

**New York City Council Hearing
Committee on Justice System**

**Oversight
The Technology Gap between Public Defenders and DAs
January 29, 2020**

Testimony of Mayor's Office of Criminal Justice

Good Afternoon Chair Lancman and members of the Justice System Committee. My name is Jorge Camacho, Senior Counsel at the Mayor's Office of Criminal Justice (MOCJ), and I am accompanied by MOCJ Senior Counsel Scott Mathews-Novelli. On behalf of the Office, we thank you for the opportunity to testify today.

MOCJ advises the Mayor on criminal justice policy and is the Mayor's representative to the courts, district attorneys, defenders, and state criminal justice agencies, among others. MOCJ designs, deploys, and evaluates citywide strategies to increase safety, reduce unnecessary arrests and incarceration, improve fairness, and build the strong neighborhoods that ensure enduring public safety.

At your request, we appear before you today on the topic of technology used by the City's public defenders and district attorneys' offices.

We would like to begin by first expressing our support of the Council's efforts to explore this matter and the resources our criminal justice partners have to fulfill their important responsibilities. It is our hope to provide the City Council with the information we currently have to aid in its consideration of this topic.

One of MOCJ's most important functions is to coordinate with our criminal justice partners, including the City's indigent defense providers and district attorneys' offices, to evaluate and meet their institutional needs. Some developing needs may be met through redeployment or utilization of existing resources. Additionally, defense providers may identify areas where they believe additional funding would be beneficial. Regardless, MOCJ has long strived to be responsive to our criminal justice partners and their needs, and we will continue to be so.

To best understand the resource interests our partners may have, MOCJ relies on a number of pathways for soliciting and receiving their input. First, MOCJ regularly hosts

various task forces and committees dedicated to particular areas, like Criminal Justice Reform Implementation, Raise the Age Implementation, and addressing domestic violence, among others.

The district attorneys' offices and the City's defense providers are consistently invited to participate in these groups, and we provide opportunities to each participating organization to offer their insights, present their challenges, and provide their proposed solutions to those challenges. These groups have been productive in addressing the challenges raised by participants, and we believe we have been responsive to requests for assistance and additional resources that have been made through them. For example, we recently asked members of the Criminal Justice Reform Implementation Task Force, including defenders and district attorneys' offices, to identify the resources they believed would be needed to facilitate their compliance with and implementation of state criminal justice reforms that were enacted last year and that went into effect on January 1st of this year. We then assisted them with their requests, resulting in a substantial allocation of new resources to them.

In addition to these task force and committee meetings, we maintain a continuous and direct line of communication with each of the district attorneys' offices and defense providers on a range of issues and for a number of purposes, including policy coordination, information-sharing, and troubleshooting of problems that may arise. This regular communication provides our partners with another channel through which they are welcome to share any resource requests that they would like for us to consider. Again, we believe we have been able to meet many of our partners' needs through these channels.

We understand that a conversation relating to technology issues involving the district attorneys' offices and defense providers is a complicated and highly technical one and that the issues that might arise merit careful consideration. It is important to note the immense promise of criminal justice reform to address at least some potential issues. For example, discovery reform has provided all parties with a clear timetable for the disclosure of key evidence, including technological data that, before the reform, may not have been disclosed prior to a case's disposition. The new discovery process may thus help address some of concerns about which technological resources were utilized by law enforcement in the investigation and prosecution of a case, permitting defense attorneys to better evaluate the merits of a case at an earlier point than was previously

typical. Accordingly, when this new process reaches maturity, it will be clearer whether issues might require additional attention and solutions.

We support the efforts recently undertaken by all of our partners to contribute to the fairness and equity of the criminal justice process, and we look forward to continuing our work with them in service of those ends. Should any of them advise us of any particular concerns they may have about technological resources, we would welcome that conversation with them.

We thank the Council for its attention to these issues and for the opportunity to engage with you further today, and we are happy to address any questions you may have for us.

THE LEGAL AID SOCIETY

Justice in Every Borough.

TESTIMONY

The Council of the City of New York
Committee on Justice System

Oversight: The Technology Gap between Public Defenders and
DAs (T2020-5624)

The Legal Aid Society
Criminal Defense Practice
49 Thomas Street
New York, NY 10013
By: Jerome D. Greco
(212) 298-3075
JGreco@legal-aid.org

January 29, 2020

Good afternoon. I am Jerome Greco, the Supervising Attorney for the Legal Aid Society's Digital Forensics Unit, a specialized unit providing support for digital evidence and electronic surveillance issues for the Legal Aid Society's attorneys and investigators, in all five boroughs. I thank this Committee for the opportunity to provide testimony on the technology gap between the public defenders' offices and the district attorneys' offices.

I. ORGANIZATIONAL INFORMATION

Since 1876, The Legal Aid Society has provided free legal services to New York City residents who are unable to afford private counsel. Annually, through our criminal, civil and juvenile offices, our staff handles about 300,000 cases for low-income families and individuals. By contract with the City, the Society serves as the primary defender of indigent people prosecuted in the State court system.

