DAY ONE PROJECT

Investing in “Privacy-at-the-Sensor” Civic Technologies to Advance the Next Generation of American Infrastructure

David Mascareñas

September 2021

Summary

The National Science Foundation (NSF) and the Department of Energy (DOE) should invest in a cohort of civic technologies that advance the next generation of American infrastructure while prioritizing individual privacy protections.

Our nation's infrastructure is in urgent need of upkeep and replacement. The next generation of American infrastructure should be designed and built to be resilient, energy efficient, and integrate harmoniously with network communications, autonomous vehicles, and other "smart" systems. Emerging civic technologies — such as sensors, computers, and software that can support billing and payment, manage public resources, monitor integrity of structures, track traffic flows, and more — can improve the performance of future infrastructure and improve community livability.[1,2] However, the public often believes that civic technologies invade individual privacy and enrich tech companies. Public distrust has disrupted multiple civic-technology projects around the world.

The federal government should invest in a suite of research and development (R&D) activities to develop new, sensor-based civic technologies that inherently preserve privacy in a manner verifiable by citizens. The federal government should also invest in complementary activities to promote adoption and acceptance of such "privacy-at-the-sensor" technologies. Such activities could include setting standards for the privacy properties of civic technologies, establishing technology test beds, funding public grants to encourage adoption of privacy-preserving sensing technologies, and creating partnerships with external stakeholders interested in civic technologies.

Challenge and Opportunity

Civic technologies (e.g., autonomous vehicles, drones, robotics, augmented reality, 5G networks, smart traffic signals, the Internet of Things (IoT), and more) are rapidly and increasingly becoming common in American communities. These technologies — also known as "smart-city technologies — hold great potential to make our cities more livable, efficient, resilient, clean, and sustainable. But much of the American public is worried that these technologies have insufficient privacy protections. Failure to address privacy concerns has set back multiple civic-technology initiatives around the world. In San Diego, for instance, a citywide "smart lamp post" project was shut down due to concerns that the police department was using video captured by the lampposts in criminal investigations[3,4,5]. This project is additionally noteworthy in that

[1] Mandarano, Lynn, and Mahbubur Meenar. 2012. "Building Social Capital in the Digital Age of Civic Engagement." Journal of Planning Literature 123-135.
[2] Mccann, Laurenellen. 2015. BUT WHAT IS "CIVIC"? May 1. Accessed 06 21, 2021. https://civichall.org/civicist/what-is-civic/.
[3] Perry, Tekla S. 2018. "San Diego Installs Smart Streetlights to Monitor the Metropolis." IEEE Spectrum, Jan 01: https://spectrum.ieee.org/computing/it/san-diego-installs-smart-streetlights-to-monitor-the-metropolis.
[4] Perry, Tekla S. 2020. "Cops Tap Smart Streetlights Sparking Controversy and Legislation." IEEE Spectrum, Aug. 8: https://spectrum.ieee.org/view-from-the-valley/sensors/remote-sensing/cops-smart-street-lights.
[5] Figueroa, Teri. 2020. "Mayor orders San Diego's Smart Streetlights turned off until surveillance ordinance in place." The San Diego Union-Tribune, Sept. 9: https://www.sandiegouniontribune.com/news/public-safety/story/2020-09-09/mayor-orders-san-diegos-smart-streetlights-turned-off-until-surveillance-ordinance-in-place.

lamp post video cameras are still turned on despite the project shutdown[6]: In a striking example of poor civic-technology design, the cameras cannot be turned off without cutting power to the rest of the lamp post.

Addressing privacy concerns also helps drive user acceptance of civic technologies,[7] which in turn is critical to reaping civic-technology benefits.[8] But the technical aspects of privacy protection with respect to smart cities have unique challenges and features, including the following:

- Civic technologies depend on pervasive ecosystem of imagers, sensors, and computation in spaces frequently occupied by the public. Because individuals must access these public spaces in order to go about their daily business, they do not have the option to opt out of being observed by civic technologies.[9] It is therefore essential that robust security- and privacy-protecting measures be embedded within civic technologies at every step of their cradle-to-grave lifecycle.

- Smart-city initiatives often require the public sector to work with large, multinational corporations that aggressively pursue their own interests. Companies have incentives to collect citizen data indiscriminately for commercial purposes. Companies also have incentives to design smart-city technologies in ways that make it difficult for competing vendors to integrate alternative technologies into the smart-city ecosystem.

