An Issue Brief on

Smart Cities

RESTORE the FOURTH

What are Smart Cities?

Back in 2017, General Electric wanted to test its newly-developed remote light dimmers. It offered the City of San Diego a 13-year loan of $30 million to install 3,000 "smart streetlights" equipped with their dimmers. The cost would be paid back through energy savings; the streetlights would generate environmental and transportation data that would guide decisions about traffic management and parking. But that's not all the "smart streetlights" did. The streetlights were also equipped with sensors that recorded "anonymized" video and audio. Local police could access this video and audio via the company Genetec, without a court order or warrant. During Black Lives Matter protests, police used this data to investigate and prosecute protesters; in all, they are known to have accessed this data in 175 criminal investigations. When news of this capability emerged in 2020, City Councilors claimed to have not been informed by the police that this was possible; whether Councilors were told at the time or not, there was no public process, and no attempt to write rules in advance for how the police could use these capabilities. Efforts are now underway to write such rules, and some councilors are calling for an end to the program.

This story calls into question the use of "smart streetlights," and our use of the term "smart cities" in general. Just because data is being generated, doesn't mean that it's the data the City wants, data is collected is under democratic control, or that the City has the internal expertise to interpret flawed or unavailable data that is collected. This technology worked to increase police surveillance, without meaningfully improving ordinary citizens' lives. "Smart cities" projects seem to carry a high risk of routing taxpayer dollars towards surveillance projects that elected officials and City employees may not fully understand, with little built-in accountability or measurable outcomes.

Unaccountable Funding Mechanisms

Cities often purchase smart cities technologies through public–private partnerships. The SafeCam program in New Orleans deployed 3,600 cameras throughout the city and made camera recordings available to the Real Time Crime Center (RTCC), which can activate the cameras and share recordings with law enforcement in response to a 911 dispatch. This system enables police access without a warrant. The cameras were paid for by the state-owned Ernest N. Morial Convention Center, local businesses who purchase cameras and data storage, and the The New Orleans Police and Justice Foundation. This private-funding mechanism prevents the New Orleans Independent Police Monitor, chartered by the city in 2009, from conducting oversight.

Smart Cities and Ransomware Attacks

The more digitized and integrated a technology is, the more likely it can serve as a point of vulnerability for a cyberattack on a municipality's systems as a whole. "Dumb" traffic lights or emergency alert systems are much harder to hack; but systematic outside pressures from private vendors, donors, and the police themselves, lead cities to make their systems more vulnerable at the same time as cities make them "smart." Cities do not generally have the internal expertise or budget to secure their systems from cyberattack. It doesn't take much imagination to consider what would happen if a city adopted smart traffic lights, failed to secure them properly, and then became the target of a ransomware attack that drained their coffers of vitally needed funds. Since companies protect both their technology and data acquired by these devices by requiring municipalities or agencies to adhere to Non-Disclosure Agreements, it's hard to tell how vulnerable cities already are, but a recent study from 76 cybersecurity experts from Berkeley's Center for Long-Term Cybersecurity identified emergency alert systems, street video surveillance, and "smart" traffic signals as being particularly vulnerable to cyberattack.

Learning from ShotSpotter

An early "smart city" technology that cities have frequently adopted showcases the limitations of such approaches. ShotSpotter, based in California, markets its gunfire-detecting microphone systems with remarkable, but uncorroborated, claims of accuracy and cost savings. They claim that rapidly identifying the location of gunfire allows a more rapid response by law enforcement, leading to more lives saved and to quicker identification and apprehension of

perpetrators. However, a recent study of ShotSpotter in St. Louis found that ShotSpotter "has little deterrent impact on gun-related violent crime in St. Louis" and "does not provide consistent reductions in police response time, nor aid substantially in producing actionable results." The company claims that ShotSpotter is 97 percent accurate. Yet, in May 2020, the MacArthur Justice Center analyzed ShotSpotter data and found that over a 21-month period, "89 percent of the alerts the technology generated in Chicago led to no evidence of a gun crime and 86 percent of the alerts led to no evidence a crime had been committed at all." Even more concerning are several recent cases where ShotSpotter has admitted to modifying audio files retroactively to make them consistent with police reports, leading to the dismissal of evidence. Any "smart city" sensor-based technology is susceptible to the same problems. Vendors exaggerate the utility of their product; police take an uncritically enthusiastic approach to new crime-solving technologies; city councilors feel deferential to police, and want city services to be more efficient; and the result is a steady ratchet of more intense surveillance on areas of the city already perceived as being "high-crime."