II. DIGITAL FORENSICS AND DNA UNITS

In 2013, the Legal Aid Society created the Digital Forensics and DNA Units to serve and support Legal Aid attorneys and investigators in our criminal defense offices. At that time, the Digital Forensics Unit had four analysts and no attorneys in one location with minimal equipment. Currently, the Unit has two digital forensics facilities, three analysts, two examiners, three staff attorneys, and one supervising attorney, with additional hiring anticipated in the upcoming year. Members of the Unit are trained in various forms of digital forensics including cell phone extractions, hard drive images, and cloud storage analysis.

The DNA Unit is comprised of ten attorneys and support staff. The Unit is nationally recognized for its expertise and its annual two-day conference, Questioning Forensics. They have

also been at the forefront of challenging the use of black box¹ algorithms in the criminal justice system.

The founding of these Units was an acknowledgment of the increasing use of science and technology in cases, hearings, and trials. The prosecutors were better staffed and better equipped with tools at their fingertips and experts in their offices. The Legal Aid Society saw a rising need for our own tools and experts to counter law enforcement, in an attempt to tip the scales of justice closer to their intended balance.

III. NATIONWIDE TREND IN THE CHANGE OF PUBLIC DEFENSE

A. The Increase in Science and Technology in Criminal Cases

Since our Digital Forensics Unit was featured in a New York Times article about the technology gap between prosecutors and defense attorneys,² I have received phone calls and emails from approximately twenty different public defender offices from around the country. Many of the offices want to create similar units to ours and some of the offices had already been working towards that goal. All of them recognized the importance and value in having such tools and expertise in-house. We have been advising them as best we can on the tools they need with the limited budgets they have or, in other cases, ways to explain to their officials the importance of acquiring the necessary products and hiring of skilled employees.

As technology becomes more deeply embedded into people's daily lives,³ its use and importance in courtrooms grows exponentially. This is especially true in the context of criminal

¹ A black box "in technology, science, and other fields, denot[es] any device, algorithm, function, or the like whose inner workings are not visible or obvious but opaque (i.e., black)." BLACK BOX, Black's Law Dictionary (11th ed. 2019)

² Kashmir Hill, *Imagine Being on Trial. With Exonerating Evidence Trapped on Your Phone.*, NY Times, Nov. 22, 2019, available at <https://www.nytimes.com/2019/11/22/business/law-enforcement-public-defender-technology-gap.html> [last accessed Jan. 27, 2020]

³ As of 2019, 96% of American adults owned a cell phone and 81% owned a smartphone. See Mobile Technology Fact Sheet, Pew Research Ctr. (Feb. 2019), available at <http://www.pewinternet.org/fact-sheet/mobile/> [last accessed Jan. 27, 2020]. See also *Carpenter v. U.S.*, 138 S.Ct. 2206, 2220 (2018) ("carrying [a cell phone] is indispensable to participation in modern society").

cases and investigations. The amount of potential evidence that a single cell phone may contain is staggering.⁴ Advances in the fields of DNA, DWI, digital forensics, electronic surveillance, and others have forced both sides of a criminal case to rely more upon science and technology than ever before.

The Legal Aid Society's unique position as the only public defender office that represented clients in all five boroughs allowed for us to create these specialized groups to save us some of the costs of the ever-rising need to hire outside experts. While third-party experts are still necessary in cases, without these Units the number of times external experts would be required would be significantly more. The importance of our Units continues to expand and it is apparent that it will continue to do so.

Public defenders are well aware of the impact that scientific evidence has on a jury, as well as the importance of technological tools for representing and advocating for their clients. Like most issues for public defense, it boils down to funding and a lack of resources. Given proper funding, defense attorneys would maximize the utilization of science and technology in their zealous defense of their clients – as the law requires.⁵ It is difficult to properly represent your clients when you cannot fully analyze the data in their cases or you are unable to obtain or preserve evidence that may be crucial to their defenses. Beyond the Legal Aid Society's own call to maintain and improve its resources, there is also a need for the other public defender offices to have similar capabilities.

⁴ *Riley v. California*, 134 S.Ct. 2473, 2491 (2014) (“a cell phone search would typically expose to the government far more than the most exhaustive search of a house.”).

⁵ *Hinton v. Alabama*, 571 U.S. 263 (2014) (defense counsel's failure to seek additional funds to replace an unqualified expert constituted deficient performance); *People v. Carter*, 167 A.D.3d 513, 514 (1st Dept. 2018) (“[T]rial counsel conceded that his only reason for not calling an expert was the inability of his client, who was also unable to pay counsel's fee, to pay for an expert. He also conceded that he took no steps to obtain a court-appointed expert, and was unaware that this remedy might be available. This constituted constitutionally deficient performance.”).

B. Caseloads Can No Longer be the Only Metric Which is Used to Measure Public Defenders Needs

As the Council is aware, the caseloads for public defense offices have decreased for individual attorneys and offices overall. But the decreased caseloads have not led to decreased work or decreased costs. Multiple factors have caused an increase in expenses and an increase in the amount of work required to be performed on each case.