- Smart-city technologies can involve very complicated sensing and computing devices that require significant expertise to understand. Cities and municipalities generally do not have the resources to effectively represent the interests of their residents in the face of the socio-technical challenges associated with emerging smart cities.

Because of these challenges, and because smart-city technologies are still relatively new, there are not yet widely accepted provisions for privacy in the smart-city realm. Yet protocols for integrating privacy into civic technologies and technology deployments are still in their infancy.

The time is ripe for the federal government to take a more active stance on privacy in civic technologies. There is strong bipartisan interest in building the next generation of American civil infrastructure, and in using civic technologies to improve the performance and usability of this infrastructure. Multiple cities and states now have

[6] Marx, Jesse. 2020. "San Diego Can't Actually Turn Its Smart Streetlights Off." Voice of San Diego, Nov. 2: San Diego Can't Actually Turn Its Smart Streetlights Off.
[7] Cilliers, Liezel, and Stephen Flowerday. 2015. "Information Privacy Concerns in a Participatory Crowdsourcing Smart City Project." International Journal of Internet Technology and Secured Transactions 3 (3/4): 280-287.
[8] Dhungana, Deepak, Gerhard Engelbrecht, Josiane Xavier Parreira, Andreas Schuster, and Danilo Valerio. 2015. "Aspern smart ICT: Data analytics and privacy challenges in a smart city." 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT). Milan, Italy.
[9] Eckhoff, David, and Isabel Wagner. 2017. "Privacy in the Smart City – Applications, Technologies, Challenges and Solutions." IEEE Communications Surveys and Tutorials 20 (1): 489-516.

chief privacy/data officers,[10–12] and an ecosystem of non-governmental organizations (NGOs) concerned with smart-city privacy issues has emerged.[13–16] These entities can support federal efforts to promote responsible and privacy-protecting use of civic technologies. A wide variety of technological advances[17] in signal processing, statistics, machine learning, security research, and privacy research can inspire and enable verifiable privacy for civic innovation projects. The U.S. research ecosystem (including academic institutions, NGOs and Federally Funded Research and Development Centers (FFRDCs)) features a vibrant community of technologists and policy experts well equipped to tackle cross-cutting research challenges associated with privacy-preserving smart cities. Finally, investing in privacy-related aspects of civic technologies could help the United States realize global strategic interests. The COVID-19 pandemic accelerated adoption of civic technologies for surveillance in some countries (including China and Russia). In these countries, civic technologies don't just pose privacy threats; rather, they are being used to directly exert control over citizen actions. By supporting innovation around civic technologies with strong embedded protections against abuse, the United States can advance a more democratic and privacy-centric approach to civic technologies at the international level.

Plan of Action

The Biden Administration, working through key agencies such as the National Science Foundation and the Department of Energy, should fund a set of research and development projects to promote smart-city technologies, architectures, and protocols that are inherently privacy-preserving in a manner that is verifiable and trusted by the public. The sections below outline specific investments, accompanied by recommended investment levels, that the administration should consider.

Develop verifiable "privacy-at-the-sensor" technologies

Recommended investment: $100 million

The federal government should fund development of novel sensing technologies that are inherently privacy-preserving in a manner that is verifiable and trustable by the public. This new class of sensors should have capabilities and features such as the ability to (i) redact information the public considers sensitive before that information is recorded in a digital storage medium, (ii) only record when specified classes of objects are observed by the sensor, (iii) anonymize collected data at the sensor, (iv)

[10] SmartCitiesWorld news team. 2018. "NYC appoints chief privacy officer." April 6
[11] SlateTech. 2016. "Why Some States Are Hiring Chief Privacy Officers." Dec 22: https://statetechmagazine.com/article/2016/12/why-some-states-are-hiring-chief-privacy-officers.
[12] Solutions, Data-Smart City. 2020. Who Are America's City Chief Data Officers? Harvard Kennedy School. December 7. Accessed 5 19, 2021. https://datasmart.ash.harvard.edu/news/article/data-leadership-at-the-executive-level-761.
[13] n.d. Future of Privacy Forumn. Accessed May 19, 2021. https://fpf.org/.
[14] n.d. Civic Innovation Lab. Accessed May 19, 2021. https://civicinnovationlab.la/.
[15] n.d. OpenMined. Accessed May 19, 2021. https://www.openmined.org/.
[16] n.d. National League of Cities. Accessed June 23, 2021. https://www.nlc.org/.
[17] Including, for instance, advances in disentanglement, optical neural networks, smart contracts, compressive sensing, sparse/optimal sensor placement, information barriers, differential privacy, secure multi-party computation, zero-knowledge proofs, homomorphic encryption, physically unclonable functions, and federated machine learning.

