2

The Indefinite Archive

I know I am being watched; Edward Snowden told me so—although I cannot experience it for myself. This strange disjuncture spells out the problem: What does it mean to "know" technological systems that grow ever larger and more complex and yet are concealed from the human subject?

In April 2015, Snowden—having sought asylum in Russia—agreed to an interview with the comedian-cum-talk show host John Oliver.[1] Oliver had brought a dose of realism for the young idealist: Do you think the American people now possess the knowledge you have given them? Do they even know who you are? His clip showed a series of passersby at Times Square: "I've never heard of Edward Snowden," said one. "Well, he's, um, he sold some information to people," ventured another. The knowledge that Snowden had risked his life to impart seemed to have dispersed into the crowded streets—visible here and there but in piecemeal and confused forms. Oliver offered consolation in textbook deadpan: "On the plus side, you might be able to go home, 'cos it seems like no one knows who the fuck you are or what the fuck you do."

* * *

Timothy Morton writes that the Anthropocene presents humans with a proliferation of *hyperobjects*: things with such broad temporal and spatial reach that they exceed the phenomenological horizon of human subjects.[2] Images of endless (but equally fast-disappearing) ice sheets, floating garbage islands in the ocean, or statistical projections of planetary destruction, each evokes an uncanny sense of displacement: phenomena that seem to defy human scales of interpretation and yet demand that we reckon with them here and now. A variation of this question is posed by the Snowden affair. How can we "know about" technologies of datafication—the "we" being the amorphous yet enduring ideal of the public? Through Snowden's leaks, the public is called on

to know for itself, a duty that it has borne since the Enlightenment. Its slogan, *Sapere aude*, bestowed by none other than Immanuel Kant, calls for individuals to have the courage to use their own understanding—to think and know for themselves.[3]

Notably, Kant ended his text with the comment that such knowing achieves nothing less than "man, who is now *more than a machine*."[4] Although he meant something a little different by that phrase, these words resonate with the tension between the good liberal subject and the datafied body. The discourse of big data presents the two as complementary. Yet the Snowden affair also raises the problem of human knowability in the age of data overproduction. Even as Snowden delivers essential information to the public, the technological systems in question increasingly defy human comprehension, producing an unstable gap between what the public is expected to know to function as rational subjects and the limits of their phenomenological horizon. Genuine and rare as they are, Snowden's documents also needed to be fabricated into the status of public knowledge. I argue that this process exposes underlying contradictions between technologies of datafication and the liberal ideal of open and transparent information.

In the Snowden affair, these problems are expressed through sets of common binaries—secrecy and transparency, knowledge and ignorance—which are then regularly transgressed, diluted, and short-circuited. This ambivalence is embodied by the Snowden files: the voluminous cache of secret documents whose leakage sparked the affair. They serve as evidence but also as objects of mystery. They are credited with radical transparency but also generate speculation and uncertainty. They establish their status as irrefutable evidence by appealing to the aesthetics of quantification but also normalize a certain kind of paranoia. The files constitute what I describe in the next chapter as "recessive objects": things that promise to extend our knowability but thereby publicize the very uncertainty that threatens those claims to knowledge. Recessive objects materialize the precarious and arbitrary nature of the groundless ground, showing how the very effort to mobilize technology for truth requires putting uncertainties to work.

To trace the public life of the Snowden files is to examine the ways in which the public is called on to "know about" hyperobjective technological systems. This chapter focuses on the Snowden files and the

problem of knowing about state surveillance technologies. It forms a duet with chapter 3, which considers how the public and the state seek to "know through" these technologies the dangerous world of twenty-first-century terrorism. Together, they pose the question: How can the public know for itself the vast, expansive world out there—the world both of terrorism as unknown dangers and of surveillance itself as a pervasive technological system?

Data at Large

20 July, 2013. Journalists at *The Guardian* descended into their company basement, power drill and angle grinder in hand. Observed by two British state officials, they duly carried out the task at hand: the physical destruction of a laptop computer. The Apple MacBook Pro had contained top-secret files about American and British state surveillance activities, leaked to the left-leaning paper by Edward Snowden. Although the material had already been studied and reported on globally, the state insisted on this act of symbolic dismemberment.[5]

It is fair to assume that everybody present understood how parochial a ritual they were performing. As the laptop expired under a cloud of dust and debris, the Snowden files had already circulated to a global network of journalists and activists, including *The Guardian*'s own offices in the United States.[6] Distributed through mundane USB drives to a smattering of journalists a month prior, some of the files had already become the biggest news stories of the year.[7] Still, the ceremony was correct about one thing: the overriding importance of the files as material evidence. They detailed activities such as the bulk collection of telephone and email metadata from domestic populations at a massive scale and made available as searchable databases for human analysts. They spoke of vast subterranean operations under the noses of the American public, sometimes literally: one key pipeline involved the "tapping" of undersea data cables to harvest personal information on online activities. Over the next several months, journalists revealed that the National Security Agency (NSA) had spied on foreign diplomats and national leaders, that it had monitored players of online video games and even surveilled pornography consumption habits as blackmail fodder against "radicalizers." In a debate where critics of surveillance had been perennially marginalized as paranoid rabble-rousers, the files were credited as being the "first concrete piece of evidence exposing dragnet domestic surveillance."[8] William Binney, a former NSA employee who had told the public much the same things Snowden did with much less impact, thought that the material documents made the difference: he regretted that he did not take any himself, the "hard evidence [that] would have been invaluable."[9]

