

Streetlights as Spyware

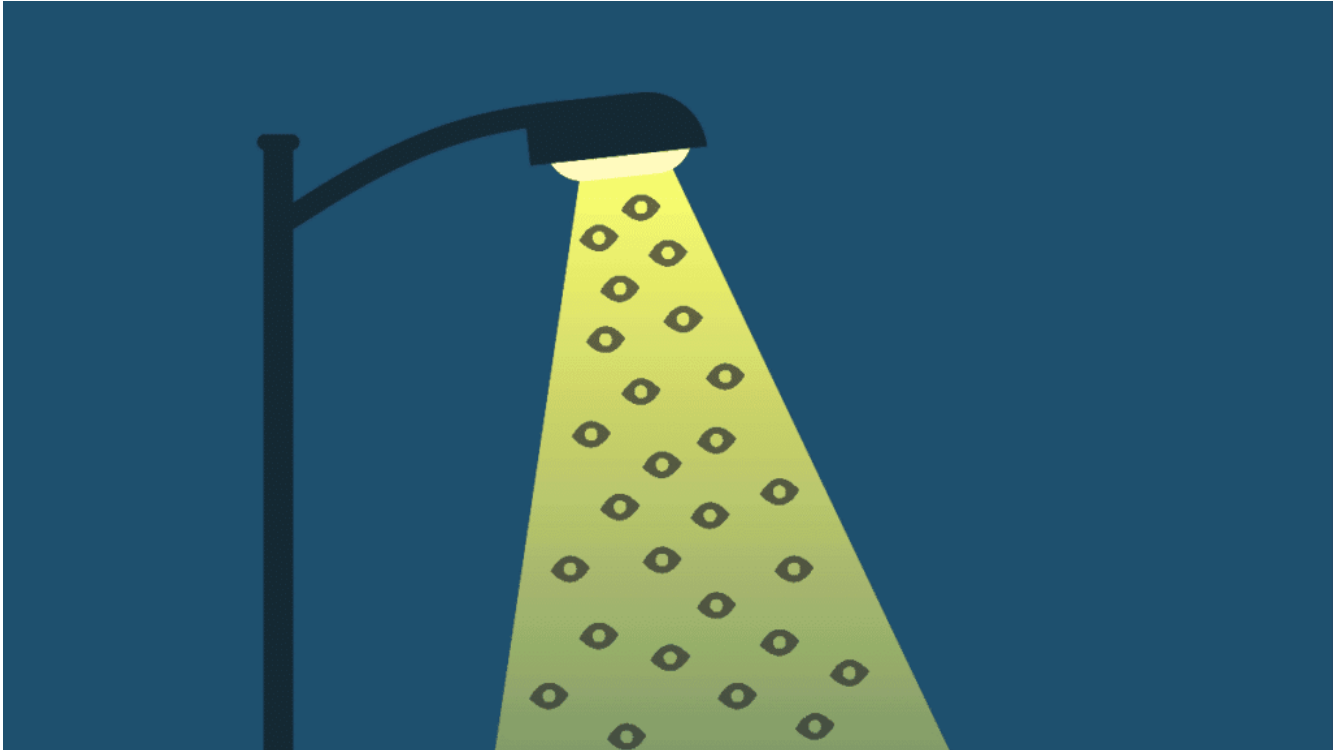
 techpolicy.press/streetlights-as-spyware

Michael Silberman

August 30, 2023

Aug 30, 2023

Smart street lights are fast becoming a trojan horse for pervasive government surveillance – unless activists intervene at key moments in local policymaking, .



Cities and towns across the United States have begun installing “smart” streetlights that promise public safety, environmental, and economic benefits while simultaneously laying the groundwork for a pervasive surveillance infrastructure. Smart streetlights put everyone’s civil liberties at risk, but they disproportionately impact the most vulnerable communities.