only indicate the presence or absence of a specified class of objects, (v) intelligently focus and defocus, and (vi) incorporate noise, randomization, and permutation to protect privacy. The federal government should also fund development of techniques for removing subtle signals in civic-technology data that could be used to circumvent otherwise robust privacy measures.

Create frameworks for analyzing the privacy, security, and performance properties of civic technologies

Recommended investment: $100 million

When it comes to civic technologies, there can often be tradeoffs between privacy/security and performance. Consider the case of at-home fall detection for senior citizens living alone. It is desirable to have a tool for automatically detecting when a senior citizen has fallen in their home so that medical personal can be alerted to provide assistance. One way to approach this problem would be to equip the senior citizen's home with a network of cameras connected to a computer-vision system. Artificial intelligence in the system would then analyze video from the cameras, alerting medical personnel if it perceives a fall. Alternatively, the senior citizen's home could be equipped with a network of strain sensors that can detect deformations in the home's structure. If the senior fell, the structure of the home would experience a rapid, but subtle deformation that the strain sensors would detect. An artificial-intelligence system would then similarly alert medical personnel if needed. Intuitively, we might expect that the sensor-based system would be less sensitive than the camera-based system but also more privacy-protecting. There is a need to develop frameworks for analyzing the privacy, security, and performance properties of civic-innovation systems and objectively summarizing tradeoffs among these properties.

Conduct a study of public perception and privacy concerns surrounding civic technologies

Recommended investment: $75 million

Successful deployment of civic technologies will require deeper understanding of how the public perceives civic technologies, and of what types of civic technologies are most likely to receive quick public acceptance. The federal government should launch a large-scale study to answer these questions. The study should also explore the extent to which the public is willing to sacrifice some elements of privacy in exchange for progress on priorities such as affordable housing, job creation, and mobility. Knowledge gained from this study should be incorporated into models and simulation tools to inform policy decisions and to facilitate design, deployment, operation, and decommissioning of civic technologies.[18]

[18] Saba, Rosa. 2020. "What Toronto can learn from the 'smart city' that never materialized." Toronto Star, June 23: https://www.thestar.com/business/2020/06/23/what-toronto-can-learn-from-the-smart-city-that-never-materialized.html.

Establish national standards for privacy assessments of smart-city products and systems

Recommended investment: $50 million

The federal government should fund the National Institute of Standards and Technology (NIST) to develop standardized testing protocols, procedures, and standards for smart-city hardware and software. Specifically, NIST should develop:

- **Protocols for evaluating the ability of a civic technology to characterize sensitive biometric information.** Such information may be genuinely necessary for applications such as facial recognition. But the public has a right to know when, how, and how much of their information is being captured, and to be aware of the potential for privacy loss. Standardized protocols are needed to ensure accurate answers to these questions.

- **Privacy-preservation standards and best practices for civic technologies.** Standards should cover all aspects of a civic technology, including the sensors used to capture data in publicly accessible spaces to the communication networks, encryption programs, and computing/memory resources used to store, process, and communicate the data. Best practices should govern design decisions that both directly (e.g., through installation of sensors and imagers) and indirectly[19] affect public privacy. Best practices must address issues such as public expectation of privacy in a public right of way, managing access and use of data collected by civic technologies, the importance of avoiding proprietary lock-ins,[20] and design of contracts for installing, operating, maintaining, and decommissioning smart-city systems. In developing these standards and best practices, NIST should engage professional organizations whose scopes of competency include infrastructure, sensing, software development, embedded systems, intelligent systems, and civic innovation (e.g., the American Society of Civil Engineers, the Institute of Electrical and Electronics Engineers, the American Society of Mechanical Engineers, and the Association for Computing Machinery).