While the number of misdemeanors has shown a substantial decline since 2015, the number of felonies has not decreased at nearly the same rate. Additionally, the amount of work, money, and resources required for each case has dramatically increased. For example, the total cost of witnesses, experts, and consultants has almost tripled in the last five years. This figure would be even greater if we needed to hire digital forensics experts on all of the cases that require them. The increase in witness, expert, and consultant costs is a reflection of the change in which cases are prosecuted and defended – spurred by the increasing use of technology and science in cases. Cases that were once limited to eye witness and complainant testimonies, now may include electronic data from multiple sources (cell phones, social media, body-worn cameras) and DNA evidence, among other types of evidence. Since there are less misdemeanor cases, both sides having additional time and energy to spend on more serious cases and therefore are litigating more issues more extensively.

The amount of evidence that may exist in the world on one case has ballooned and some of it may only be available for a limited time. This requires attorneys and investigators to move quickly before something gets deleted or overwritten. Investigators are tasked with finding video cameras at the scene of an incident as quickly as possible because the video may disappear if we wait too long. Similarly, they must scour the internet and social media to see if there are videos of incidents, people describing what they saw as possible witnesses, etc. All of that information can disappear in a blink of an eye, a person can shut down his or her account and crucial

evidence may be lost to the defense forever.⁶ Unlike the prosecutors, we do not have both in-house investigators and an army of police officers with law enforcement powers available for our investigations. The duty to investigate our cases quickly and thoroughly comes with its own needs and costs.

Although this hearing is about the technology gap, it is important to note how other changes to public defense have impacted resources. There has been a greater acknowledgement in the justice system and in society overall that mental health, substance abuse, employment, and housing issues significantly affect whether someone has contact with the criminal justice system. With that information in mind, public defense offices are investing in resources to better serve our clients by trying to decrease the likelihood that they will be our clients again in the future. In order to do that, we have increased our reliance on social workers and attorneys specializing in diversion programs and courts. A lot of time, energy, and people power goes into getting mental health and other medical records, determining appropriate programs, finding availability in those programs, and then regularly coordinating with the programs. Furthermore, the number of cases in which prosecutors and judges are requesting pre-pleading memoranda to justify a particular plea offer or to agree to diversion has steadily increased and so has the amount of information that they require.

At the same time we have attorneys and staff to advise and advocate for issues related to immigration, housing, and employment. Typically, these are the three highest concerns of our clients, right after incarceration – which often directly negatively affects these other areas. We have a constitutional obligation to research our client's possible immigration issues and advise

⁶ This is also made more difficult by the Stored Communications Act which is discussed further below.

them accordingly.⁷ The effects that a conviction, arrest, or ongoing case may have on a person's housing or employment is also a legitimate concern that does not have a one-size fits all answer.

IV. THE IMPORTANCE OF RESOURCES

A. The Digital Forensics Unit

The Legal Aid Society's Digital Forensics Unit has the rare distinction of having access to some of the same tools that law enforcement does.⁸ As a result, we are able to use these tools to benefit our clients and aid in their defenses, without outsourcing to a third-party. There are multiple benefits to this.

One, we do not have to pay for an expert or rely upon the prosecution or the NYPD to agree to help us. Two, our client's privacy is protected and they are more comfortable with handing over their personal information. Three, we can testify with first-hand knowledge. Four, we do not have to take into account whether an expert or a process is "necessary" or "worth it." Five, we can appropriately advise attorneys on how to challenge evidence in their clients' cases by having direct access to the systems that preserved or created the evidence. Lastly, we are able to make our own analyses and interpretations of the data, independent of any prosecution witness.

The effects of these benefits are made apparent to us daily. Clients may be reluctant to turn over their devices to law enforcement (or anyone for that matter) because, as is true for many of us, it contains some of the most private information of their lives. A short list of examples includes private messages between partners, medical information, banking information, photos of friends and family, and location information.⁹ Clients are put at ease

⁷ See *Padilla v. Kentucky*, 559 U.S. 356 (2010).

⁸ We have hardware and software from Cellebrite, Magnet Forensics, OpenText/Guidance Software, and others.

⁹ See *People v. Weaver*, 12 N.Y.3d 433, 441-442 (2009) (the Court describes how location data alone can be used to reveal the most intimate details of a person's life: "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on.")

because we have already developed a relationship with them as their attorneys and we have ethical and legal obligations to fight for them as well as protect their confidential information. Law enforcement and prosecutors do not owe them any such duty.

