

The New York Times

The Opinion Pages

The Stone January 26, 2014, 7:15 pm

The Age of 'Infopolitics'

By COLIN KOOPMAN

The Stone is a forum for contemporary philosophers and other thinkers on issues both timely and timeless.

Tags:

Identification Devices, Philosophy, Surveillance of Citizens by Government

We are in the midst of a flood of alarming revelations about information sweeps conducted by government agencies and private corporations concerning the activities and habits of ordinary Americans. After the initial alarm that accompanies every leak and news report, many of us retreat to the status quo, quieting ourselves with the thought that these new surveillance strategies are not all that sinister, especially if, as we like to say, we have nothing to hide.

One reason for our complacency is that we lack the intellectual framework to grasp the new kinds of political injustices characteristic of today's information society. Everyone understands what is wrong with a government's depriving its citizens of freedom of assembly or liberty of conscience. Everyone (or most everyone) understands the injustice of government-sanctioned racial profiling or policies that produce economic inequality along color lines. But though nearly all of us have a vague sense that something is wrong with the new regimes of data surveillance, it is difficult for us to specify exactly what is happening and why it raises serious concern, let alone what we might do about it.

Our confusion is a sign that we need a new way of thinking about our informational milieu. What we need is a concept of *infopolitics* that would help us

understand the increasingly dense ties between politics and information. Infopolitics encompasses not only traditional state surveillance and data surveillance, but also “data analytics” (the techniques that enable marketers at companies like Target to detect, for instance, if you are pregnant), digital rights movements (promoted by organizations like the Electronic Frontier Foundation), online-only crypto-currencies (like Bitcoin or Litecoin), algorithmic finance (like automated micro-trading) and digital property disputes (from peer-to-peer file sharing to property claims in the virtual world of Second Life). These are only the tip of an enormous iceberg that is drifting we know not where.

Surveying this iceberg is crucial because atop it sits a new kind of person: the informational person. Politically and culturally, we are increasingly defined through an array of information architectures: highly designed environments of data, like our social media profiles, into which we often have to squeeze ourselves. The same is true of identity documents like your passport and individualizing dossiers like your college transcripts. Such architectures capture, code, sort, fasten and analyze a dizzying number of details about us. Our minds are represented by psychological evaluations, education records, credit scores. Our bodies are characterized via medical dossiers, fitness and nutrition tracking regimens, airport security apparatuses. We have become what the privacy theorist Daniel Solove calls “digital persons.” As such we are subject to infopolitics (or what the philosopher Grégoire Chamayou calls “datapower,” the political theorist Davide Panagia “datapolitik” and the pioneering thinker Donna Haraway “informatics of domination”).

Today’s informational person is the culmination of developments stretching back to the late 19th century. It was in those decades that a number of early technologies of informational identity were first assembled. Fingerprinting was implemented in colonial India, then imported to Britain, then exported worldwide. Anthropometry — the measurement of persons to produce identifying records — was developed in France in order to identify recidivists. The registration of births, which has since become profoundly important for initiating identification claims, became standardized in many countries, with Massachusetts pioneering the way in the United States before a census initiative in 1900 led to national standardization. In the same era, bureaucrats visiting rural districts complained that they could not

identify individuals whose names changed from context to context, which led to initiatives to universalize standard names. Once fingerprints, biometrics, birth certificates and standardized names were operational, it became possible to implement an international passport system, a social security number and all other manner of paperwork that tells us who someone is. When all that paper ultimately went digital, the reams of data about us became radically more assessable and subject to manipulation, which has made us even more informational.

We like to think of ourselves as somehow apart from all this information. We are real — the information is merely *about* us. But what is it that is real? What would be left of you if someone took away all your numbers, cards, accounts, dossiers and other informational prostheses? Information is not just *about* you — it also *constitutes* who you are.

We understandably do not want to see ourselves as bits and bytes. But unless we begin conceptualizing ourselves in this way, we leave it to others to do it for us. Many government agencies and giant corporations are all too eager to continue the work of producing detailed data profiles of all of us. These profiles may be produced for varying purposes (targeting terrorists is not the same work as targeting consumers), but they all involve informational pictures of who we are — as well as who we can become. These agencies and corporations will continue producing new visions of you and me, and they will do so without our input if we remain stubbornly attached to antiquated conceptions of selfhood that keep us from admitting how informational we already are.

We need a concept of infopolitics precisely because we have become infopersons. What should we do about our Internet and phone patterns' being fastidiously harvested and stored away in remote databanks where they await inspection by future algorithms developed at the National Security Agency, Facebook, credit reporting firms like Experian and other new institutions of information and control that will come into existence in future decades? What bits of the informational you will fall under scrutiny? The political you? The sexual you? What next-generation McCarthyisms await your informational self? And will those excesses of oversight be found in some Senate subcommittee against which

we democratic citizens might hope to rise up in revolt — or will they lurk among algorithmic automatons that silently seal our fates in digital filing systems?

As soon as we learn to see ourselves and our politics as informational, we can begin to see the importance of surveillance reforms of the sort proposed by Senator Ron Wyden, Democrat of Oregon, as well as the wisdom implicit in the transgressions of “hacktivists” whose ethics call for anonymity and untraceability. Despite their decidedly different political sensibilities, what links together the likes of Senator Wyden and the international hacker network known as Anonymous is that they respect the severity of what is at stake in our information. They understand that information is a site for the call of justice today, alongside more quintessential battlefields like liberty of thought and equality of opportunity. Willingness to see ourselves as informational persons subject to informational powers could help us bring into view what will be required to protect the many individual rights and social ties now inhering in all those bits and bytes.

Colin Koopman is an assistant professor of philosophy at the University of Oregon, where he is also a resident scholar at the Wayne Morse Center for Law and Politics. He is the author of “Genealogy as Critique” and “Pragmatism as Transition,” and is at work on a book about infopolitics.

The Stone, _featured, Identification Devices, Philosophy, Surveillance of Citizens by Government