**Selected Papers of #AoIR2020:**
**The 21st Annual Conference of the**
**Association of Internet Researchers**
Virtual Event / 27-31 October 2020

# THE MORALISATION OF PREDICTIVITY IN THE AGE OF DATA-DRIVEN SURVEILLANCE

Sun-ha Hong
Simon Fraser University

This paper argues that emerging technologies of datafication are intensifying a moralisation of predictivity. On one hand, this describes the growing pressure to quantify and predict every kind of social problem. Reluctance to adopt emerging technologies of surveillance is construed as abdication of a moral responsibility via negligence to inevitable progress. On the other hand, it describes the corresponding demand that human subjects learn to live in more predictable and machine-readable ways, adapting to the flaws and ambiguities of imperfect technosystems. This argument echoes that of Joseph Weizenbaum (1976), a pioneer of early AI research and the inventor of the ELIZA chatbot: that well in advance of machines fully made in our image, it is the human subjects that are asked to render themselves more compatible and legible to those machines.

Drawing from a book-length research project into the public presentation of surveillance technologies, I show how messy data, arbitrary classifications, and other uncertainties become fabricated into the status of reliable predictions. Specifically, the bulk of the presentation will examine the rapid expansion of counter-terrorist surveillance systems in 2010's America, focusing on three vignettes:

## 1. The Whole Haystack

I begin by examining the moralised public discourse around the predictivity (and preventability) of terrorism, and increasingly, its anchoring in the promises of data-driven surveillance. Expansive 'dragnet' surveillance as publicised by the Snowden leaks were rooted in the post-9/11 legitimisation of the idea that terrorism was becoming radically unpredictable. New systems for data collection and processing were thus justified through the persistent interpellation of uncertainty towards a moralised argument, in which the rapid expansion of new surveillance technologies was an ethical obligation to 'do something' as much as a calculated response to statistical and geopolitical realities. As Keith Alexander, the NSA's long-time director (2005-2014) put it, they were to not simply look for the needle in the haystack but to "collect the whole haystack" (Nakashima and Warrick 2013). The projected unknowability of the 'new

Suggested Citation (APA): Hong, S. (2020, October). *The Moralisation of Predictivity in the Age of Data-Driven Surveillance.* Paper presented at AoIR 2020: The 21th Annual Conference of the Association of Internet Researchers. Virtual Event: AoIR. Retrieved from http://spir.aoir.org.

breed' of terrorist was thus leveraged to broker public trust and political legitimacy for a new breed of data-driven surveillance and, in turn, pre-emptive intervention.

**2. The Lone Wolf**

Such revisionist narratives about past terrors in turn feed into unprovable claims in favour of new surveillance technologies from NSA dragnets to sentencing algorithms. Central here is the social life of the 'lone wolf' terrorist: a figuration of an unpredictable and unknowable threat, yet also the object of public belief around the possibility of prediction. Attacks like the Boston bombings and the Las Vegas shootings have been accompanied by formulaic public retrospectives, agonising over how the individuals must have been radicalised and how they could have been stopped with better data. This project to predict (and prevent) the unpredictable terrorist becomes a site of not simply indiscriminate surveillance or data-driven objectivity, however, but a back-door for enduring forms of discrimination and prejudiced heuristics. A leaked 2017 survey, used by the FBI to assess suspects under watch, attempted to datafy the risk of lone wolf terrorism through 'weak indicators' like playing paintball, laser tag, or 'undergoing religious conversion' (Currier 2017). An internal NSA slide, leaked by Edward Snowden, show fictional names like 'Mohamed Badguy' and 'Mohammed Raghead' used to denote hypothetical lone wolves (Davidson 2014). In this way, the 'anybody and everybody' of the 'whole haystack' is reduced down into the Arab and the Muslim. Yet the very phrase of the 'lone wolf', in fact, originates with white supremacist discourse in the 1990s. I argue that the insistence on predictivity reflects a broader faith in data as pure and sanitising — intersecting all too well with the older fantasies of national and racial purity in the war on terror (Puar and Rai 2002).