When working with limited resources you are always forced to make decisions on how to allocate those resources. The reality is that this forces a series of decisions where an attorney and an organization must decide: “Do I need to hire an expert in this case?” “Can we afford to hire this particular expert or do I have to use someone else?” “How do I balance the cost of the expert’s rate with my need to have a long discussion with the expert?” For our purposes, we do not need to engage in such thinking because we already have our own experts and equipment with little to no additional costs for each case. As a result, it encourages attorneys to use our services even in situations where they are not sure it will help or the usefulness is not completely clear. Numerous times when our Unit has been engaged in one of these situations we have found or explained important information or data that would otherwise not have been discovered or would have come as a surprise during a hearing or trial. Had those attorneys been forced to hire outside experts and pay to access their resources, it is unclear how often they would have done so. These are also issues that wealthy defendants do not have to consider and, as a result, the disparate treatment of indigent defendants is exasperated.

Case Examples¹⁰

Work from members of the Digital Forensics Unit has helped in numerous cases across the City. I have chosen a few examples to illustrate the benefits of the necessary tools in the hands of qualified individuals within our office.

Misidentification: Mistaken witness identification has long existed as a problem in criminal cases and has been a substantial contributor to false convictions.¹¹ Digital forensics

¹⁰ To preserve attorney-client privilege, attorney-work product, and client confidences, I have intentionally limited the use of identifying details in these examples.

evidence is not perfect and not always available but when the processes are performed correctly, they are typically much more reliable than witness identifications.

An example of when that was true was for a client identified in a photo array and later charged with robbery. Our client was alleged to be a known sex worker and the complainant alleged that he set up a date to meet our client for sexual services in exchange for money. The complainant alleged when he arrived, he was robbed. He later identified our client in a six-person photo array as the woman who robbed him. Our client was arrested and bail was set pending the outcome of the grand jury.¹² Our client maintained her innocence and told us she was in another state at the time of the alleged incident. Using the data from her phone, social media accounts, and cloud storage, we were able to show that photos with attached Exif¹³ data and other location data demonstrated that her alibi was accurate. Therefore, she could not have committed the crime charged as she was far from the location at the time of incident. Shortly after presenting our findings to the prosecutor the client was release on her own recognizance and her case was later dismissed.

In an unrelated robbery case, our client was identified in a photo array by the complainant, who knew our client from the neighborhood but did not have a personal relationship with her. Our client was subsequently arrested. She maintained that she was at a theme park that day with her friends. Some of her friends could not be found and others were reluctant to get involved. We asked the client if she had any photos from the day of the incident and she advised us that she did and they were on her phone. We extracted the photos from her

¹¹ 29% of exonerated cases since 1989 involved mistaken witness identification. *Exonerations Contributing Factors*, The National Registry of Exonerations, available at <https://www.law.umich.edu/special/exoneration/Pages/ExonerationsContribFactorsByCrime.aspx> [last accessed Jan. 28, 2020].

¹² Pursuant to Criminal Procedure Law §180.80.

¹³ EXchangeable Image Format. “Descriptive data (meta-data) in an image file that include the date the photo was taken, resolution, shutter speed, focal length and other camera settings.” *Definition of EXIF*, PCMag, available at <https://www.pcmag.com/encyclopedia/term/exif> [last accessed Jan. 27, 2020].

phone in a forensically sound manner. We knew that the photos of her in a theme park without more would not prove her innocence; we needed to establish the date, time, and location of the photo. Using the metadata from the photos we were able to do that and the case was dismissed.

Another client of ours was identified as the perpetrator of a gun-point robbery. A few days after the incident, the complaining witness saw our client walking down the street and reported to the police that he had found the man who had robbed him earlier in the week. Using call logs, text logs and content, and call detail records with historical cell-site location information from his cell phone service provider, we were able to show that at the time of the incident our client was in another borough arguing with his girlfriend over text messages. The case was dismissed.

Spoofing¹⁴ and Fake Information: A concern for all actors in the criminal justice system is the use of fake information or fraudulent evidence. The rise in access to electronic devices and powerful software has given more people the ability to fabricate evidence but few can truly deceive a trained expert. A properly performed digital forensics investigation can reveal a multitude of inconsistencies and red flags.

We had a case where our client was accused of violating an order of protection. His ex-girlfriend alleged that he had called her multiple times and threatened her. She showed officers screenshots of her phone's call log with his number displayed as having called her. Our client was arrested based upon her claims and the screenshots. Her phone was never examined and at that point no phone records were obtained. Our client maintained his innocence and denied having any contact with the complainant. The prosecution later provided copies of the complainant's phone records from the phone company which showed calls made to the

¹⁴ "Spoofing is when a caller deliberately falsifies the information transmitted to your caller ID display to disguise their identity." *Caller ID Spoofing*, Federal Communications Commission, available at <https://www.fcc.gov/consumers/guides/spoofing-and-caller-id> [last accessed Jan. 27, 2020].

complainant from our client. We had examined our client's phone and found no indication that he had communicated with the complainant. We also ordered his phone records and noticed an anomaly. Despite the complainant's records showing calls made from our client, his records did not show any calls from him to his ex-girlfriend. Through our investigation we were later able to show that the complaining witness was using a spoofing service to call herself but make it appear to her phone and phone company that our client was calling her. His case was eventually dismissed.