Yet the stream of revelations also provoked a great mystery: Just how many documents were there, how many secrets to be told? The exact size, scope, and location of the Snowden files captivated the American news media—as if getting it right would provide some handle on the knowledge on offer.[10] Not that anyone could figure out just how many documents even existed. Snowden himself never deigned to supply a number. In an interview with the German public broadcaster ARD, Glenn Greenwald claimed that he possessed a "full set" of nine to ten thousand top-secret documents;[11] a year later, he would appear on New Zealand television and speak of "hundreds of thousands" of documents.[12] Meanwhile, the US government also tossed numbers into the air. A Defense Intelligence Agency report to Congress claimed that Snowden took nine hundred thousand files from the Department of Defense alone, distinct from his haul from the NSA.[13] One of the most widely cited estimates claimed that Snowden "touched" 1.7 million files while contracted for NSA work in Hawaii[14]—a figure often misconstrued as documents *taken*.[15] The wider public, without any means to check for themselves, could only watch.

This seemingly trivial mystery around the numbers danced around a more crucial question: How can the files speak the truth about data-driven surveillance? How can the public know such complex, secret, vast technological systems? The files are a clandestine archive of documents, offered as a map of another secret archive of surveillance data. It is data about data, information about information, and, like Borges's infamous map of the empire, made to be as large as the physical empire itself, the files replicate the problems of scale and comprehension surrounding state surveillance systems. The rapid expansion of electronic surveillance systems after September 11 required a massive boost in the NSA's funding, and a corresponding boom in internal hires, new infrastructure, and outsourcing contracts to the private military-industrial arm of

the surveillance apparatus.[16] By 2010, the government itself lacked comprehensive and precise metrics for mapping its own surveillance apparatuses or estimating the overall costs of antiterrorism.[17] As if a parody of corporations "too big to fail," the landscape had become littered with big data too big to account for.

The Snowden files, then, were not self-evident forms of proof but a collective mobilization of belief in knowability relying on the *appearance* of numbers. Very much in Wittgenstein's tradition, Steven Jay Gould writes that "numbers suggest, constrain, and refute; they do not, by themselves, specify the content of scientific theories."[18] Distinct from the mathematical order that generates these numbers, their public appearance often produces an impression of calculability, a groundless ground we conventionally agree not to doubt. Quantification has long been a social technology.[19] Each presentation of numbers translates credibility across people and things, and more generally contributes to the evidentiary reputation of numbers as something to look for and seek assurance from. And once this trust is (slowly) won, the faith in quantification—that is, statistics and probability as a way of seeing the objective facts underlying every kind of situation—injects a mythological strand into what is advertised to be the triumph of cold, impersonal reason.[20]

This is not to fall back on a false consciousness argument, where modern subjects are tricked into believing in a sham objectivity. The seductiveness of numbers is an essential aspect of the public's ability to trust in numbers, and numbers' ability to stabilize social norms of factmaking. Popular "scientism"—the overblown faith that science alone produces absolutely certain truth about the world—has become a radicalization of the kind of trust that normal science asks of the lay public. In the same way, numbers and statistics often become ciphers for objective knowledge production presumed to be occurring backstage. Sheila Jasanoff retells the views of an American lawyer, who argued that the deluge of charts, tables, and figures in court cases risked becoming a strategy of *painting by numbers*: as judge and jury stare blankly into yet another mystifying graph, the totality of the numbers, their very inscrutability communicates a certain sense of objective authority.[21]

Evidence of a Secret

These affective and impressionistic uses of numbers do not merely stabilize dominant narratives. The vastness of the files, sketched with a numerical brush, also supports the flourishing of speculation: What is the information that we now "have" but still cannot access? What remains secret about that which is technically exposed, and what wider landscape of secrets does such exposure make visible? The files were so vast that even Snowden himself could not confirm if he had personally read all of the documents.[22] The gradual drip of new leaks (table 2.1) not only successfully kept the files in the news for months but also added up to a marathon of information ingestion that the public struggled to keep up with. Even in the first week of the leaks, a survey suggested that 50 percent of Americans followed the news on surveillance "not too closely" or "not at all closely."[23] Those who sought to read the files and know for themselves found a bewildering morass of information, often requiring a great deal of technical and institutional context to parse through terms, such as *selectors detasked*, or code names, such as Pinwale and Egotistical Giraffe.[24] These many mundane gaps between the promise of revelation and the messiness of information meant that the leaks served to generate speculation as much as it settled them.

Out in the public, the Snowden files had become an indefinite archive: credited as a source of transparency and public information but in practice as an amorphous stream of gradual revelations, whose elusiveness mirrored the secrecy of the very surveillance state it sought to expose. For Derrida, the archive is the desire for an origin, an origin-as-truth; its very form reflects the desire for an ultimately impossible dream of total containment and retrieval.[25] Evidence does not extinguish uncertainty but redirects it and refocuses it. It is only because the documents exist that the public can enter into speculation, indignation, skepticism—even if nobody can be quite sure of what is and is not in those documents: the halo of potential justifications and harms still to be uncovered, the bulk of the iceberg still submerged. In the world of supermassive databases and hyperobjective tech infrastructures, the archive fabricates a sense of knowability—not through acts of deliberate deception but by serving as a container of the desire for knowledge and control.[26] Whether the voluminous cache of the Snowden files or the

enthusiastically embraced proliferation of "big" databases, these enormous archives become mobilized as a mystical embodiment of the truth out there—and of the hope that all these secrets, all these complexities, could be ordered, bounded, and accounted for.