**3. Hollywood Endings**

On closer inspection, furthermore, surveillance data raises its own ambiguities. I show how practices like the FBI's counter-terrorist sting operations often reveal intense pressures to claim certainty on the basis of deeply uncertain data. 'Weak' indicators and other uncertain data are repackaged into more palatable forms to meet the political and moral demand to 'do something'. I discuss the case of Sami Osmakac, where FBI undercover agents and informants supplied Osmakac with money, with fake weapons and explosives that he could buy with that money, the training to use that equipment, and so on, until he has produced enough behavioural data to justify arrest. Here, electronic surveillance intersects with more traditional practices, legal classifiers like 'probable cause', and the heavily moralised climate of 'zero tolerance'. The result is a practice of not merely surveillance, but the active fabrication of the kinds of tangible data that can legally count as evidence of terrorist intent – or, as the FBI agents called it, a 'Hollywood ending' (Aaronson 2015).

These episodes are part of a broader pattern around the moralisation of predictivity vis-à-vis the fabrication of data's certainty. The presentation ends by noting how such algorithmic performances of objectivity and control are replicated in growing public-private partnerships for surveillance. For instance, I show how Amazon Ring's aggressive data-sharing with local law enforcement spearheads a broader corporate strategy for cultivating a new Faustian bargain between customer convenience and data extraction (see Zimmer 2008; van Dijck 2013). From the state's counter-terrorist strategies or consumer technologies' sales pitch, the deeply speculative nature of these

predictions are repackaged as both morally necessary and technologically inevitable. In short, we find a bias towards “actionism” (Hannah 2010) where doing something is construed as better, and more ethical, than doing ‘nothing’.

All in all, the moralisation of predictivity helps suture the many imperfections of data-driven surveillance, and provide justificatory cover for their breakneck expansion across the boundaries of public and private. They perpetuate the normative expectation that what can be predicted must be, and what needs to be predicted surely can be. In the process, spaces for human discretion, informal norms, and sensitivity to human circumstance – what we might call margins of tolerated ‘illegality’, in Foucault’s sense (2015) – are being squeezed out.

**References**


Aaronson, Trevor. 2015. “The Sting: How the FBI Created a Terrorist.” *The Intercept*. March 16. https://theintercept.com/2015/03/16/howthefbicreatedaterrorist/.

Currier, Cora. 2017. “48 Questions The FBI Uses To Determine If Someone Is A Likely Terrorist.” *The Intercept*. February 13. https://theintercept.com/2017/02/13/48-questions-the-fbi-uses-to-determine-if-someone-is-a-likely-terrorist/.

Davidson, Amy. 2014. “The N.S.A.’s Spying on Muslim-Americans.” *The New Yorker*. July 10. http://www.newyorker.com/news/amy-davidson/the-n-s-a-s-spying-on-muslim-americans.

Foucault, Michel. 2015. *The Punitive Society: Lectures at the College de France 1972-1973*. Edited by Bernard E Harcourt. New York: Palgrave Macmillan.

Hannah, Matthew G. 2010. “(Mis)Adventures in Rumsfeld Space.” *GeoJournal* 75 (4): 397–406.

Nakashima, Ellen, and Joby Warrick. 2013. “For NSA Chief, Terrorist Threat Drives Passion to ‘Collect It All.’” *The Washington Post*. July 14. https://www.washingtonpost.com/world/national-security/for-nsa-chief-terrorist-threat-drives-passion-to-collect-it-all/2013/07/14/3d26ef80-ea49-11e2-a301-ea5a8116d211_story.html.

Puar, Jasbir K, and Amit S Rai. 2002. “Monster, Terrorist, Fag: The War on Terrorism and the Production of Docile Patriots.” *Social Text* 20 (3): 117–48.

van Dijck, José. 2013. *The Culture of Connectivity: A Critical History of Social Media*. Cambridge: Oxford University Press.

Weizenbaum, Joseph. 1976. *Computer Power and Human Reason: From Judgment to Calculation*. New York: W.H. Freeman and Company.

Zimmer, Michael. 2008. “The Externalities of Search 2.0: The Emerging Privacy Threats When the Drive for the Perfect Search Engine Meets Web 2.0.” *First Monday* 13 (3).