Second draft, La Gaîté lyrique / 4 Jan 2016

Where Thou Art Shall I Be

By Finn Brunton

One of the earliest ghost stories on film is also about the most unsettling kind of haunting: 1913's *The Student of Prague.*[1] The titular student, a wild lad and swordfighter named Balduin (Paul Wegener), pining after a woman above his station, cuts a deal with a solicitous stranger named Scapinelli who offers him a fortune in return for any one item from Balduin's rooms. The item Scapinelli picks is Balduin's reflection, called out of the mirror. Balduin no longer appears in mirrors, and his *doppelgänger* turns up in his stead -- killing a man in a duel whom Balduin had sworn not to fight, among other things. At every step, his double -- him and yet not-him -- is there, poisoning his intimacies and ruining his chances, taken as him at critical moments to bring disaster. When they meet in a cemetery his double offers a terrifying promise: "Where thou art shall I be, unto the hour when I seat me on the stone of thy grave."

Paul Wegener also directed, as it happens. He made movies about the Golem of Prague, and it was tales of golems, demons, and other potent supernatural forces that dominated the imaginative folklore of computing for the second half of the twentieth century. These were sedulously literal-minded and limitlessly powerful beings who fulfilled their commands with horrific efficiency, and sometimes slipped off the leash. "If we ask for victory and do not know what we mean by it, we shall find the ghost knocking at our door," said Norbert Wiener

---

[1] Ewers, Hanns Heinz, and Stellan Rye. 1913. *The Student of Prague.*

in the 1950s, warning of the possible consequences of the computerization, cyberneticization, and automation of society, particularly the use of computers and game theory to control America's nuclear arsenal.[2] (Wiener is alluding to W.W. Jacobs's ghost story "The Monkey's Paw," in which parents wishing for money from a magical artifact receive it in the form of an insurance payment for their son, who is killed in a factory accident. Then they wish for him back, and back he comes -- but not *alive.*[3]) The spread of the Internet, social networks, mobile computing, and the blurring of on- and offline domains has produced a new vocabulary of fantasy for understanding the dangers we face, one that starts with Scapinelli inviting the reflection out into the room: not golems, but ghosts.

Because, of course, there are many of "you." There is the you who reads this now, in a body (presumably) that answers to a name, with traits and memories and social context. But many others answer to that name, that set of traits, that nodal position in a social network. Some of these yous are drawn in outline by browser fingerprinting and supercookies and Javascript for a variety of different advertising tracking networks whispering among themselves as you move from page to page, app to app. One lives on Facebook, another on WeChat, another in the database of a credit rating agency and a bank, another in your accelerometer, step, and sleep data, others still in the collections and dossiers of state security and surveillance services. The British surveillance

---

[2] Wiener, Norbert. 1961. *Cybernetics, or Control and Communication in the Animal and the Machine* (2nd ed). Cambridge, MA: MIT Press. 177.

[3] Jacobs, W.W. 1906. “The Monkey’s Paw.” In *The Lady of the Barge.* London: Harper & Brothers.

agency GCHQ maintains a suite of tools for analyzing the billions of intercepted materials it is accumulating, among them an "Internet diarisation tool" called SAMUEL PEPYS, which produces a kind of realtime "diary" of a target's online activity.[4] Pepys was one of the greatest diarists in the English language, and the choice of name is wonderfully telling: instead of the production of a rich, unique, private, internal subjectivity in the work of the diary, *this* is the kind of record that matters -- for their purposes, a truer and more useful record than whatever account a person might give of themselves. To the usual range of human hauntings (memories, regrets, unfinished tasks, lives we might have led) we have added a new category: a whole population of doppelgängers for every one of us -- some of whom wax in strength, standing in for us and acting in our name. As a practical matter, we live out that moment of cinematic horror when we look at the mirror and someone else looks back, with a smile for which we have no corresponding expression.

At least Balduin knows the root of his trouble, his singular double: they meet in the forest as his reflection walks from the duel he'd promised to decline, wiping blood from his sword. We may never be informed of the sins our many doubles have committed in our name, directly or indirectly, making us persons of interest for law enforcement, damaging our ability to get insurance or loans, even offering us correspondingly higher prices for the same goods. Our doppelgängers

---

[4] See "GCHQ Profiling: An Appendix," at https://theintercept.com/gchq-appendix/, as reported in: Gallagher, Ryan. 2015. "Profiled: From Radio to Porn, British Spies Track Web Users' Online Identities." *The Intercept,* 25 September 2015. https://theintercept.com/2015/09/25/gchq-radio-porn-spies-track-web-users-online-identities/.