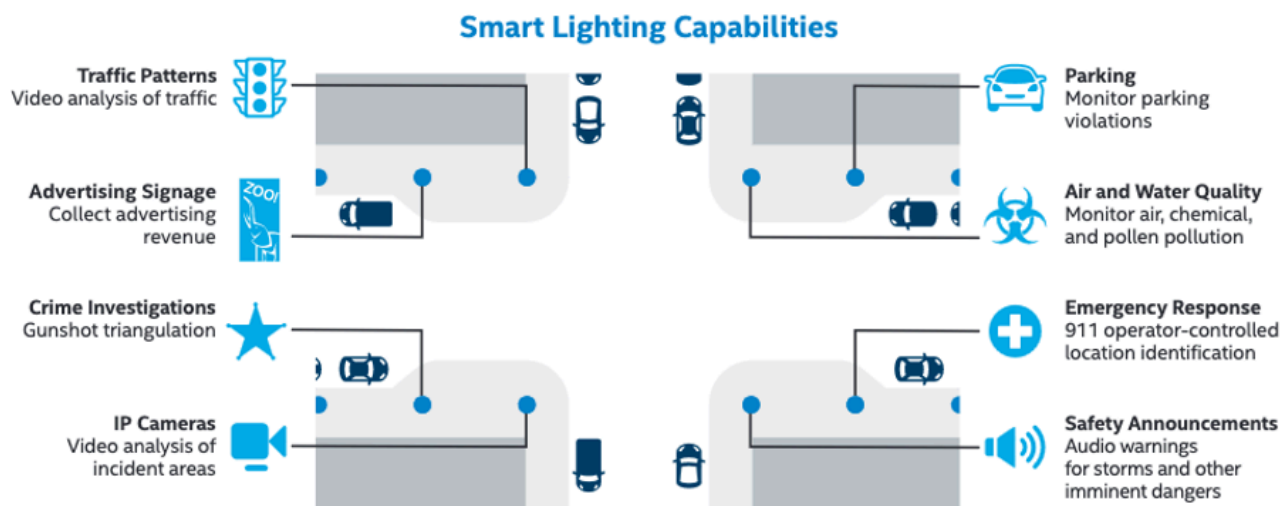
Unlike more obviously intrusive technologies, like the Transportation Security Administration’s (TSA) [facial recognition at major airports](#), smart streetlights have largely escaped public scrutiny as they quietly become permanent fixtures of the urban landscape. Local policymakers must begin addressing smart streetlights like police body cams – not as mere safety infrastructure. Residents and civic organizations will need to begin engaging in local permitting processes to ensure that smart street light projects include protections over the collection and use of data from streetlights *prior to* approving budgets and implementation plans.

Much more than LEDs

Smart streetlights have already arrived, even if they haven't turned heads or drawn much attention. They represent the backbone of burgeoning "smart city" programs in Chicago, Dallas, Atlanta, Philadelphia, Cleveland, and other cities. According to one industry report, smart streetlights will be the focus of [\\$8.2 billion in municipal spending](#) in under a decade.

For instance, in Washington DC, the Smart Street Lights project is part of a broader "Smart City Initiative" championed by Mayor Muriel Bowser. [According to the city](#), these technology initiatives "leverage intelligent city infrastructure, including connected devices, sensors, and data analytics, to improve quality of life for residents, enhance economic growth, and address city challenges." Last year, the District of Columbia [approved](#) a \$309 million public-private contract to convert the city's 75,000 streetlights to LEDs. The city says that bulb replacement will ultimately deliver an impressive 50% reduction in energy use and help cut the city's greenhouse gas emissions. The city claims additional [benefits](#) for residents, such as improved safety, reduced light pollution (through more focused, downward lighting), and improved "equity of service" stemming from the ability to monitor lights remotely rather than depending upon residents to report outages. Remote management is made possible by the "smart" components, or wireless connectivity installed with the new lights to not only provide remote light monitoring but also extend public wireless internet access coverage.

The following illustration from smart streetlight contractor [Intel](#) shows how smart street lights are marketed as synonymous with much more than lighting – from traffic control to crime detection:



Source: Intel "Solution Brief"

Civil liberties at risk

Potential benefits notwithstanding, Washington, DC appears to have avoided addressing the significant civil liberties risks associated with smart city technologies. Once the citywide network connectivity is implemented through the streetlights retrofit program, the city's ability to add video cameras, "shot spotter" gunshot detectors, license plate readers, and similar technologies becomes almost trivial, even if in its vendor [RFP](#) the *current* project scope "does not include the installation of sensors, cameras, or microphones."

Pervasive surveillance violates everyone's right to privacy and can easily impact fundamental freedoms of assembly and expression, but these technologies disproportionately impact people of color and already marginalized communities. Predictive policing capabilities, enabled by AI and facial recognition, [exacerbate racial profiling](#) and biased policing. "Installing these light bulbs makes your city a less safe city, especially if you happen to be poor or a person of color," an [ACLU attorney observed](#).

These technologies also enable existing biases in policing to take root and metastasize in more venues. While the D.C. government likely has various rationale for its geographic prioritization of the Smart Street Lights rollout, from a potential police surveillance perspective, it is notable that the city's first phase of streetlight replacement, slated to begin earlier this year, is focused entirely on the three [wards](#) with the highest population of Black or African American residents—Wards 5, 7, and 8.

Despite the disproportionately negative impacts of surveillance tech on communities of color, some policymakers suggest that smart city tech can help to mitigate inequities. In Dallas, city officials [argued](#) that installing AI-equipped cameras on street lights in a Southeast neighborhood suffering high crime rates helped to achieve the city's racial equity plan. As if to demonstrate the risks of this program to residents, the smart street lights program was paused earlier this year after sensitive information, including social security numbers, was stolen from the city's servers in a [ransomware](#) attack.