TABLE 2.1. Cryptome's table of Snowden files leaked by *The Guardian* alone in the first few months of the affair

Number	Date	Title	Pages
	The Guardian		276
	27 February 2014	GCHQ Optic Nerve	3
21	16 January 2014	SMS Text Messages Exploit	8
20	9 December 2013	Spying on Games	2
18	18 November 2013	DSD-3G	6
19	1 November 2013	PRISM SSO SSO1 Slide SSO2 Slide	13
18	4 October 2013	Types of IAT Tor	9
17	4 October 2013	Egotistical Giraffe	20
16	4 October 2013	Tor Stinks	23
15	11 September 2013	NSA-Israel Spy	5
14	5 September 2013	BULLRUN	6
13	5 September 2013	SIGINT Enabling	3
12	5 September 2013	NSA classification guide	3
11	31 July 2013	Xkeyscore	32
10	27 June 2013	DoJ Memo on NSA	16
9	27 June 2013	Stellar Wind	51
8	21 June 2013	FISA Certification	25
7	20 June 2013	Minimization Exhibit A	9
6	20 June 2013	Minimization Exhibit B	9
5	16 June 2013	GCHQ G-20 Spying	4
4	8 June 2013	Boundless Informant FAQ	3
3	8 June 2013	Boundless Informant Slides	4
2	7 June 2013	PPD-20	18
1	5 June 2013	Verizon	4

Source: Re-created by the author from "42 Years for Snowden Docs Release, Free All Now," Cryptome, February 10, 2016, http://cryptome.org/2013/11/snowden-tally.htm.

These basic contours of the affair identify a paradox that I call *recessive*. On one hand, the Snowden files materialize the unknown. It promises direct contact with the depths of state secrecy and technological complexity. The language of exposure, leaks, and shedding light expresses the familiar trope of knowledge as illumination; the materiality of the files provides veridical guarantee that they bring undistorted fact and information into the sunlight—the "best of disinfectants," as Louis Brandeis said. On the other hand, this rare artifact from a secret place, brought to the public as a beacon of transparency, now compels citizens to journey into that still-strange world out there.[27] Like the hyperobjective images of climate change, these files let us glimpse at the tip of the iceberg and, in doing so, make the still invisible iceberg an unavoidable topic of discussion. If the public previously generated its decisions and opinions by tacitly accepting the unknowability of state surveillance (for instance, by having no particular opinion of it or by dismissing any criticism as conspiracy theory), then the Snowden files compel reasonable citizens to speculate and extrapolate—not just because the files present new information but precisely because the files tell us there is so much we do not know and that this unknown must now be a matter of concern.[28]

This performative, incomplete, speculative relationship between the Snowden files and state surveillance systems spell out the asymmetries of visibility and knowability that characterize systems of datafication as public matters of concern. As chapter 5 shows, the NSA protested that there were good reasons for its surveillance systems to be so secret and inscrutable; a popular counterargument against Snowden's leaks was that disclosing these technologies would allow terrorists to better evade them and, indeed, that Snowden's actions had put lives of agents at risk. (In Britain, a senior Home Office official asserted that the leaker had "blood on his hands"—even as Downing Street, on the same story, put it on record that there was no evidence the leaks had harmed anyone.) In effect, the public is asked to invest their rights and beliefs in a system of knowledge production that requires ordinary individuals to be maximally exposed and the system itself to be maximally concealed. Such a situation pressurizes the relationship between knowledge and uncertainty. The ideal of the informed public is confronted with both surveillance's inherent need for secrecy and what Bernard Harcourt has called "phenom-

enal opacity"[29] and Frank Pasquale, the "one-way mirror":[30] the ways in which big data technologies become resistant to everyday, experiential grasp. The growing ubiquity of data-driven decision-making across not just intelligence agencies but also local law enforcement, and their interoperability across private systems, such as CCTVs in stores or cameras installed in individual homes, exponentially increase the distance[31] between individuals and their data. In this context, the traditional reliance on the virtuous cycle of transparent information for an empowered public begins to lose their bearings.

Connecting the Dots

> New tools have a way of breeding new abuses. Detailed logs of behaviours that I found tame—my Amazon purchases, my online comments . . . might someday be read in a hundred different ways by powers whose purposes I couldn't fathom now. They say you can quote the Bible to support almost any conceivable proposition, and I could only imagine the range of charges that selective looks at my data might render plausible.
>
> —Walter Kirn, "If You're Not Paranoid, You're Crazy," *The Atlantic* (2015)

November, 2015. With the Snowden leaks still fresh on the mind, *The Atlantic* magazine advised that paranoia is the new normal.[32] As humans promiscuously supply all manner of personal data to electronic networks,[33] the machines, in turn, communicate and triangulate ceaselessly in a wireless hum. Social networks know you have been to Alcoholics Anonymous, Google and Facebook know you have been visiting porn websites,[34] and state surveillance systems suck in an unknown proportion of your emails, your Skype calls, and your internet banking records. *The Atlantic* piece concluded that paranoia was no longer a disorder but a "mode of cognition with an impressive track record of prescience." (Three years later, the public would be told that many smart devices *do* listen in on their users while dormant—and that in some cases, human analysts access those recordings for product improvement purposes.[35])

To try to know secret surveillance systems is to learn to perceive a certain cohesiveness, to rescue some sense of certainty out of the muck, to be able to connect the dots. The early twentieth-century psychiatrist Klaus Conrad called it *apophenia*: the tendency to identify meaningful patterns in random data. He pegged it to the acute stage of schizophrenia. Daniel Paul Schreber, the mythological "origin figure" of modern schizophrenia, was indeed greatly concerned with a complete and systematic order of meaningful truths, describing an *Aufschreibesystem*, an automated writing system that might perfectly represent his thoughts.[36] Conrad's neologism, assembled out of the Greek ἀπό (away, apart from) and φάνειν (to show, reveal), shares with the much older paranoia (παρά [besides] + νόος [mind]), a clear pathologization of this desire for order and meaning. What does it mean, then, to say that paranoia has become normal, a sensible and prudent response to the exigencies of the world around us?

