Want to Predict the Future of Surveillance? Ask Poor Communities.

VIRGINIA EUBANKS JANUARY 15, 2014

Marginalized groups are often governments' test subjects. Here are a few lessons we can learn from their experiences.

Since Edward Snowden started disclosing millions of classified NSA documents in June, terms like metadata, software backdoors, and cybervulnerability have appeared regularly in headlines and sound bites. Many Americans were astonished when these stories broke. In blogs, comment sections, and op-ed pages, they expressed disbelief and outrage.

But I wasn't surprised. A decade ago, I sat talking to a young mother on welfare about her experiences with technology. When our conversation turned to Electronic Benefit Transfer cards (EBT), Dorothy* said, "They're great. Except [Social Services] uses them as a tracking device." I must have looked shocked, because she explained that her caseworker routinely looked at her EBT purchase records. Poor women are the test subjects for surveillance technology, Dorothy told me ruefully, and you should pay attention to what happens to us. You're next.

Poor and working-class Americans already live in the surveillance future. The revelations that are so scandalous to the middle-class data profiling, PRISM, tapped cellphones–are old news to millions of low-income Americans, immigrants, and communities of color. To be smart about surveillance in the New Year, we must learn from the experiences of marginalized people in the U.S. and in developing countries the world over. Here are four lessons we might learn if we do.

Lesson #1: Surveillance is a civil rights issue.

Counterintuitive as it may seem, we are targeted for digital surveillance as groups and communities, not as individuals. Big Brother is watching *us*, not *you*. The NSA looks for what they call a "pattern of life," homing in on networks of people associated with a target. But networks of association are not random, and who we know online is affected by offline forms of residential, educational, and occupational segregation. This year, for example, UC San Diego sociologist Kevin Lewis **found** that online dating leads to fewer interracial connections, compared to offline ways of meeting. Pepper Miller has **reported** that sometimes, African Americans will temporarily block white Facebook friends so that they can have "open, honest discussions" about race with black friends. Because of the persistence of segregation in our offline and online lives, algorithms and search strings that filter big data looking for patterns, that begin as neutral code, nevertheless end up producing race, class, and gender-specific results.

Groups of "like" subjects are then targeted for different, and often unequal, forms of supervision, discipline and surveillance, with marginalized communities singled out for more aggressive scrutiny. Welfare recipients like Dorothy are more vulnerable to surveillance because they are members of a group that is seen as an appropriate target for intrusive programs. Persistent stereotypes of poor women, especially women of color, as inherently suspicious, fraudulent, and wasteful provide ideological support for invasive welfare programs that track their financial and social behavior. Immigrant communities are more likely to be the site of biometric data collection than native-born communities because they have less political power to resist it. As panicked as mainstream America is about the government collecting cellphone meta-data, imagine the hue and cry if police officers scanned the fingerprints of white, middle-class Americans on the street, as has happened to day laborers in Los Angeles, **according** to the Electronic Frontier Foundation.

Marginalized people are in the dubious position of being both on the cutting edge of surveillance, *and* stuck in its backwaters. Some forms of surveillance, like filmed police interrogations, are undoubtedly positive for poor and working-class communities and racial minorities. But marginalized people are subject to some of the most technologically sophisticated and comprehensive forms of scrutiny and observation in law enforcement, the welfare

system, and the low-wage workplace. They also endure higher levels of direct forms of surveillance, such as stop-and-frisk in New York City.

The practice of surveillance is both separate and unequal. Acknowledging this reality allows us to challenge mass surveillance based on the 14th Amendment, which provides for equal protection under the law, not just on the 4th Amendment, which protects citizens against unwarranted search and seizure. Surveillance should be seen as a collective issue, a civil rights issue, not just an invasion of privacy.

Lesson #2: To a hammer, everything looks like a nail.

We can intuit the shape of surveillance-to-come by keeping an eye on developing countries, as well as exploring its impacts on marginalized communities here in the United States. The most sweeping digital surveillance technologies are designed and tested in what could be called "low rights environments"—poor communities, repressive social programs, dictatorial regimes, and military and intelligence operations—where there are low expectations of political accountability and transparency. Drones that deliver Hellfire missiles, Long Range Acoustic Devices (LRADs) that send pain-inducing tones over long distances, and stun cuffs that deliver 80,000 volts to detainees via remote control allow users to avoid direct responsibility for the human suffering they cause.

Many of these technologies are first developed for the U.S. military to deploy in the global south, and later tested for civilian purposes on marginal communities in the United States. LRADs, for example, were developed by San Diego-based military contractor American Technology Corporation in response to the bombing of the USS Cole in Yemen in 2000, and then **famously used** to disburse G20 protestors in Pittsburgh in 2009. Technologies designed for the military carry expectations about the dangerousness of the public, and can be used over-aggressively in community policing and crowd control. To a technology designed for counter-terrorism, everyone looks like a bad guy.

Then there is the digital side of things. "Law enforcement agencies, intelligence agencies, and militaries invest in Trojans, bad software, malicious network attacks and other things that we normally associate with heavy criminality,"

says **Amelia Andersdotter**, member of the European Parliament and the Swedish Pirate Party, which is dedicated to reforming copyright and patent laws. “No one is obliged to inform users of security flaws or to fix vulnerabilities.” In fact, as the ***Guardian*** and ***The New York Times*** reported in September, the NSA spends $250 million a year to work with technology companies to make commercial software—including encryption software—more “exploitable.” Insecure by design, this software is passed on to business and the public sector.