In a similar case, a third-party was harassing our client's ex-girlfriend while pretending to be our client. We extracted data from multiple phones, social media accounts, email accounts, and cloud storage. We obtained phone records and also preserved public social media information. We were eventually able to present to the prosecution that not only was our client not the person harassing the complainant but we also identified the individual responsible, despite the fact that he worked information technology (IT) and had attempted to cover his tracks while creating evidence to point to our client. Thankfully, the prosecution had done a proper forensic extraction of the complainant's phone. After comparing the information, we obtained and the complainant's information our client's case was dismissed. This case took extensive work, time, and energy to prove the available evidence was false or misleading. At the time the case had been dismissed, our client had been falsely arrested multiple times in regards to the harassment of the complainant – at no fault of the complainant. It would have been difficult to prove the charges as false solely through cross-examination because the complainant legitimately believed that our client was the harasser. The NYPD's investigation never came close to the level of our investigation. We cannot solely rely upon law enforcement; a well-funded and resourced defense office is necessary.

Trial Work: The above discussed cases were all eventually dismissed by the prosecution but our analysts have also testified in trials when prosecutors have refused to dismiss cases.

One example is when our client was charged with a series of petit larcenies from different stores. The client was originally charged with one larceny but based upon a pattern identified by law enforcement, he was also charged with the other larcenies that allegedly fit the pattern. We obtained our client's call detail records from the phone company including his historical cell-site location information (the records of the location of cell phone towers used for each call). Mapping that location information showed that for almost all of the alleged incidents it was unlikely that our client could have committed the crime which also cast doubt on the alleged pattern. A jury acquitted our client of all charges.

In another case, our client was charged with the sale of a controlled substance, despite the fact that there were no drugs found on him. The prosecution alleged that when our client saw someone he knew in a store and shook his hand that he was delivering drugs to that person. An undercover officer had previously bought drugs from the acquaintance but now the officer was requesting a different drug which the acquaintance did not have on him. The acquaintance was alleged to have made a phone call to have someone else deliver the other drugs to him. The prosecution alleged that our client was the recipient of that call. At trial, our client testified to his locations throughout the day, his activities, his reason to have been at that store at that time, and his relationship (or lack thereof) to the person alleged to have sold controlled substances to an undercover officer. Using the data extracted from his phone and his historical cell-site location information, the analyst was able to testify to her analysis of the data which was consistent with our client's testimony – including that there was no record of a communication between the acquaintance and our client. The jury acquitted our client.

Mitigation: Dismissals and acquittals are always welcomed outcomes but every public defender knows that mitigation of charged conduct is important as well.

One of our clients was charged with burglary, among other charges, for allegedly stealing money from the company he worked for from a location he allegedly did not have authority to access. Our client had told us that there were messages from his boss on his old phone that showed that he had been authorized to take the money and access the location. When the client brought the phone to our office it was in pieces. Worse yet, he had previously brought the phone to a repair shop to fix since it was no longer under warranty. The repair shop appears to have been less than reputable as they claimed they were unable to fix his device but they also seemed to have taken some of the parts from the phone, presumably for spare parts to fix other customer's phones that required less work. We knew the call detail records from the phone company only confirmed that messages were sent between our client and his former boss but it would not show the content of the messages. As a result, we ordered a phone of the same model and swapped out the necessary parts, fully repairing the original phone. We then were able to extract the messages from the client's phone which mostly supported our client's version of the events. Unfortunately, some of the messages were no longer available and could not be recovered. The client was offered and took a disorderly conduct violation. His case went from a felony charge to a non-criminal disposition.

In another case, our client was a ride share driver who was alleged to have assaulted his passengers on one of his trips. Our client maintained while he did have physical contact with the alleged complainants, it was only in response to their actions which included getting naked in the back seat of his car after he asked them not to, damaging his vehicle, standing in front of his car refusing to allow him to leave, and one of them placing their hands on him first. The complainants' stories were that our client had assaulted them because our client was anti-gay and

they denied any of the conduct the client alleged. Our client had a dash cam video recorder that was facing the inside of his vehicle but the memory card that the video was being saved to had been corrupted so the video could not be played. We created an image¹⁵ of the memory card and were able to recover the video file but the file itself was still not playing. Using forensic video software, the analyst was able to salvage parts of the video, then separately recovered the audio track, and synced the audio to the recovered video. It contained clear audio and video which verified much of the client's allegations (some acts took place outside the vehicle and was not captured by the camera). Our client took a plea to a violation, a non-criminal offense, preventing him from receiving a criminal record.

Even in cases where the information we obtain is negative or our analysis does not support the client's defense, it can still be useful. Attorneys then feel more comfortable and knowledgeable when advising their clients about whether or not to take a plea and how we expect the evidence may be used at a trial.

B. The DNA Unit

The Technology Gap: DNA testing in New York is performed by the Office of the Chief Medical Examiner at the request of the prosecution or police. Although housed in the Department of Health as an independent agency, the OCME's DNA testing arm, the Forensic Biology Laboratory, works for the prosecution, not the defense. The imbalance in accessibility, resources and information between the prosecution's and defense's access to OCME creates a significant technology gap in this area.