I would like to pursue this charge of normalized paranoia not from a psychiatric or psychopathological viewpoint but an epistemological one. In effect, *The Atlantic*'s conclusion amounts to a recommendation that we fabricate more actively and aggressively than before—and that such a shift in the norms of factmaking is necessary to cope with a data-driven society. To be sure, suspicions about government surveillance, and, more generally, a state's tendency to abuse its powers, has long been a public secret: something that is generally known (or assumed) but rarely becomes officially articulated.[37] What objects such as the Snowden files do is bring those subterranean ways of seeing out into the open of public discourse. It is not that millions of individuals will specifically feel that the government is out to get them. The change occurs not at the layer of subjective experience but in the normative structure of epistemological expectations. The files' appearance as veridical objects provokes a renewed focus on surveillance's secrets; the public is presented with an urgent necessity for constructing meaning even—or especially—in the presence of unknowns.

The recessiveness of datafication thus encourages the "ruthlessly hermeneutic logic"[38] of a paranoid subject—the intensification of that search for a grid of intelligibility that, in varying degrees and shapes, is a feature of any regime of knowledge. There is an apocryphal story that some conspiracy theorists were rather put out when the Snowden leaks

happened: now that their theories had been proved right, they would have to come up with some new ones! For a more concrete example, consider a post on Reddit's /r/conspiracy, a hangout for conspiracy peddlers (or, as the site itself puts it, "free thinkers"): "If it weren't for Edward Snowden conspiracy theories would still just be 'theories' . . . High five to the sane ones <3."[39] This slippage between conspiracy theories and "just theories" reflects the fragile social boundaries that demarcate what is and is not an acceptable way to fabricate explanations. To label undesirable, deviant, threatening modes of knowledge making "conspiratorial" is to engage in a "rhetoric of exclusion," where the very act of naming marks that discourse out as illegitimate.[40] One does not, after all, engage conspiracy theories seriously to refute their various claims but summarily dismisses them from being "possible candidates for truth."[41] "That's just crazy" is the mantra of foreclosure that refuses to enter into reasoned debate with the theory at hand. (The same way in which our parent had told the Wittgensteinian child, "Stop asking; just believe that this is a tree.") However, events such as Watergate or the Snowden affair push the pseudo-conspiratorial, semi-acknowledged truths about government surveillance into more respectable public discourse. Much maligned and yet widely circulated and entertained, conspiracy theories demonstrate the ways in which the candidacy to knowledge is strictly policed. At the same time, these disavowed rejects are constantly smuggled in to cope with looming uncertainties. Like paranoia as a structural, rather than a pathological, symptom, conspiracy theories reflect not an antimodern strain of irrationality in the system but a *useful* by-product of rational knowledge production.[42]

This shift in what sounds paranoid or appropriate is thus not restricted to card-carrying "free thinkers" but reprises what Richard Hofstadter called the paranoid style in American politics: a mainstream tradition of conspiratorial and indignant mode of expression that could be found in McCarthyist America of the 1950s or even the moral panic over the Illuminati in the late eighteenth century.[43] In particular, Hofstadter argues that the right-wing paranoia in his own time—the 1960s—is founded on a sense of presumptive dispossession: the idea that they have *already* lost the country to powerful and shadowy forces that control their every move. This postapocalyptic imagination provokes not only a militant reaction but a general sense of agency panic. Specific

fears about communist plots or omniscient machines supply the broader sentiment that the liberal ideals of individual autonomy and freedom are under siege.[44] Mainstream news media coverage of the Snowden affair was awash with conspiratorial language, especially among those critical of the whistle-blower. Speculations that Snowden was a Russian or Chinese double agent, or at least their gullible puppet, were fuelled by Keith Alexander and other high-ranking NSA officials.[45] One *Washington Post* piece suggested that Glenn Greenwald, Julian Assange, and others had conned the gullible Snowden into risking his life for the former's ambitions—at least, before the paper had to issue a series of corrections to dial it down.[46]

The Snowden files became generative of new theories, new speculations, projecting ever larger shadows behind the actual facts it revealed. What matters is not just the information these documents provide but a variant of what Tor Nørretranders calls exformation: the bits of a message that are "explicitly and knowingly discarded,"[47] the bits that the available information leaves unsaid and unproved but that now gain a social presence in a provisional and anticipatory form. A paranoid epistemology is thus an apophenic one: the trouble is not that meaning is secret, hidden, or lost but that it is too much and everywhere.[48] Yet to label such strategies irrational would be to reproduce the ideal notion that information should lead us to proof and certainty. Instead, we might look to what Tobin Siebers called the "Cold War effect": a generalized epistemological climate where paranoia and suspicion were seen not as delusions or pathologies but as virtues, and to be paranoid was not to be ill but to be in tune with contemporary reality.[49] Indeed, Cold War rhetoric was frequently reprised in a concealed form in Snowden-era paranoia.[50]

Merleau-Ponty understood that the "mad" experience their own madness as no error or illusion but a naturalized and intuitive access to truth. A schizophrenic experiences voices not as hallucinations superimposed over reality but something as genuine as the ground beneath our feet. (Thus, Merleau-Ponty describes a schizophrenic woman who believes two individuals with similar-looking faces *must* know each other: a connection that "normal" humans would dismiss as apophenia gone haywire, but for the woman, this is simply common sense.[51]) The point is that any given system for rendering the world around us into intelligible pieces requires some reliance on presumptions about the unknown—a

reliance that, to outsiders, appears arbitrary or nonsensical. It may be technically prudent to wait until all the facts are in hand, but in the case of a secretive surveillance program and the logic of preventive prediction, nobody will ever reach such a privileged position. The public, as much as politicians and counterterrorism officials, are increasingly asked to judge and act well in advance.