can disclose our pregnancy, our sexual orientation, our activist tendencies, our routines and movements -- whatever we might prefer to keep secret. Still more worrying, they are so often flawed doubles, fakes only barely resembling us, sometimes only due to a coincidence of names or minor facts, and yet still able to influence and interfere with our lives. As data is packaged, resold, shared, and subject to steadily more powerful analytical tools, they turn up in the strangest places. We met "at your house," says the cryptic pale man to Fred Madison in David Lynch's *Lost Highway.*[5] "As a matter of fact, I'm there right now," he adds as they talk at someone's party -- and has Madison call his own home to confirm, as the pale man stands there, and the call picks up: "I told you I was here." Your phantom double has your phone already; as a matter of fact, they're being generated by it right now, as it produces data about its physical location and its proximity to other phones. "Where thou art shall I be."

This is our ghost story, and we live it every day -- a new "doppelgänger boom" to echo the one Friedrich Kittler identifies at the time of *The Student of Prague,* as directors explored the uncanniness of the new medium.[6] But this is no unsettling fantasy of depersonalization and enigmatic selves: it is a concrete situation that can result in *de facto* discrimination, and in economic and political injustice. The provisional, mischievous solution Helen Nissenbaum and I propose in our book *Obfuscation* is to recognize this condition and vastly multiply the number of doubles -- reducing their value and reliability -- through the deliberate

---

[5] Lynch, David. 1997. *Lost Highway.* October Films.

[6] Kittler, Friedrich. 1999. *Gramophone, Film, Typewriter.* Stanford, CA: Stanford University Press. 155.

production of misleading, ambiguous, and confusing information.[7] Why not bury the signal in the noise?

The core of our proposal precedes digital technologies, but we assert that it is most relevant to them -- a kind of anticipatory atavism, a response that preceded its stimulus. In 2009, Helen was working with developers on the TrackMeNot project, a browser plugin that generated search queries it would make to Google (or another search engine of your choice), so the logs of your searches would not produce an accurate model of your interests, problems, and needs: did "halogen lamp" or "concussion symptoms" come from you or the plugin? I was looking at the early history of computing in the development of radar during World War II -- a story which involves chaff, pieces of foil dumped from planes to create "false echoes," signals that looked like planes on the radar and made coordinating anti-aircraft attacks much harder. As we talked, we realized these two examples, with different technologies, different goals and contexts, had a common shape: when you cannot escape observation, generate many additional signals -- give your adversary *more* of the information they're looking for, much more.

We found many other examples of this approach, from the deliberate overdisclosure of legal documents to the design of location-based phone services, from the operation of the anonymous communications tool Tor to the evolved defenses of the orb weaver spider. All, digital or analog, temporary or permanent, shared this pattern. Getting directions on your phone involves

---

[7] Brunton, Finn and Helen Nissenbaum. 2015. *Obfuscation: A User's Guide for Privacy and Protest.* Cambridge, MA: MIT Press.

disclosing your location and destination; catching insects in your web means being exposed to birds and wasps. Sometimes superior methods of concealment, refusal, or disappearance aren't available, and our best approach -- if we have some sense of what our adversary is looking for -- is to make a multiplicity of targets. The purpose couldn't be more different: the spider (which has evolved a strategy of making fake "spiders" on the web to distract predators) buys itself a few seconds to scramble away; the smartphone user, with an app that makes a variety of different directional requests and then extracts the relevant one client-side, gets the information they need while protecting their data from future misuse. Some obfuscation techniques work best with a crowd of users muddying the waters, and others with just a few obfuscators; some work best if they're known by the adversary to be in use, and others if they're kept secret; some work best fast, and others slow. All enact the allegorical question given by G.K. Chesterton: "Where does a wise man hide a leaf?" In the forest. What if there is no forest?" He grows a forest to hide it in -- obfuscation.

Growing this "forest" -- sending false search queries, generating alternate identities on social networks, flooding hashtags to dilute their utility -- is not just a defense of privacy, however. It can also be an act of protest: if our data is misused, transformed, manipulated without our consent, one response is to make the data worse -- whether indiscriminately, or in a careful and targeted fashion -- and we find examples of this from resistance to softly coercive social networks to strategies for beating police profiling and advertising market analysis. One of the most interesting technical developments in obfuscation is software

that can modify user data to be useful for only one purpose, to provide some kind of functionality which the user needs, without being adaptable to unwanted, unplanned purposes -- targeted advertising, discriminatory insurance pricing, or other unintended appropriations.

What we suggest, then, is to turn the logic that produces all our uncanny data-selves against itself. One reflection is a tormentor, and ten digital phantoms built of our data trap us in our own traces. But a thousand, diluted, wildly different, boring, ambiguously real reflections: they are a crowd into which we can disappear for the time being, becoming ghosts ourselves.