¹⁵ "An exact bit-stream copy of all electronic data on a device, performed in a manner that ensures the information is not altered." *Computer Security Research Center Glossary*, National Institute of Standards and Technology (NIST), available at <https://csrc.nist.gov/glossary/term/Image> [last accessed Jan. 27, 2020].

The OCME Forensic Biology laboratory currently employs more than 160 forensic scientists and performs DNA testing on approximately 40,000 pieces of evidence each year.¹⁶ Its annual budget exceeds ten million dollars.¹⁷ These vast resources are entirely at law enforcement's disposal: police and prosecutors request testing of evidence as they see fit in any given case. They may choose to have certain items tested, or not tested. OCME, almost always in our experience, follows that direction. In fact, the OCME refers to law enforcement as their "customers," and treats them as such by providing them with services on demand.

At the same time, the OCME's vast and experienced staff are available to meet with prosecutors, and testify on their behalf, free of charge, in every case in which they are asked. In other words, the prosecution has at its disposal a multi-million dollar laboratory and army of experts to help build their case.

The defense does not have the same access to OCME. The OCME, in our experience, has refused defense requests for testing in cases where the prosecution does not consent. In cases where DNA results are dependent on data that is input into the commercial software program used by the laboratory (STRmix), the OCME typically refuses our requests to consider different, reasonable hypothetical datasets that may exonerate our client. This is so even though leading scientists encourage defense input into the datasets used by DNA expert software systems.¹⁸

Additionally, prosecutors, but not the defense, are regularly invited to the OCME to discuss new testing methods and technologies in the laboratories. For example, the OCME

¹⁶ See Office of the Chief Medical Examiner, Finance Division Briefing (2019), p. 5, available at <https://council.nyc.gov/budget/wp-content/uploads/sites/54/2019/03/816-OCME-2020.pdf> [last accessed Jan. 28, 2020]

¹⁷ See Office of the Chief Medical Examiner, Finance Division Briefing (2018), p. 12, available at <http://council.nyc.gov/budget/wp-content/uploads/sites/54/2017/03/OCME.pdf> [last accessed Jan. 28, 2020]

¹⁸ See Peter Gill, et al, *DNA commission of the International society for forensic genetics: Assessing the value of forensic biological evidence –Guidelines highlighting the importance of propositions*, Forensic Science International: Genetics 36 (2018), 189-202; Simone Gittleston, et al, *A Practical Guide for the Formulation of Propositions in the Bayesian Approach to DNA Evidence Interpretation in an Adversarial Environment*, Journal of Forensic Sciences, 61 (2018), 186.

recently met with members of all five New York City DA's offices to discuss what information it will turn over from the software programs it uses under the new discovery law.¹⁹ When members of the Legal Aid Society asked for a similar meeting to discuss the new discovery law, the OCME refused.

The Legal Aid Society's Efforts to Bridge the Gap: The Legal Aid Society's DNA Unit was formed, in large part, to provide resources to defense attorneys to bridge this information and access gap. Formed in in 2013, the Unit focuses on understanding the DNA evidence generated by the OCME and used in court against our clients.

Our Unit has 10 attorneys and support staff, who are trained in forensic sciences and the law. The Legal Aid Society subscribes to scientific journals, and DNA Unit lawyers attend scientific continuing education seminars. The DNA Unit lawyers, in turn, consult with staff attorneys across the Criminal Defense and Juvenile Rights practices, and provide regular trainings to them. The resources expended on these efforts all are critical to providing our clients' their Constitutionally-guaranteed right to counsel. Indeed, New York's Court of Appeals, as well as a lower appellate court, reversed convictions based on ineffective assistance of counsel in cases where defense lawyers did not understand DNA.²⁰

When a defense lawyer understands DNA results, he or she can prevent wrongful convictions. For example, in 2016, Jenny Cheung, an attorney in the DNA Unit represented a Queens man named Terrell Gills.²¹ Jenny was assisted by other members of the DNA Unit, who provided back-up support. Mr. Gills was prosecuted for a robbery of a Dunkin Donuts that he did not commit. Even though video surveillance showed a man other than Mr. Gills committing the

¹⁹ CPL Article 245

²⁰ *People v. Wright*, 25 N.Y.3d 769 (2015); *People v. Powell*, 165 A.D.3d 842 (2d Dept. 2018).