There were cautionary voices, encouraging the public to return to a more conservative range for crafting explanations out of available data. Some pointed out that the risk posed by terrorist attacks remained rather small compared to, say, gun shootings.[52] Others simply insisted that criticizing surveillance programs would require presuming too much corruption and impropriety on the NSA's part for it to be realistic: "fearing the NSA . . . requires you to believe that hundreds, if not thousands, of American employees in the organisation are in on a conspiracy."[53] The only reasonable solution would be to trust in the NSA because not trusting would require us to be, well, paranoid. These disputes reflect the contested recalibration of what counts as *reasonable*, of what might count as a conventionally acceptable performance of reason between paranoia and naivety. Here we are reminded of a basic lesson in machine learning around overfitting and underfitting. Simply put, analysts are instructed to avoid following the data too closely, resulting in a model that reflects the vagaries of the available data rather than the underlying phenomenon, or not closely enough, in which case the result fails to properly model the trends in the data. Whether a model is appropriately fit thus is a question of human judgment, a convention guided by circumstance as well as mathematics. Even as these technical practices were being challenged as full of error, uncertainty, and arbitrary judgment, the human debate around these technologies was facing a similar dilemma: What counts as a "reasonable" response to the asymmetric information environment of the Snowden affair?

It was a question with direct relevance to not only the public deliberation but also in institutionalized decisions around known and unknown—such as the courts. Snowden's first leaks in 2013, and the preceding leaks by *The New York Times* and *USA Today* in 2005–2006, precipitated a series of legal cases against government surveillance. In each of these, the most important issue turned out to be a basic question of available facts: What kind of harm is *known* to be caused by surveillance? Despite the new availability of Snowden's files, efforts to contest NSA surveillance at the judicial level struggled to gain standing due to the difficulty in constructing a definition of surveillance harm that is compatible with the existing legal conceptualization (in the United States) of harm as "concrete, particularised and actual."[54] In *ACLU v. NSA* (2007), the district court concurred that phone/internet data collection is both unconstitutional *and* counts as concrete, particularized, and factual harm; however, the Sixth Circuit Court of Appeals ruled that the injury claimed is "mere belief" of intercepted communications, and the lack of any "personal" harm, only a "possibility," denied them standing.[55] A similar reliance on a narrow definition of harm has also dogged efforts to sue technology companies for breaches of data privacy.[56] Such debates reflect a fundamental problem with public secrets: What must one "know" to bring the unknown to trial? What should and should not count as "known" in the face of such relentless uncertainty? The changing standards of reasonable extrapolation thus correspond directly to the legal and institutional scope for recognizing and addressing datafication's consequences—a problem we shall return to in chapter 5.

The Transparency Illusion

This entanglement of knowledge and uncertainty makes a parody of the contemporary enthusiasm for transparency. Transparency is axiomatic for whistle-blowers, and Snowden, too, framed his actions in this light.[57] More generally, the concept had grown in prominence over the preceding decades, empowered and idealized as a universal tonic for liberal democracy and the Enlightenment.[58] Since the 1990s, buzzwords bloomed by the dozen in the wake of enthusiasm about the transformative powers of internet communication technologies: e-government, e-transparency, e-democracy . . . as if digital technologies would finally eradicate ignorance and misinformation and furnish the optimal basis for the public's rational judgment.

Such mythologization of transparency as an unalloyed good and universal solution reflects two kinds of conflations about how knowledge works in the data-driven society. First, this idealized belief in transparency involves a "virtuous chain": the public is injected with information, which is linearly correlated with more rational deliberation, and,

in turn, the arrival at an "optimal" decision.[59] Like the aforementioned pyramid from data to wisdom, this consolidated, linear model equates transparency with a global good, sweeping away the long essential role that secrecy and opacity had played in Western statecraft.[60] We find here another instance of the fantasy of epistemic purity, one that stands blissfully ignorant of what politics *is*. As Latour quipped, asking politics to tell unvarnished facts without rhetorical trickery is like asking science to tell truth without peer review, without experiments—and, yes, without any mediation of its own![61] Second, and related, is the belief in transparency as an indispensable cog in the apparatus of liberal democracy. Kant's *Sapere aude!* here becomes a directive for stuffing each and every citizen with maximum information about issues of public import. Yet, as we have seen, there is no easy connection between the theoretical availability of information and its uptake as knowledge.[62] As with the Snowden files, the presentation of solid, reliable information can *increase* the public labor of speculation and inquiry until citizens simply cannot keep up.

What becomes clear is that transparency is not a binary opposite to secrecy, the purifying sunlight idealized by Louis Brandeis. It is instead part of a wider ecosystem of knowledge that allows the circulation of ideas and impressions across different types of truth—types that exhibit different gradations of openness and publicity. This system might involve formal and institutional moves, such as declassification of formerly secret documents. It also includes perceptual and social shifts in which a public secret becomes a matter of concern or a percolating suspicion becomes legitimized into a belief that citizens feel they may wear on their sleeves. Importantly, these practices are not arrayed in a linear scale of progressive visibility or informed public deliberation. Consider electronic state surveillance's pre-Snowden status as an open secret, in which the public suspects and even assumes it is happening, but an official game of denial just about maintains the technical status of secrecy. As one reading of Kant's secrecy suggests, "the veil always also unveils, or promises an unveiling, but that promise, and the prospect of finally seeing what is behind it, are also part of the veiling."[63] Although transparency presents itself as a necessary harbinger of truth, it does so precisely by idealizing a specific conflation of publicity, honesty, and innocence—and forgetting the myriad other ways in which claims to knowledge may be paired up with speculation, interpretation, and judgment.