A standard of design liability—already common for architects—might work to hold software producers accountable. Presently, we mandate penalties for vendors that fail to security test their software in the airline and shipping industries, but not in other crucial areas: healthcare, nuclear plants, electricity grids. Andersdotter suggests that design liability regulations could hold software companies liable for not disclosing security flaws, responsible for damages they cause, and obliged to help users fix problems. But this solution may pose more questions than it settles: Who will administer the standards if software vendors and national governments are already subverting data-security requirements? How much transparency is possible when data holdings are centralized by commercial entities like Google, or by state entities, as in Brazil’s proposed national data centers?

Lesson #3: Everyone resists surveillance, not just the bad guys.

Resistance to surveillance is as common as surveillance itself. “There is always a cross-section of the population working to trick the system,” explains John Gilliom, co-author of *SuperVision: An Introduction to the Surveillance*. “Whether it's a college kid getting a fake ID, or the middle class family hiding a little bit of cash income to lower its tax bill, or the food-stamp recipient hiding an extra roommate. We often call this fraud or cheating, but something this widespread is more than misbehavior. It is resistance.”

“Data is the new oil. Beyond collecting information, it also means gathering power,” argues Joana Varon Ferraz, researcher from the **Center of Technology and Society at Fundação Getúlio Vargas** in Rio de Janeiro, Brazil, “Every government has become dataholic.” Dataholic political and commercial systems foster defiance. We don’t necessarily

resist because we've done something wrong. We resist because surveillance is not just about privacy; it is about power, control, self-determination and autonomy.

If people remain concerned about the impact of surveillance on their lives they may voluntarily withdraw from the digital world. Gilliom suggests we might even see "a hipster social trend where disengagement becomes a form of cache." But digital disconnection can simply be an excuse for maintaining ignorance; many people don't have the option to disengage. For example, public assistance applicants must sign a personal information disclosure statement to permit social services to share their social security number, criminal history, personal, financial, medical and family information with other public agencies and private companies. Technically, you can refuse to sign and withhold your social security number. But if you do not sign, you cannot access food stamps, transportation vouchers, cash assistance, childcare, emergency housing assistance, and other basic necessities for survival, or even talk to a caseworker about available community resources.

There are alternatives to disengagement. Brazil and Germany introduced a **joint resolution** to the UN condemning the member countries of what is unofficially known as the Five Eyes Alliance—the U.S., U.K., New Zealand, Canada, and Australia—for massive electronic surveillance and infringement of human rights. The EU is developing a **General Data Protection Regulation** that would unify data protection under a single European law. The **BRICS cable**, a 21,000 mile, 12.8 Terabyte per second fiber system connecting Brazil, Russia, India, China, South Africa, and Miami—is creating an alternative data pipeline to lower the cost of communication among major economies of the global south and provide non-U.S. routes for world communications.

Answers to the dilemmas we face in the surveillance society are not likely to come fr ey or Washington. This year, the Obama administration was put in the position of defending the Nationa nistration's snooping while stumping for a **Consumer Privacy Bill of Rights** that boosts security ppers. It is still unclear how President Obama will respond to his Review Group on Intelligence and Communications Technologies' **report** calling to terminate the storage of bulk data collected under the Foreign Intelligence Surveillance Act.

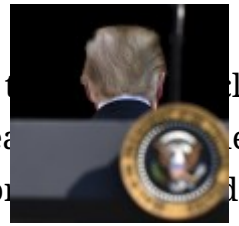
Lesson #4: Privacy is not the problem.

In his **Christmas Day address** on the U.K.'s Channel 4, Edward Snowden trotted out t[illegible]liches about George Orwell, Big Brother, and the end of privacy. But for most people, privacy is a pipedrea[illegible]ense urban neighborhoods, public housing, favellas, prisons, or subject to home visits by casewo[illegible]d working people might wish for more personal space, but they don't make Snowden's mistake of assuming that privacy is "what allows us to determine who we are and who we want to be."

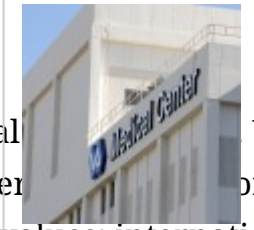
We need to move away our fixation on privacy and towards a future based on digital [illegible]. We can take some cues from Brazil, which is currently creating a collaborative, multi-stakeholder "Inter[illegible]on," the **Marco Civil da Internet**. The Marco connects digital communication to deeply held democratic values: internationalism, active citizenship, access to information, freedom of expression, democratic governance, civic participation, multilateralism, inclusivity and non-discrimination, plurality, cultural diversity, freedom of speech. The Marco also addresses network neutrality, personal data protection, and, yes, even privacy. But it is not the central issue. Seeing privacy as the cornerstone for democracy is a kind of naiveté we can no longer excuse nor afford.

We should care when national governments engage in surveillance of any kind, not just when they spy *on us*. Shock and outrage are callow luxuries, and the Snowden leaks eliminated our last justification for ignorance. Software designed for authoritarian political aims spawns repressive political environments wherever it is used. Systems tested in low rights environments will, as Dorothy informed me a decade ago, eventually be used on everyone.

* A pseudonym



while the country is being looted.



Memo to Next V.A. Chief: How Technology Allowed Corruption to Flourish, Hurting Veterans

VIRGINIA EUBANKS

President Obama has tapped Robert A. McDonald to run the embattled Department of Veterans Affairs. Here's what he'll need to understand about the limits of the V.A.'s vaunted electronic records program.

- The Weekly Prospect (Friday)

Sign Up