ALBANY LAW SCHOOL
GOVERNMENT LAW CENTER

WARREN M. ANDERSON LEGISLATIVE BREAKFAST SEMINAR SERIES

Surveillance Technology

Summary by Michele A. Monforte, GLC Publications Editor

The Government Law Center held the second of its 2020 Warren M. Anderson Legislative Breakfast programs on February 25th. The purpose of the program was to provide an overview of surveillance technology: what it is and how it manifests in our lives; the pros, cons, and tradeoffs; and how it can unequally affect the lives of minorities and the poor.

The audience heard views from three panelists, who are experts on the topic: **Robert Heverly**, Associate Professor of Law at Albany Law School, who teaches a class entitled "*The Legal, Ethical, and Operational Impacts of Unmanned Aviation Systems*"; **Ángel Díaz**, Counsel in the Liberty & National Security Program at the Brennan Center for Justice and the author of the report "*New York City Police Department Surveillance Technology*"*;* and **Virginia Eubanks**, Associate Professor at the Rockefeller College of Public Affairs and Policy and author of the book "*Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor.*" The program was moderated by Patrick K. Jordan '02, General Counsel to the Albany Port District Commission and a member of the Advisory Board of the Government Law Center at Albany Law School.

Heverly offered two definitions of surveillance from the *American Heritage Dictionary*: close observation of a person or group, especially one under suspicion, and the act of observing or the condition of being observed, as well as a terser definition from the *Concise Oxford American Dictionary*: observing and being observed.

Where is surveillance? Everywhere. Police cars have dashboard cameras, police officers have body cameras, we have cameras in our private residences and even on our doorbells to monitor who comes to our door in real time. Step into a supermarket and technology creates a record of our behaviors and provides information on our shopping patterns: when we enter, where we go, and how often we visit. Cell phone apps, software, and social media collect huge amounts of information about us. Our modern vehicles gather data. Tesla uses cameras and other sensors to log details about what the car encounters while driving—data used to make the car safer, but this data also includes information about the

driver. Uber collects data on riders; it knows, for example, when you leave and return to your residence and which businesses you prefer.

We leave breadcrumbs through web beacons and cookies that keep track of how we navigate through and process the content contained in a website. The information that is collected can be used to improve the site, but can also be used for future marketing purposes.

Why does it matter if we are being observed and some of our data is being captured? Technology is good, isn't it? It helps us solve problems and makes day-to-day life more convenient. We want technology to make the world safer, improve efficiency, give us more free time, and ensure better and faster medical diagnoses and treatment. We may love being able to tell our car where to go. And renewing our driver's license online is much less of a hassle than standing in line at the DMV. So, what is the downside and tradeoff?

Three principles of processing personal data should be kept in mind: awareness, transparency, and consent.

There is the secretive nature and extent of surveillance systems set up, for example, to monitor us in business establishments or to read our license-plate number. In these cases, you may not know you are being observed and data on you is being collected; you do not have an opportunity to opt in or opt out of these situations. They often are happening without a person's awareness.

Transparency relates to what happens to the information once it is captured. Institutions in the past kept information on index cards and in manila file folders—and they did not keep the information forever. Storage is boundless now. What data is being collected? What happens to your data? How long it is being stored? How is it being used? Who has access to it? What are the costs versus the benefits of your data being captured?

Consent, as a legal term, means a willingness in fact for conduct to occur, but we tell by how your actions appear. Online we are constantly clicking on terms of service, the legal agreements between a service provider and a person who wants to use that service. When we, for example, install a new app, we click and agree to abide by the terms of service for that app—most often without reading through the document. It would take too much time to read each one. In fact, it is estimated it would take 76 work days for a person to read all of the terms and conditions they agree to in a year.

Another concern is mission creep, or the broadening of an organization's original objectives. Law enforcement and policymakers may gather data for a legitimate purpose, but once a surveillance and data storage infrastructure has been put into place, it may be tempting to use the technology and the data for additional purposes and share it across entities. Public and private sectors may be in a position to share information. For example, law enforcement may turn to private-sector

databases to access personal information.

We have some policies intended to protect the personal data of citizens. For example, HIPAA (the federal The Health Insurance Portability and Accountability Act) has procedures in place to notify individuals if their information is impermissibly used or disclosed. The city of Syracuse has an ordinance limiting the use of drones by city officials to prevent the unlawful use of collected data. New York State's revenge porn law is intended to stop the malicious publication of an intimate image of a person without their consent. And federal wire-tapping statutes are meant to protect our personal data to some extent.