The genre of media *exposure*—which also became the basic format for reportage in the Snowden affair—also adds its own patterns to the unveiling. It is not coincidental that, at least in the American case, transparency emerged as a universal virtue in tandem with the rising centrality of exposure in journalism.[64] Both the sensationalist tabloid exposé and the somber investigative report share this foundational assumption that there always remain more secrets to be uncovered, that each story, each leak, gives an approximation of the rest of the iceberg submerged beneath the visible. Likewise, the frenetic pattern of constant updates in new media platforms[65] cultivates the "public's persistent feeling that 'there is always something'" more behind the scenes.[66] After all, no exposure can ever claim to reveal the whole truth, nor can it guard that truth from the swarming multiplicity of interpretation. As such, this normalized expectation of exposure is met by a prevalence of cynicism (in Sloterdijk's sense[67]): the revelation invites not acceptance but further interrogation of the leaker and the leaked, generating an economy of speculation that feeds on each effort at transparency (or, for that matter, secrecy). Transparency's practical function, then, is a clearinghouse, a switchboard: a technique that redraws the local boundaries of what counts as speculation, what counts as "on the ground" facts, what may pass as consensually assumed truths. Brandeis's sunlight receives a McLuhanian correction: illumination is neither natural nor neutral but a technological medium.[68]

The relation between transparency's idyllic promise and its multifaceted practical function can be better understood when we remember the highly contingent—and recent—history of its emergence. As Michael Schudson has shown, today's ubiquitous celebration of transparency only took off in the United States during the mid-twentieth century. It did so not through a broad public demand to "know for itself" but through political shifts in relations of trust and communication across the branches of government and media industries, such as a more adversarial model of journalism and the rise of public advocacy groups.[69] Inaccurate accreditations—such as the belief that Thomas Jefferson called information the "currency of democracy" (it was, in fact, Ralph Nader)—bestow mythical origin stories to what is in reality a more pro-

fane and youthful idea. This recognition of transparency's historicity forces a new perception of its present form: not as a fundamental ideal for the fulfillment of deliberative democracy but as part of a specific generation of (imperfect) machinery for that deliberation. Fast-forwarded to the times of vast electronic surveillance systems and their subjection to digitally proliferating leakage, transparency constitutes not an external panacea to these problems but their companion in mediating what kind of veridical force is given unto that which we think we know.

The Burden of Knowing

If transparency is a switchboard for different ways of knowing, each marked by the kinds of decisions and interpretations they authorize, then we must inquire into the practical consequences of fetishizing transparency. What kinds of powers and responsibilities are given over to the public in an act of transparency? The Snowden affair is one example in the wider story where the Enlightenment injunction to "know for oneself" thrusts an impossible labor onto the internet-age citizen. In the context of liberal, representative democratic societies, transparency mobilizes the citizen anew with an old responsibility: not just to participate in politics in prescribed moments and ways (e.g., voting every four years) but also to become an unblinking eye poring over every aspect of government. The citizen has been recruited as a free auditor for the state. This is to be distinguished from earlier forms of citizen redress, such as petitions of grievances and injustices. The long Western history of petitions, from written pleas to the Roman emperor to the *cahiers de doléances* in eighteenth-century France, was not the normal duty of subjects but extraordinary actions—and the work of assessment and redress remained the task of the governing prince.[70] This case was also for the literary trope of the king who speaks with his subjects in disguise to hear their grievances, most famously Shakespeare's Henry V and James V of Scotland's legend as "King of the Commons."[71] Again, it remained the king who must listen, gather data, make his population legible, and reconfigure his apparatuses of government according to that knowledge. In the e-transparency paradigm, however, the government (or the whistle-blower) merely uploads, makes

"available"—a passive position, after which it is the public's responsibility to request, read, cross-reference, judge, and prosecute. The proof may be *in* the Snowden files, but the burden of proof is *on* the subject.

The problem is that much of the time, it is a burden that the members of the public cannot afford to or are reluctant to bear.[72] When another realm of online surveillance—corporate data mining—became scrutinized for invasions of privacy, one popular solution was to push for greater transparency on the part of online platforms. Predictably, the result was an even greater onslaught of privacy policies that many people do not want to read, do not have the time to read, and do not have the background knowledge to fully understand. As one study showed, it would cost 781 billion USD per annum in salary if Americans used their working hours to read the privacy policy of every website they visited.[73] Well intentioned as they may be, such measures risk drowning the citizen in pointless information. And so, the impossibility of fully taking up, or "owning," the burden of transparency produces a new chain of deferrals and delegations. Set against systems for the production, circulation, and resale of information that are too distributed, complex, and technologically backgrounded for human upkeep, the tacit ideal of the maximally informed subject summons an overbearing specter of guilt. Although maintaining a skeuomorphic appearance of a liberal public sphere, digital transparency becomes an extension of the entrepreneurial, individualized responsibility that we have sloganized as "neoliberal." Even as technology promises that information shall be free, citizens are asked to work for free to support these growing mechanisms of truth production. Here, transparency functions as a false dawn, or even a barrier, to becoming political.

