SMART CITIES: FOURTH AMENDMENT

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

Fourth Amendment

Unreasonable Search & Seizure

Absent a lawful warrant, the government cannot perform searches or seizures in areas where a reasonable, objective person would expect to have privacy. There are exceptions to this rule, such when a search occurs in conjunction with a lawful arrest. What constitutes an unreasonable search and seizure has becoming increasingly difficult to define in the context of Big Data and smart cities, due to the advent of new technologies such as smart phones as well as the massive amounts of digital data generated and stored by individuals compared to past eras. Another difficulty arises from the expansion of surveillance technologies into the mass marketplace, since everyday consumers can now easily perform actions (for example, using a thermal imaging device) that courts have previously found to constitute unreasonable searches when performed by the government.

Third Party Doctrine

A person cannot have a reasonable expectation of privacy in information voluntarily given to a third party. In many cases, modern technology such as cell phones simply do not work without the automatic, mandatory sharing of certain information (such as location data) with third parties (such as cell phone service providers). Current Supreme Court doctrine indicates that information automatically shared in this fashion does not fall under the third party exception and individuals still maintain a reasonable expectation of privacy in such automatic data. This raises a host of unsolved questions for smart city technologies that involve decision making based on information automatically generated by individual city dwellers and passed on to third party systems, particularly for law enforcement.

Helpful case law

Katz v. United States, 389 U.S. 347 (1967). Fourth Amendment protections don't apply against governmental action unless a defendant can establish that they had a "reasonable expectation of privacy" in the place to be searched or items to be seized.

Kyllo v. United States, 533 U.S. 27 (2001). Government use of devices not available to the public, such as thermal imaging cameras, to perform surveillance that would otherwise require physical intrusion counts as a search and is unreasonable absent a warrant.

United States v. Jones, 565 U.S. 400 (2012). Fourth Amendment provided some protection for trespass onto personal property, and the vehicle was a "personal effect."

SMART CITIES: FOURTH AMENDMENT

Riley v. California, 573 U.S. 373 (2014). The warrantless search exception following an arrest exists for the purposes of protecting officer safety and preserving evidence, neither of which is at issue in the search of digital data.

Carpenter v. United States, 585 U.S. __ (2018). Tracking a person's movements and location through extensive cell-site records is far more intrusive than the precedents anticipated, and cell phone use requires the giving of information to a wireless carrier, making it involuntary. Third-party doctrine does not apply to cell-site location information.

Other helpful sources

Jeffrey Bellin, *Fourth Amendment Textualism*, 118 MICH. L. REV. 233 (2019), https://repository.law.umich.edu/mlr/vol118/iss2/3/. This article discusses how the sort of data at issue in *Carpenter* does not fit within a textualist interpretation of the Fourth Amendment and argues that *Carpenter* ought to have come out the opposite way.

Andrew G. Ferguson, *Personal Curtilage: Fourth Amendment Security in Public*, 55 WM. & MARY L. REV. 1283 (2014), https://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=3524&context=wmlr. This article discusses how Internet of Things devices dovetail with the concept of curtilage and how the information generated and contained within such devices should be protected within an individual's sphere of privacy.

Janine S. Miller & Jordan M. Blanke, *Smart Cities, Big Data, and the Resilience of Privacy*, 68 HASTINGS L.J. 309 (2016), https://repository.uchastings.edu/cgi/viewcontent.cgi?article=1007&context=hastings_law_journal. This article discusses threats to privacy brought on by smart cities and related technology, and how the doctrine and practice of privacy changes and adapts in the smart city context.

Dalmacio V. Posadas, Jr., *The Internet of Things: Abandoning the Third-Party Doctrine And Protecting Data Encryption*, 53 GONZ. L. REV. 89 (2017), https://gonzaga-university-law-review.scholasticahq.com/article/9714-the-internet-of-things-abandoning-the-third-party-doctrine-and-protecting-data-encryption. This article discusses the privacy concerns arising out of strict application of the third-party doctrine in modern, high-tech society.

SMART CITIES: FOURTEENTH AMENDMENT

"No state shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any state deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws."

Fourteenth Amendment

Equal Protection

The government cannot engage in disparate treatment against a person or class. Disparate treatment occurs when a person or group is treated unequally by the government based on a characteristic protected by statute or by the Constitution, such as race, sex, or religion. In order to successfully sue under equal protection, a person or class must demonstrate that the government has engaged in disparate treatment that has caused harm to that person or class. Notably, socioeconomic status is not considered a protected characteristic, even if there may be strong correlations between lower income levels and being a member of a protected group in certain cities or regions. In the context of smart cities and Big Data, the use of third party vendors is an important issue to be aware of, since third party contractors are not necessarily bound to abide by the Equal Protection clause even if they perform government-like duties or support. Additionally, various Big Data tools can inadvertently produce biased results that could lead to disparate treatment, even if there was no intent to reach that outcome.

Right to Political Participation

There is no affirmative right to participate or have your voice heard in political discourse in the Constitution. As a result, there is no safeguard in place to ensure that all relevant demographics are heard or considered by the government when enacting policy or taking actions. While this sort of under-inclusion likely does not run afoul of the Equal Protection clause, it can result in skewed perceptions. In the smart city and Big Data context, using new technologies to solicit feedback or carry out city services (for example, taking feedback through a smartphone app) can result in disproportionate underrepresentation of poorer or less tech-savvy residents who don't have access to those technologies.

Helpful case law

Harris v. Mcrae 448 U.S. 297 (1980). One of a number of Supreme Court cases standing for the proposition that socioeconomic status is not a protected class.

Watson v. Fort Worth Bank & Trust, 487 U.S. 977 (1988). A disparate-treatment plaintiff must prove "that the defendant had a discriminatory intent or motive" for taking a job-related action.

State v. Loomis, 881 N.W.2d 749 (Wis. 2016). An example of a case involving a Big Data tool whose automatic processes allegedly resulted in disparate treatment of an inmate.

Other helpful sources

Michael Saliternik, *Big Data and the Right to Political Participation*, 21 U. PA. J. CONST. L. 713 (2019), https://scholarship.law.upenn.edu/jcl/vol21/iss3/2/. This article discusses the lack of an affirmative right to political participation and proposes a reading of the Constitution that does make room for such a right.

Nicol Turner Lee, et al., *Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms*, BROOKINGS (May 22, 2019), https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/. This paper is a primer on the sort of biased results that can come out of Big Data tools and how they can be mitigated.