Surveillance ordinances, sometimes developed and recommended by Restore The Fourth, can help to ensure that cities make decisions on adopting such technologies thoughtfully and democratically. Municipalities can follow the lead of Oakland, CA, among other jurisdictions, and establish a municipal Privacy Commission which can report back to elected officials on the privacy implications of new technologies.

What does Restore the Fourth recommend?

Based on these sources, we recommend that the federal government take the following approaches to Smart City technologies:

1. The federal government should establish a statement of privacy principles that it wants municipalities to adhere to.
    a. Technology vendors, the federal government, and state and local government must make every effort to protect people's privacy. No data generated by Smart Cities should be available to law enforcement or intelligence services without a warrant from an independent judge, based on probable cause of a specified individual's involvement with an actual crime.
    b. All technology should be considered for its possible disparate impact upon Black, Indigenous, People of Color (BIPOC) and other minority communities, both with respect to utility and privacy, with the goal being equitable treatment.
    c. Technologies should also be evaluated for their vulnerability to cyberattack and the impact of any attack.
    d. All parties should be transparent about exactly what data they are collecting, for how long (since much of the funding is for pilot projects), who will have access to it, who has had access to it, data retention should be limited to the least time possible consistent with project evaluation. Data-sharing should be limited to what is necessary for the project to function and private partners should be barred from retaining, selling or otherwise sharing the data onwards with other third parties.
    e. If applicable, people should be allowed to review any data that is specific to them and if there is a mistake, have it corrected. The government should be required to correct the error within 120 days.
    f. Data collected for non-law enforcement purposes, such as utility data, should be explicitly barred from being shared with any law enforcement agencies.
    g. Contracts with vendors should not involve NDAs, because these limit municipalities' access to information about possible unintended data collection.
    h. Municipalities should carefully consider who will have ownership of the data because this impacts the ability to benefit from it for planning or for profit through sale of the data.
2. A cost benefit analysis should be undertaken for each technology under consideration, so that expensive technologies that have the potential to undermine privacy are not unnecessarily adopted, and to ensure that only collection of the type of data necessary for the project occurs.
3. Before funding, each project should be subject to

a "surveillance impact review" by a privacy review board, with representation from members of civil liberties and privacy organizations, as well as affected communities. This review would ensure that the exact purpose of the project is clearly defined, as are the technology involved, the data that will be collected, how long it will be retained, who will have access, and how data retention will be limited.

4. After the project has operated for its term, the privacy review board should be given a report documenting how the technology was used, including information on who had access to the data, for how long, and its impact upon the local communities. This report will ensure that any disparate impact will be noticed and that policy amendments necessary to better protect civil liberties or to achieve public safety goals are made before long term use of the technology is adopted.

What does Restore the Fourth advocate for smart city technology?

$500 million of the $1.2 trillion that the Senate has approved for upgrading American infrastructure would be allocated to the "Strengthening Mobility and Revolutionizing Transportation" initiative, to assess how data-gathering devices and new vehicles can improve "transportation efficiency and safety by reducing traffic, enhancing access to jobs and health care, lowering pollution, and incentivizing private sector investments." Representatives DelBene and Clark have proposed the Smart Cities and Communities Act to launch a coordinated effort by the entire federal government to support adoption of SCT. SCT can enable improvements in many fields, including adaptive illumination, traffic control, bicycle and pedestrian congestion, parking space procurement, pollution monitoring, Wi-Fi access, and rapid detection of gunshots and leaking pipes.

While SCT represents an opportunity to introduce cost savings and efficiencies, the privacy risks are significant. We believe that, as Congress allocates these funds, they should also require that these funds may only be allocated subject to the procedural requirements that already exist in municipalities that have adopted surveillance oversight ordinances, and that we outline above. Citizens need protection from the self-interested advocacy of companies that are interested only in selling a product, not in whether that product genuinely builds the mutually caring communities we need in order to thrive as human beings.