What if we thought of the work of politics, the work of being informed, as a form of labor? In economic terms, transparency appears as a practice of outsourcing, of creating externalities: costs that are not counted by the producers directly but are passed onto the rest of society.[74] The fantasy of e-government relies on this standing reserve of public engagement that transparency shall mobilize for free. Indeed, such mobilization already occurs in the American tradition of citizen surveillance: from vigilante neighborhood watches to the use of social media by police to receive tip-offs, the state has long relied on ordi-

nary subjects' sense of autonomy and agency to supplement the work of government.[75] Closer to home, the subject of the data-driven society is already well trained in another kind of free labor—the work of staying connected to keep uploading photographs, to keep participating—that generates the economic surplus of platform capitalism.[76] In their capacity as citizens, those same subjects are enjoined to stay more informed about more things than ever—as a way not simply to empower the good liberal subject for the demands of a complex information society but also to defray its costs.

The moralization of transparency has pernicious effects on the ideal of the public that "knows for itself"—effects that recall the earlier warnings from writers such as Walter Lippmann. In a world where information encourages speculation as much as consensus, transparency is too often a Trojan horse, not a panacea. Again, there are uncanny parallels with what we have said of conspiracy theory. If the concept of conspiracy taints the information thus labeled and expels it from the normative realms of deliberation (even as it continues to circulate and communicate), the name "transparency" invokes the presumption that a full and equal distribution of information is possible and desirable. If the shining light of novelty blinded early internet-age optimists into believing that everyone really could become the public that knows and decides for themselves, then we are still struggling to clear the afterglow from our eyes. To know through deferred and simulated means, to agree tacitly to exclude certain doubts or uncertainties from debate, and even to operate within restricted information flows is to protect the possibility of consensus and shared grounding in a democratic society. The untrammeled pursuit of transparency opens each time a hermeneutical Pandora's box, even as it promises to illuminate and disinfect the black box of datafication.

Mary Douglas once suggested that "certainty is not a mood, or a feeling, it is an institution"; that is, "certainty is only possible because doubt is blocked institutionally."[77] In other words, it is the product of conventional norms that we learn to avoid the stigma of conspiracy, the abyss of paranoia, and exercise our public judgment on the basis of what may be officially admitted (and what is unofficially and tacitly understood). We learn not to question Wittgenstein's subject and to operate on the shared basis that what I say I know to be a tree is indeed a tree. The corollary is that uncertainty is not kept at bay by the sheer strength of our knowledge and reason but by the decisions we make on what to believe and how to believe. And when those decisions become challenged by changing conditions, such as the vast and backgrounded complexity of new technological systems, the rules governing those boundaries begin to shift. The moral question, then, is clear: What kinds of boundaries and tacit norms should we adopt in an age of excessive information, of ever more ubiquitous yet concealed technological systems, and of unparalleled speculation in the public domain?

* * *

In the winter of 1998, the philosopher Thomas Nagel published "Concealment and Exposure."[78] It asks: Should information always be analyzed, disseminated, acted on? In what cases can new information be distracting or inappropriate to the judgment at hand? Written amid the scandal over Bill Clinton's extramarital affairs and his attempted impeachment, the question applies far more broadly to the benefits and limits of transparency. Nagel understood that information is not always beneficial in the same way and that it can infect public discourse with a cacophony of the trivial, the irrelevant, and the half-true. He argued that the increasing pressures for transparency need to be balanced by a corresponding provision of tolerance and *nonacknowledgment*: to know something and to not speak of it, to not bring it into one's decision-making. Since Nagel wrote his piece, such balance has only broken down further. Whereas Clinton was almost removed from office over his adultery, Barack Obama, the next Democratic president, was subject to incessant accusations about his religious allegiances and even his birth certificate. The question of what *should* be relevant to a given judgment was overwhelmed by transparency's slogan that everything that can be scrutinized should be. The argument for nonacknowledgment exposes the unbalanced nature of transparency as a style of fabrication and its dangerous proximity to political cynicism.

Perhaps the most counterintuitive aspect of Nagel's argument is that we should use nonacknowledgment to exclude the kinds of information about which *we know the public cannot come into agreement.* "Leave people to their mutual incomprehension," Nagel advises: pick your battles or risk devolvement into interminable squabbles over each citizen's

allegiance on every kind of issue. His chosen example is the generic demand that citizens "stand up and be counted"—perhaps by reciting a patriotic slogan or by professing their support for multiculturalism. What was meant to be an ethical and reflexive move of disclaiming one's bias comes to support an indiscriminate demand for transparency. In the Snowden affair, this exhibitionist tendency demands that every actor plot themselves on a binary grid: hang on, before you say anything—which side are you on? Do you believe Edward Snowden a hero or a traitor? Which side are you on in this war between regimes of truth? He is a hero, said John Cassidy of *The New Yorker*, Shami Chakrabarti of *The Guardian*, and civil rights groups such as Amnesty International;[79] a traitor, argued Fred Fleitz at the conservative-leaning *National Review* and politicians such as then former vice president Dick Cheney.[80] Some, like Nate Fick writing for *The Washington Post*,[81] decided to sit on the fence and say a "little bit of both." Yet such insistence on disclosure lends itself to prejudiced readings of those actors' discourse. It reflects not the opposite of having good faith in other members of the public but the very *lack* of good faith. Ironically, this exhibitionism erodes a useful fiction central to the "virtuous chain" of transparency: the idea that the public will judge each argument in a fair and reasonable way, making proper use of available information to reach the optimal decision.