- **A standardized gradation of privacy levels for smart-city technologies.** For instance, technologies with a high privacy level might rely on sensors that can indicate the presence of a human but are not capable of uniquely identifying that human with more than a specified level of probability. Technologies with a moderate privacy level might be able to both detect the presence of a human and record certain features (e.g., hair color or eye color). Technologies with a low privacy level might be able to identify individuals. Assignment of privacy levels may need to factor in the capabilities of computational systems that process the data from a given technology in addition to the capabilities of the technology itself.

[19] Simon, Matt. 2021. "How Underground Fiber Optics Spy on Humans Moving Above." Wired, June 28: https://www.wired.com/story/how-underground-fiber-optics-spy-on-humans-moving-above/.
[20] Cloudflare, Inc. (n.d.). What is vendor lock-in? | Vendor lock-in and cloud computing.

Finally, NIST should work with the Federal Trade Commission to develop, communicate, and maintain procurement standards for smart-city technologies.

Develop frameworks for evaluating acceptable privacy levels and communicating potential privacy losses in public spaces

Recommended investment: $20 million

Using the NIST-developed standardized gradation of privacy levels referenced above, the federal government should promulgate frameworks for evaluating acceptable privacy levels in different public spaces. For example, the potential for privacy loss to the public should be much smaller in a publicly accessible park, library, or post office (places that individuals may need to access frequently and where there is little expectation of surveillance) than in the lobby of a federal building (a place that most individuals do not need to access frequently and where security concerns may trump some personal expectations of privacy). Frameworks are needed to evaluate and communicate the privacy level associated with a given space.

Clear and standardized signage is also needed to inform the public about the types of smart-city technologies in use at a particular location and to indicate when the privacy level associated with a given public space exceeds a yet-to-be determined threshold of privacy violation. Signage should indicate the nature of the potential privacy violation and potentially also the sensing and computing technologies being used.

Establish smart-city test beds

Recommended investment: $150 million

The federal government, in cooperation with civic authorities, NGOs, and academic institutions, should establish a network of test beds to evaluate the performance, privacy and safety issues, and public acceptance of civic technologies before they are deployed at scale. These test beds can also be used to determine how to structure public-private partnerships in ways that equitably balance needs and interests of all parties. Security properties of civic technologies should be studied in depth at these test beds. In recent years, critical infrastructure has been the subject of high-impact cyberattacks.[21] Smart-city test beds should be used for penetration testing and red-teaming activities to ensure that American infrastructure that incorporates civic technologies is safe and secure. Test beds should be operated in a transparent manner to gain and maintain public trust and should be flexibly designed to accommodate future civic technologies.

[21] WBTV Web Staff. 2021. "N.C. governor issues state of emergency after Colonial Pipeline cyber attack." WBTV, May 10: https://www.wbtv.com/2021/05/10/nc-governor-issues-state-emergency-after-colonial-pipeline-cyber-attack/.

Fund grants to encourage adoption and deployment of privacy-preserving civic technologies

Recommended investment: $200 million

These grants should support local governments in purchasing and deploying privacy-preserving civic technologies. The grant money should also be used to fund studies of public perception and trust of proposed civic innovation early in the conceptual phase of civic innovation projects. Funding for these studies should be contingent on open sharing of results. Grants should also be made available to cover costs of local government representatives attending workshops, conferences, and training sessions associated with security and privacy for civic innovation.

Host an annual workshop and foster a community of practice related to developing privacy-preserving smart cities

Recommended investment: $10 million

The Federal Trade Commission (FTC) should host an annual workshop focused on "Addressing Smart City Privacy Concerns." As part of this activity, the FTC should make travel grants available to appropriate researchers, community members, municipal representatives, and civic authorities who can contribute to and/or benefit from the workshop. The FTC should also partner with nonprofits and professional organizations with experience in civic innovation (such as National League of Cities, Metro Lab Network, Code for America, and the American Society for Civil Engineers) on building a community of practice around civic innovation that preserves privacy and is accepted and trusted by the public.