While extended public WiFi coverage and lower carbon emissions can help reduce inequities, they need not come at the cost of reduced privacy and increased risks to civil liberties.

The cakewalk from street lights to surveillance

Smart streetlights are increasingly establishing the backbone of citywide surveillance infrastructure in municipalities across the country. However, while public notice and consent processes are typically required for street light replacement, [most municipalities do not have laws](#) requiring that residents be notified if cities add cameras or other surveillance equipment.

The District of Columbia's [Data Policy](#), for example, does not require the city to solicit approvals before collecting and storing data for law enforcement or other purposes. To address this policy gap, the ACLU launched a [campaign](#) in 2016 encouraging cities and towns to “ensure that local residents ... are empowered to decide if and how surveillance technologies are used ... by maximizing the public’s influence over those decisions.”

Given the relative ease with which many cities can quietly layer invisible surveillance technologies atop smart street lights once they’re in place, public engagement (or resistance) is most critical in the earliest phases of streetlight replacement planning. Streetlight replacement typically triggers mandated public notice and comment processes that may not be required for the addition of surveillance technologies. Streetlight replacement also represents a more conspicuous change to a streetscape or neighborhood aesthetics and, therefore, may be more likely to trigger public engagement than the installation of seemingly innocuous cameras or sensors.

In Washington, D.C., a community engagement process was implemented through early 2021, including a public comment period, a public hearing, and six public meetings (2018-2019). The Mayor also appointed and selected a [Streetlight Advisory Panel](#) composed of community members to “discuss key issues of the project” with the DDOT through the first year of operation. According to public records, the panel appears to have met monthly for one year, from November 2018 through December 2019. Published minutes reveal a complete lack of discussion on the city’s broader “smart city” plans; meetings primarily focused on the new lighting. Only [one meeting](#) appears to have (inadvertently) touched on questions of surveillance technology. A member of the group asked what effect the new lights might have on policing technology, to which a Metropolitan Police Department Captain [noted](#) that license plate readers and fixed cameras work better under LEDs rather than traditional/existing lighting. It’s unclear what authority this advisory panel had over the project’s ultimate approval, but it appears to have been a missed opportunity for holding the city accountable to protecting civil liberties when surveillance technologies are likely to be added to the light posts without public notice or consent.

In the absence of meaningful challenges from the public, the private sector or municipalities have little reason to oppose smart street light programs or raise privacy concerns. Telecom providers and “Internet of Things” (IoT) contractors like GE, AT&T, Philips, and Cisco are financially motivated to secure contracts for building out smart city infrastructures. Cities hope to [earn revenue](#) from installing digital billboards on poles, leasing space to 5G providers, and selling the data generated by the streetlights. Cities can also generate revenue from fines issued by traffic cameras and earn support from new city services, such as parking spot availability programs.

Safer street lights that protect people's rights

Smart streetlight deployments need not *automatically* lead to unchecked privacy intrusions—even in the absence of comprehensive, federal privacy laws. In San Diego, residents and activists challenged the city's streetlight data collection program. San Diego police touted smart streetlights as a “game-changer” for finding suspects and criminals, but after reports showed that police used the surveillance cameras to track Black Lives Matter protesters and shared other data with neighboring cities and fusion centers, [residents balked](#).

[San Diego](#) has now joined other municipalities, including [Oakland](#), in developing and implementing policy guidelines that govern the city's use of surveillance data and facial recognition. Prior to the implementation of public policy in both cities, the police [wrote its own rules](#) governing the use of surveillance data from street poles.

Smart streetlights approved and deployed in a vacuum puts people's fundamental rights at risk. Residents can and must play an active role in defining how new technologies are deployed in their communities, especially when these technologies directly impact their privacy, safety, and freedoms of expression and association.

Through participatory planning processes that include diverse stakeholders, cities can achieve the environmental, public safety, and economic gains they need through smart city technologies without entirely compromising civil rights. Key policy [solutions](#) governing streetlight data collection include requiring city council approvals prior to adopting any new surveillance technologies, transparent reporting on the use of any new technologies, prohibiting nondisclosure agreements with surveillance-related vendors/companies, and establishing privacy commissions comprised of privacy experts, community members, and lawyers to evaluate and review new technology projects.

To increase participation in these critical policymaking processes, activists, artists, and creative communicators are needed to help make “invisible” smart streetlight privacy issues visible to others. And community organizers need resources and support from national civil rights groups and democracy funders to ensure that smart street lights are not just “smart” for governments but also protect the rights of residents and citizens.

Authors



[Michael Silberman](#)

Michael Silberman guides organizations through challenges at the intersection of technology and social justice. His graduate research at the Georgetown University Law Center focuses on the impacts of repressive technologies, such as digital surveillance and disinformation, on human rights, climate j...

Topics

Recent