Díaz discussed the New York City Police Department's use of the Domain Awareness System, a vast network of cameras, software, sensors, databases, devices, and related infrastructure that provides information and analytics to law enforcement. The system includes cameras owned by the police department and private entities who share their information with the police. They collect huge amounts of data, including information about drivers from 500 license plate readers. They also have a series of databases, including one on gangs—made up almost entirely of people of color and including children as young as 13—that civil-rights groups see as police overreach based on lack of transparency about who is included and what criteria is used, and lack of a mechanism for contesting inclusion in the database.

We all want to feel safe in our homes and communities and we, therefore, accept having cameras and other devices we feel we need to keep us safe. We are also hierarchical and, thus, we often are comfortable stepping on the rights of others, in particular the rights of the poor and communities of color, to create this feeling of safety.

As mentioned earlier, surveillance can operate in secrecy without oversight or accountability. There are no protections prohibiting or regulating the use of facial-recognition technology in public settings, even though its accuracy is sometimes in doubt, it can produce racially biased results, and there is potential for the expansion of its use beyond its stated goals of facilitating the detection, prevention, or deterrence of crime. So, for example, the intention may be to stop serious crimes but use gets expanded to selectively enforce lower-level offenses, often unfairly targeting minority groups.

New York City's surveillance system was developed in partnership with Microsoft. It, therefore, is funding a private company's profits. Furthermore, as part of the partnership, the city receives 30 percent of the revenue of the company's sale of the surveillance system to other jurisdictions. Critics of the partnership are uneasy about the introduction of a profit motive into law enforcement.

There are major concerns about facial recognition technology, specifically about how accurate the technology is and if there are biases and misinformation in these technologies. The technology has

been proven in studies to be particularly unreliable at identifying people of color, especially women of color. The system is replete with bias and high rates of error. It can result in false positives, concluding two photos are the same person when they are not. There are also instances where it has been misused. Díaz cited a case where the New York Police Department captured a grainy photo of a suspect accused of stealing beer at a CVS. They thought the suspect looked like the actor Woody Harrelson, so they ran the actor's photo, rather than the suspect's photo, through their facial recognition software to make the arrest.

Eubanks tells three stories in her book, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. In her discussion, she focused on the impact of automated decision-making on a child abuse reporting program in Allegheny County, Pennsylvania. The County implemented the Allegheny Family Screening Tool, a statistical model used to predict which children might be victims of abuse.

The stakes were high, and Allegheny County implemented the technology for all the right reasons, including to improve accuracy and consistency. The system was designed by the Centre for Social Data Analytics at Auckland University of Technology in New Zealand. The process was very transparent and open. The agency was involved in the design. There is public accountability because it is controlled by a public agency.

When a call first comes in from someone reporting potential abuse, it is handled by an intake screener. The screener runs the information through the model which provides a score. The software screens for 131 predictive variables to decide which calls should be investigated. The tool compliments the screeners' decision making. Depending on the score, the screener may decide to open an investigation.

There is great potential in the data-driven technology used by social assistance programs such as this one, but technology does not affect everyone in society the same way. This screening tool focuses on variables seen in poor working-class families because the model is built upon data from various public programs used by that population. The data does not reflect the entire population; it focuses on people in poverty and oversamples this population even though child abuse also occurs in middle class and wealthy families. So even if everything is done for the right reasons, it may result in tools that make a group feel more vulnerable. In this case, the tool may also fail to detect child abuse in other socioeconomic populations.

Many of the concerns outlined earlier about police surveillance also exist here. The data is eternal. It never gets thrown away. Once a name is recorded in the child abuse registry, the process of expunging, or removing, it is extremely difficult. Once an individual is indicated for abuse on the registry, it affects that person's job possibilities—they are not able to work, for example, as a school

aide, daycare worker, bus driver, coach, or scout leader.

Another concern is leadership change. A community may trust the current official overseeing the program to handle the data correctly, but what happens when that official leaves office and a new administration comes in?

The family members who Eubanks interviewed experienced the tools as deeply dehumanizing, as if their future was being "flattened down" to this "flashing red score" determined by the screening tool. She encouraged the audience to look at the situation from the point of view of the people whose lives are impacted.