Conclusion

The rollout of civic technologies is increasing and will be further accelerated by the pandemic. Civic technologies have great potential for making our cities more livable, more efficient, and more productive. But if we as a nation do not address the privacy concerns associated with civic technologies, we risk turning our smart cities into surveillance states and technocracies unduly influenced by tech companies and their interests. By investing in techno-social research and development for privacy preservation in smart cities, the federal government can facilitate adoption and acceptance of smart-city technologies. Responsible use of these technologies will in turn increase the performance, economic competitiveness, livability, sustainability, and robustness of our cities and communities.

Frequently Asked Questions

1. How are the research and development (R&D) investments proposed in this memo distinct from existing R&D investments into security and privacy?

R&D related to civic technologies that inherently preserve privacy in a manner that is verifiable by the public and gains public trust is a subfield of the broad R&D areas of security and privacy. The most distinguishing characteristic of privacy and security R&D as it relates to civic technologies is that civic technologies are often deployed in public spaces that individuals must inhabit, with limited or no choice to opt out of being surveilled by those technologies. This sets the civic-technology space apart from other settings where security and privacy are important, such as participating in social media.

A wide range of technologies have been produced to strengthen security and privacy. These technologies include differential privacy, secure multi-party computation, encryption, secret sharing, private information retrieval, zero-knowledge proofs, random/compressed sampling, shuffling, authentication, information barriers, physically unclonable devices, homomorphic encryption, physically unclonable functions, and federated machine learning. However, applications of these technologies have been largely limited to data that has already been recorded in a digital form by a sensor. As soon as data is recorded in a digital form, that data can be copied, transmitted, and manipulated. Furthermore, the application of privacy-preserving solutions in software is not verifiable by the public and is hence unlikely to gain widespread public trust.

In recent years, those involved in weapons-treaty verification have shown that verifiable privacy preservation at the sensor is possible.[22,23] The weapons-treaty verification community has adapted technologies generated by the broader security and privacy field to the problem of enabling verifiable privacy-at-the-sensor for protecting sensitive technical information under adversarial conditions. Advances made by this community can in turn be adapted and more widely developed to address pressing challenges around privacy in civic innovation. Efforts to do so should be accompanied by development of frameworks for quantitatively assessing the privacy characteristics of civic technologies, studies to better understand the characteristics that make civic technologies trustable and acceptable to the public, and grants that accelerate awareness, adoption, and acceptance of civic technologies.

[22] J.Gilbert, Andrew, Brian W.Miller, Sean M.Robinson, Timothy A.White, William Karl Pitts, Kenneth D. Jarman, and Allen Seifert. 2017. "A single-pixel X-ray imager concept and its application to secure radiographic inspections." Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment 90-97.
[23] Philippe, Sébastien, Robert J. Goldston, Alexander Glaser, and Francesco d'Errico. 2016. "A physical zero-knowledge object-comparison system for nuclear warhead verification." Nature Communications (https://www.nature.com/articles/ncomms12890): 7.

2. What are some examples of "verifiable privacy-at-the-sensor"?

At-home fall detection, as explained in the body of the memo, is one example. In this example, privacy-at-the-sensor for a home equipped with cameras to detect and report falls could be achieved by installing "smart lenses" on the cameras that automatically blur faces optically before the light rays reach the image plane of the camera and are digitally recorded.

A second example, as mentioned above, is weapons-treaty verification. In the weapons-treaty verification problem, there is a need to verify an aspect of a system (for instance, verifying that treaty-controlled items have been rendered inoperative) without revealing technical information about that system.[24–27]. Similarly, sensors and computation for civic innovation must be able to sense and compute based on limited data associated with an individual without revealing any additional information about that individual. The weapon-treaty verification problem is also characterized by very tight coupling between technical and political considerations, similar to the coupling between civil-liberties and technological dimensions of preserving privacy in civic innovation. Lessons learned from the weapons-treaty verification problem can be applied to the problem of privacy preservation in civic technologies. The weapons-treaty verification community has particularly valuable experience building sensor systems that inherently preserve privacy even when adversarial actors are using the sensor system to observe the state of high-consequence weapon technology.

3. What are examples of civic innovations that experienced setbacks due to public perception that civic technologies were violating individual privacy?