However, Nagel's analysis is blind in one important respect: it presumes that consensus is possible as long as codes of civility and nonacknowledgment invisibilize intractable differences. This blind spot is all too similar to the way the early Habermasian public sphere was often idealized as an open space for rational deliberation. Scholars such as Nancy Fraser have shown at length how such inclusivity and equality were often restricted to a small group of citizens—often white male bourgeoisie who read and wrote for each other. In this sense, nonacknowledgment risks reproducing the boundary policing work we have seen in the definition of conspiracy theories. Especially telling in this regard is Nagel's example of sexual thoughts. Woman D applies for an academic job in C's department, who is "transfixed by D's beautiful breasts." Yet C refrains the best he can from expressing his "admiration," and D accordingly refrains from voicing her disgust.[82] Here, nonacknowledgment hardly solves the problem. Even if we very generously interpret C's behavior as that of a polite fellow who does his best not to objectify D, the result is neither equitable nor desirable. Conventions such as civility and nonacknowledgment secure knowability precisely by sacrificing whatever does not fit. D's ability to contest her objectification is curtailed by norms of nonacknowledgment—especially because C, in his position of power, is likely to exert greater influence over what is or is not suitable for disagreement. Across counterterrorism operations and quantified analyses of individual bodies, we will continue to find these political and ethical implications of the shifting boundary between known and unknown, the sayable and the inadmissible.

In short, the idealization of transparency risks conflating exposure with truth and expression with honesty. In doing so, it encourages speculation of a promiscuous kind—one that erodes and overwrites existing norms for the boundaries of relevance and credibility. There is a telling parallel here between the exigencies of big data technologies and the challenges facing the public in a data-driven society. If the former involves enormous quantities of data processed by automated machines, leaving users struggling to figure out how to make sense of it all, the latter asks the public to "know for itself" despite being ill equipped to consume this information responsibly and effectively. The relation between the injunction to know, excessive information, and speculative uncertainty occurs not only in the public's effort to know *about* state surveillance systems but also in the state's efforts to know *through* those systems also. The next chapter turns to this latter side of the problem, understood through another kind of fabricated object: the figure of the "lone wolf" terrorist.

The Gap

In Agatha Christie's novels, we find a trope of revelation: when enough "secrets" (i.e., objective facts) have been accumulated, the illusions topple all at once to reveal a perfect picture of the crime. The pleasure of this revelation is itself an expression of our shared intuition that, back in real life, things rarely seem to work out so neatly. Sherlock Holmes, too, insisted on a progressive and ultimately conclusive process: "when you have eliminated the impossible whatever remains, *however improbable*, must be the truth."[83] Holmes's world, of course, is a conveniently finite and localized one. It is rare that the suspects do not wear every relevant

aspect of their psychology and history on their person for the discerning eye of the detective. But what happens when tens of thousands of government-employed analysts roam the four corners of the internet, from massive headquarters the size of a small city? (The NSA's Fort Meade is larger than Cambridge, Massachusetts, in land area.) What happens when the nature of data collection mechanisms is such that nobody, not even the collectors, knows whether your data will ever be seen by a human? The linear eradication of the secret is replaced by an open struggle of speculative hypotheses that must all admit their partiality and uncertainty, even as they bid publicly for our belief.

This entanglement of knowledge and uncertainty comes down to a *gap* between the document as evidentiary object and the "knowing" it is meant to produce. It defies the transmissional imagination that proving, verifying, and informing humans can work like a digital file transfer. This gap is at the level of neither metaphysics nor the content of individual experience but the embodied and social structures that any regime of knowledge depends on. Known and unknown, transparency and secrecy, turn out very rarely to manifest in such pure forms. The Snowden files, celebrated and feared in equal measure, were supposed to provide truly solid, material grounding, as solid as it gets short of catching an NSA agent nibbling at your Ethernet cable. But the documents end up bringing in the distant and black-boxed "out there" into public concern. What does it mean for an object to acquire the status of proof? What other proof must exist for this object to tell its truth, and what are the subterranean beliefs, objects, conventions, and rhetoric that prop up its veridical authority? The recessivity of data and technology, so fundamental to surveillance's project of knowing, undergirds these phenomena.

3

Recessive Objects

In *The Watchers*, the journalist Shane Harris tells the story of the "BAG":[1]

> [It] stood for something unexpected: Big Ass Graph. In the late 1990's the engineers and systems gurus at the NSA became enamoured of computerised graphs to display huge sets of information . . . The graph builders of the NSA wanted to turn raw data into visual knowledge.
>
> But if the BAG was a useful tool, it was also a demanding one. For the BAG to tell them things, the [terrorist] hunters had to fill it . . . the resulting analysis overwhelmed them. The BAG's very design, the way it compressed information into more manageable forms, actually diluted nuance . . . For [the BAG] to tell them things, they had to feed it. But the more they fed it, the less it actually told them.

The big-ass graph materializes the gap between the human subject and the world out there, parallel to the problem of public knowledge in the Snowden affair. Deep within the hyperobject that is the surveillance apparatus, its human agents struggle to come to grips with a hyperobject of their own: an increasingly unpredictable and distributed terrorist threat. Between at least 2006 and 2013, the agency's internal mail service distributed weekly columns from the "SIGINT [Signals Intelligence] Philosopher." They contained brief musings that suggested "data is not intelligence" or that analysts increasingly face "analysis paralysis" and "cognitive overflow."[2] Yet the massive expansion of data collection and storage continued, under the idea that if everything could be tracked about everybody, the hidden correlations to the most unpredictable threats could be disclosed. The database as archive thus reprises Borges's famous story of the Library of Babel: a place containing every book ever written, every book that it is *possible* to ever write.[3] Initially celebrated as a holy grail of knowledge, its denizens quickly find that they are stuck