low Orbit Ion Canon that creates DDOS attacks). Within this space there are levels of automation, which allow script kiddies or 'clicktavists' to engage through the inactivity that accompanies automation. How have you seen this line between (in)activity and automation breached in hacker culture, and do you see those types of active political moments filtering into more widespread modes of political engagement?

SD: First, I think it is important to differentiate between the Hacktavists, and their desire to be positive social change agents, and the script kiddies. There are some script kiddies who are Hacktavists and vice versa but it is not a matched set.

Second, I don't agree that clicktavists are 'engaged in inactivity' so much as 'engaged efficiently'. They spend their most valuable resource - time - reading about a cause and then participate in the most time-efficient manner for them by exercising *voice*. It is highly efficient for them to contribute in a common format that matches the format of others they agree with because this sends a simple, unified message of what is demanded to decision-makers. Automated technology allows this 'opt-in conformity'. In doing so it also has the added benefit of providing a fairer voice to those who may be unable to exercise voice by, say, choosing to march in the streets (the single mother home with a baby, the elderly person who is disabled, etc.).

Script kiddies are another story. They are also maximizing efficiency, but differently. They do so because it would be too hard and take too long for them to learn how to develop and to use particular exploits they originate. So they 'buy it' off the shelf, so to speak. There can be lots of motivations at play here, from fraud and gangster behavior down the spectrum to civil disobedience based on a high moral ground, and further down to hacktavism and whistleblowing. It is a spectrum with many different points on it.

LH: Finally, I wanted to shift gears from the hacker activity to journalistic activity. As a publisher, WikiLeaks changed perceptions about how newsworthy information should be obtained, mediated and published. How do you see roles and models of publication evolving? Will journalistic freedom be a creature of the light feeding on open data? Or will it be a creature of the shadows, pecking away at what is hidden?

SD: Journalistic freedom will be both. But feeding on the open data may pry open more hidden data in the long run because it will revolutionise thinking for the next generation. The open data movement is shoveling the secrecy culture - so symptomatic of the War on Terror - backwards. Prying open secrets is coming from both the inside and outside.

For example, whistleblowers that reveal serious wrongdoing provide the evidence for more need of accountability (and fewer secrets). However, the open data movement is pushing very much from inside organisations outwards. Good people inside corporations, government - any number of institutions - are gently coaxing their organisations toward a culture of open data from the inside out. They are slowly replacing the crusty Mandarins, with their rigid old-think attitudes that the public must be kept in the dark, and that information should be kept confidential unless there is a good reason to release it.

This is starting to happen around the world. The new paradigm is arriving. Representative sample surveys - which I have been involved in - have revealed that half of all Australians believe too much information is kept secret in organisations. Indeed only about a quarter or so of people think the right amount of information is kept secret. That's a pretty good indicator that people want a change. They don't necessarily want to fling open the doors of every government office to everyone. Most people are sensible and balanced. But they also seem to be saying, "Hey, we are at the wrong point in this spectrum."

Even more tellingly, more than 80 percent of people in Australia want whistleblowers to be protected rather than punished for revealing serious wrongdoing, even if the whistleblowers have to publically disclose inside information. There are similar or even stronger figures out of the UK and Iceland. There is significant empirical evidence that shows this. The large majority of citizens in these countries want whistleblowing to be a protected activity.