Examples include:

- San Diego smart lamp post project. The City of San Diego was hailed as a leader in smart-city technology deployment when it installed 3,200 lamp posts across the city featuring cameras for reducing traffic congestion, improving parking, and helping with city planning[28–30]. Shortly after the lamp posts were installed, San Diego's police department realized the lamp posts could also aid criminal

[24] Philippe, Sébastien, Robert J. Goldston, Alexander Glaser, and Francesco d'Errico. 2016. "A physical zero-knowledge object-comparison system for nuclear warhead verification." Nature Communications (https://www.nature.com/articles/ncomms12890): 7.
[25] J.Gilbert, Andrew, Brian W.Miller, Sean M.Robinson, Timothy A.White, William Karl Pitts, Kenneth D. Jarman, and Allen Seifert. 2017. "A single-pixel X-ray imager concept and its application to secure radiographic inspections." Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment 90-97.
[26] Kemp, R. Scott, Areg Danagoulian, Ruaridh R. Macdonald, and Jayson R. Vavrek. 2016. "Physical cryptographic verification of nuclear warheads." Proceedings of the National Academy of Sciences of the United States of America 8618-8623.
[27] Jayson R. Vavrek, Brian S. Henderson, and Areg Danagoulian. 2018. "Experimental demonstration of an isotope-sensitive warhead verification technique using nuclear resonance fluorescence." Proceedings of the National Academy of the Sciences of the United States of America 4363-4368.
[28] Quain, John R. 2018. "How 3,000 streetlights turned San Diego into America's smartest city." digitalTrends, July 25: https://www.digitaltrends.com/cool-tech/how-3000-streetlights-turned-san-diego-into-americas-smartest-city/ .
[29] City of San Diego. n.d. Smart Streetlights Program. Accessed 11 16, 2020. https://www.sandiego.gov/sustainability/energy-and-water-efficiency/programs-projects/smart-city.
[30] Perry, Tekla S. 2018. "San Diego Installs Smart Streetlights to Monitor the Metropolis." IEEE Spectrum, Jan 01: https://spectrum.ieee.org/computing/it/san-diego-installs-smart-streetlights-to-monitor-the-metropolis.

investigations.[31] Privacy objected to this use. In the summer of 2020, it was discovered that the San Diego police department was using video captured by smart lamp posts to investigate protester activities.[32] Privacy advocates objected even more strongly to the lamp post data being used against protesters. The smart lamp post program is currently on hold until concerns associated with police use of the lamp posts are addressed.

- Toronto Quayside smart-city project. In this project, the urban innovation company Sidewalk Labs attempted to deploy a variety of civic technologies across the Toronto waterfront.[33] Privacy advocates labeled the project as a highly evolved version of "surveillance capitalism",[34,35] causing the project to be abandoned in spring 2020. Academics attributed the failure of the Quayside project to failure to proactively put in place proper governance and regulatory frameworks for use and management of collected data, as well as failure to consider the needs and concerns of Toronto's citizens from the beginning of the project[36].
- Hong Kong smart lamppost project. Smart lamp posts were installed across Kowloon Bay in Hong Kong to help with traffic management and to monitor air quality. During pro-democracy protests in summer 2019, the lamp posts were torn down by protesters who feared the data they collected was being used to spy on Hong Kong residents.[37]
- New York City robotic police dog deployment. In spring 2021, the New York Police Department (NYPD) deployed a robotic police dog on the streets of Brooklyn and Queens to help fight crime in places deemed too dangerous for human police officers.[38,39]. Early and severe backlash caused the NYPD to terminate its contract with the robot's manufacturer.[40]