²¹ Eli Rosenberg, *Can DNA Evidence Be Too Convincing? An Acquitted Man Thinks So*, NY Times, May 16, 2017, available at <https://www.nytimes.com/2017/05/16/nyregion/can-dna-evidence-be-too-convincing-an-acquitted-man-thinks-so.html> [last accessed Jan. 28, 2020]

robbery, and that other man on the video had in fact been convicted of two other, nearly identical, Dunkin Donuts robberies, the Queens DA's Office insisted on prosecuting Mr. Gills for one reason alone — his DNA was detected on the store's cash register. Ms. Cheung, through her expertise as a DNA Unit member, was able to explain this bizarre event: the cleaning solution used by that branch had the ability to extract and transfer DNA throughout the store. Mr. Gills, who was a regular customer at that location, had his DNA inadvertently moved from an innocent place to an incriminating one. OCME never explained this possibility to Ms. Cheung. In fact, the analyst told the jury that this explanation was "highly unlikely," despite overwhelming scientific evidence to the contrary. It was only through the resources she was able to access at Legal Aid that she was able to convey this information to a jury and ultimately earn her client's acquittal.

The Need for More Resources: Despite the DNA Unit's expertise, they are still attorneys, not scientists and are only ten people amongst the Society-wide staff of approximately 1,000 staff attorneys. Thus, despite the resources The Legal Aid Society has devoted to its DNA Unit, we are still vastly outpaced by the DAs. Unlike the prosecution, we do not have access, free-of-charge, to 160 OCME-trained analysts. Instead, when we encounter a case with DNA results, we must find a qualified DNA expert and pay to retain his or her services. The field of forensic DNA experts is competitive, driving hourly rates up and availability down. At OCME's rate of testing tens of thousands of cases per year, the lack of access to on-call scientists, like the prosecution, is financially overwhelming. The Council should provide for public defenders to have staff scientists.

In addition, while the prosecution can request testing of any item of evidence at will, the defense must pay independent laboratories for adversarial testing. Adversarial testing is critical to the defense function — scientists have observed that different software programs can get

different results, including results that either include or exclude a defendant.²² Even running different datasets within the same program can make the difference between inclusion and exclusion.²³ The Council should ensure that public defenders are funded both to purchase, and employ experts to use, the software program used by OCME as well as competing software programs that may lead to exculpatory results.

The OCME's DNA testing is only getting more sophisticated, and prosecutors are only going to use it in more cases. The gap in access to the laboratory, as these measures increase, will become starker. Without increased funding for staff, training, experts and software, defenders will fall far behind in understanding DNA technology. The next Terrell Gills may not result in an acquittal, but a devastating wrongful conviction.

C. Law Enforcement Only Tools and Capabilities

It may be beyond the scope of this hearing and the Council's abilities but it is important to note the disparities that exist as a result of companies that restrict their sales to law enforcement only. It also important to note how laws governing obtaining information have allowed police and prosecutors to get data and records that defense attorneys cannot. Some tech giants have actively sought to make the imbalance worse.

There are an assortment of tools that are explicitly law enforcement only and others that by their refusal to cooperate with the defense are essentially law enforcement only. Two examples of law enforcement only tools are Cellebrite Premium²⁴ and GrayKey by Grayshift.²⁵

²² See President's Council of Advisors on Science and Technology, Report to the President: Forensic Science in Criminal Courts: Ensuring Scientific Validity of Feature-Comparison Methods, p. 79n, available at https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_forensic_science_report_final.pdf.

²³ *Supra*, n.17.

²⁴ *Cellebrite Premium*, Cellebrite, available at <https://www.cellebrite.com/en/ufed-premium/> [last accessed on Jan. 27, 2020].

²⁵ *Introducing GrayKey*, Grayshift, available at <https://graykey.grayshift.com/> [last accessed on Jan. 28, 2020] and *GrayKey*, Magnet Forensics, available at <https://www.magnetforensics.com/graykey/> [last accessed on Jan. 28, 2020].

Both are mobile forensics tools that can extract more data off of more secure phones than the standard mobile forensics options are capable of doing.

Even more troubling is the Stored Communications Act,²⁶ a federal law that requires a search warrant to get “content” from a provider of remote computing services or electronic communications services. The Stored Communications Act only requires a subpoena or a court order for non-content. In short, this means that the defense is barred from obtaining “content” from Facebook, Instagram, Twitter, Google, and others because defense attorneys are not able to get search warrants.²⁷ Content includes, but is not limited to, photos, videos, wall postings, messages, comments, emails, and location information. Even though, in theory, defense attorneys can obtain non-content, like subscriber information, through a subpoena, some of the companies make it incredibly difficult and at the same time bend over backwards for law enforcement.

Facebook is a perfect example of this. It offers a law enforcement only portal for police and prosecutors to upload warrants, orders, and subpoenas.²⁸ Defense attorneys are not permitted to use that portal. Additionally, Facebook argues that in order for a defense attorney’s subpoena to be valid and enforceable the subpoena must be personally served on their office in Menlo Park, California. In order to do this, an attorney would need to get a subpoena signed by a New York judge, brought to a judge in California to be signed, and then have it served upon Facebook’s office. This would require either the attorney going to California each time, having an attorney in California do them a favor each time, or retain a law firm in California for this

²⁶ 18 U.S.C. 121 §§2701–2712

²⁷ See generally Megan Cassidy, *Facebook, Twitter hold evidence that could save people from prison. And they're not giving it up.*, San Francisco Chronicle, Jan. 21, 2020, available at <https://www.sfchronicle.com/crime/article/Facebook-Twitter-hold-evidence-that-could-save-14990176.php> [last accessed Jan. 28, 2020]

²⁸ *Law Enforcement Online Requests*, Facebook, available at <https://www.facebook.com/records/login/> [last accessed Jan. 28, 2020].

purpose. Even though Facebook has an office right here in New York City²⁹ and is required under New York State law to accept service in this State, they are currently arguing that they do not have to accept service here and they will only honor subpoenas personally served on them in California.