[31] Perry, Tekla S. 2020. "Cops Tap Smart Streetlights Sparking Controversy and Legislation." IEEE Spectrum, Aug. 8: https://spectrum.ieee.org/view-from-the-valley/sensors/remote-sensing/cops-smart-street-lights.
[32] Marx, Jesse. 2020. "Police Used Smart Streetlight Footage to Investigate Protesters." Voice of San Diego, June 29: https://www.voiceofsandiego.org/topics/government/police-used-smart-streetlight-footage-to-investigate-protesters/.
[33] Vincent, Donovan. 2019. "Sidewalk Labs' urban data trust is 'problematic,' says Ontario privacy commissioner." The Star, Sept. 26: https://www.thestar.com/news/gta/2019/09/26/sidewalk-labs-urban-data-trust-is-problematic-says-ontario-privacy-commissioner.html.
[34] Cecco, Leyland. 2019. "'Surveillance capitalism': critic urges Toronto to abandon smart city project." The Guardian, June 6: https://www.theguardian.com/cities/2019/jun/06/toronto-smart-city-google-project-privacy-concerns.
[35] Zuboff, Shoshana. 2019. "Toronto is surveillance capitalism's new frontier." Toronto Life, Sept. 4: https://torontolife.com/city/toronto-is-surveillance-capitalisms-new-frontier/#:~:text=The%20city%20of%20Toronto%20now,for%20translation%20into%20behavioural%20data.
[36] Saba, Rosa. 2020. "What Toronto can learn from the 'smart city' that never materialized." Toronto Star, June 23: https://www.thestar.com/business/2020/06/23/what-toronto-can-learn-from-the-smart-city-that-never-materialized.html.
[37] Huaxia. 2019. "Spotlight: Rumors on smart lampposts easily refuted, but damages far-reachin." Xinhuanet, August 27: http://www.xinhuanet.com/english/2019-08/27/c_138342569.htm.
[38] Olla, Akin. 2021. "A dystopian robo-dog now patrols New York City. That's the last thing we need." The Guardian, March 2: https://www.theguardian.com/commentisfree/2021/mar/02/nypd-police-robodog-patrols.
[39] Amanda Woods. 2023. "Video shows NYPD's new robotic dog in action in the Bronx." New York Post, Feb 23: https://nypost.com/2021/02/23/video-shows-nypds-new-robotic-dog-in-action-in-the-bronx/?utm_medium=SocialFlow&utm_source=NYPTwitter&utm_campaign=SocialFlow.
[40] Tayeb, Zahra. 2021. "The NYPD has terminated its contract with the maker of a 'creepy' robot dog, following a fierce backlash over its use in policing." Business Insider, May 1: https://www.businessinsider.com/nypd-terminates-contract-boston-dynamic-creepy-robotic-dogs-2021-5.

4. Can you provide an example of potential language for an NSF/DOE technical call for proposals for civic technologies that inherently preserve privacy at the sensor, are verifiable by the public, and gain public trust/acceptance?

Language for such a call could draw from the following:

"Acceptance of civic technologies by the inhabitants of the cities they are meant to serve is increasingly becoming contingent on ensuring that the components, architectures, and uses of these technologies respect the privacy rights of said inhabitants. Realizing the benefits of smart cities requires concerted research into and development of smart-city technologies and protocols that are inherently privacy preserving, verifiable by the public, and publicly trusted and accepted. Development of smart-city technologies must consider political and sociological considerations as well as community needs and concerns. We seek the development of novel technologies, sensors, computation, protocols and architectures for smart-city technologies that are inherently privacy preserving. We are interested in proposals that leverage and build on technologies such as differential privacy, secure multi-party computation, information barriers, encryption, secret sharing, private information retrieval, zero-knowledge proofs, authentication, physically unclonable devices, homomorphic encryption, physically unclonable functions, privacy-at-the-sensor, compressive sensing, sparse/optimal sensor placement, federated machine learning, and quantum information theory. The scope of interest also includes research into the social, political, design and user acceptance/interfaces associated with privacy preserving civic technologies. Cross/multi/inter/trans-disciplinary proposals that coherently address the techno-social challenges associated with privacy-preserving civic technologies are encouraged."

About the Author

David Mascareñas has a background in the research and development of novel sensor nodes for monitoring structural health. During his doctoral work, David developed arguably the first application of rotorcraft for the structural-health monitoring/inspection problem. David is currently working on the development of low-power and imager-based distributed-sensor network technologies for monitoring structural health. As part of this work, David has become acutely aware of the security and privacy challenges surrounding use of video in smart cities. He is a strong advocate for smart-city technologies and protocols that respect individual privacy while simultaneously delivering important societal benefits.

About the Day One Project

The Day One Project is dedicated to democratizing the policymaking process by working with new and expert voices across the science and technology community, helping to develop actionable policies that can improve the lives of all Americans, and readying them for Day One of the next presidential term. For more about the Day One Project, visit **dayoneproject.org**.

The Day One Project offers a platform for ideas that represent a broad range of perspectives across S&T disciplines. The views and opinions expressed in this proposal are those of the author(s) and do not reflect the views and opinions of the Day One Project or its S&T Leadership Council.