D. The Technology Knowledge Gap

Another issue that arises is that the technology gap is not always possible to fully gauge. For example, despite articles about the Manhattan District Attorney's Office's ten million-dollar digital forensics facility,³⁰ there are technologies that we are not always aware of³¹ and that they have sometimes fought to prevent us from knowing about.³²

The NYPD and the District Attorneys' Offices appear to have a wide range of technologies to choose from but we are often the last to know and they seem to prefer it that way.³³ As a result, the "technology gap" or the justice system "digital divide" may be even broader than I am capable of discussing here. Only upon an accounting of everything available to these agencies can we actually know the true size of the issue.

V. COURT ROOM TECHNOLOGY

Public defenders also suffer from a lack of court room technology. Long gone are the days of poster boards and markers. Juries expect digital presentations and our evidence itself is quickly becoming more and more digitally based. Furthermore, the Court of Appeals has

²⁹ 770 Broadway, New York, NY 10003 and their Dept. of State Process Address is Facebook, Inc., C/O Corporation Service Company, 80 State Street, Albany, NY 12207

³⁰ Jeff John Roberts & Robert Hackett, *Inside America's Newest Digital Crime Lab*, *Fortune*, Nov. 15, 2016, available at <https://fortune.com/longform/vance-crime-lab/> [last accessed Jan. 27, 2020].

³¹ Michael Hayes, *Inside New York City's Partnership With Israeli iPhone Hacking Company Cellebrite*, *OneZero*, Oct. 7, 2019, available at <https://onezero.medium.com/exclusive-inside-new-yorks-partnership-with-israeli-iphone-cracking-company-cellebrite-12a2252c3ebf> [last accessed Jan. 28, 2020]

³² See *The Legal Aid Soc. v. New York County Dist. Atty.'s Off.*, 2019 N.Y. Slip Op. 31106[U] (Sup. Ct., New York Co. 2019) (the Manhattan DA's Office fought the Legal Aid Society's FOIL request for information on its social media monitoring tools).

³³ See *People v. Gordon*, 58 Misc.3d 544 (Sup. Ct., Kings Co. 2017) (the Legal Aid Society was the first to identify the use of a secretive cell-site simulator device in an open NY state case).

endorsed the use of PowerPoint presentations and similar demonstrative exhibits in summations.³⁴

Digital videos, pictures, and audio recordings are common pieces of evidence in criminal cases. Defense attorneys often have difficulty presenting these forms of evidence due to a lack of our own technology that we can deploy in courtrooms. This has led to some attorneys bringing their own personal devices from home, which are still inadequate. Tiny computer speakers and miniature screens cannot be compared with loud clear sounding speakers and screens larger than the average person's living room television.

Sometimes we have been able to rely upon the prosecutor's technology during trial but if we are required to rely upon our adversaries to provide us with the necessary resources to present our clients' defenses then it is no longer a true adversarial system. An adversarial system is not possible when one side must rely on the other side's graciousness and support to effectively represent its client. Additionally, their technology may not always be available to use. If the prosecution does not plan to present a particular item then they have no reason to bring the technology to display it to court.

Proper representation of our clients in the modern age requires the ability to fully present the evidence and their cases in a manner that best conveys its importance. There are two possible solutions to this issue. One, provide the necessary money for public defender offices to have the correct presentation and display tools or, two, upgrade the courts so that the tools are built into the court rooms and accessible to anyone from any side. Option number two is being implemented in court houses around the country including here in New York State. The Commercial Division of the Westchester County Supreme Court received upgrades that included sound systems, monitors for displaying testimony, and an evidence presentation system, among

³⁴ See *People v. Williams*, 29 N.Y.3d 84, 89 (2017) ("There is no inherent problem with the use of a PowerPoint presentation as a visual aid in connection with closing arguments. Indeed, it can be an effective tool.")

other technological improvements.³⁵ The technology used there may or may not be the same as we would want used in New York City courthouses but it proves it can be done.

VI. TECHNOLOGY ALONE IS NOT SUFFICIENT; QUALIFIED STAFF AND TRAINING IS ALSO NECESSARY

A. Knowledgeable and Properly Trained Staff is Required

Although the majority of my testimony has been in regards to access to the necessary tools, the usefulness of such tools is greatly diminished without sufficiently qualified staff. The Legal Aid Society's Digital Forensics Unit's examiners and analysts studied digital forensics and cybersecurity in college. Upon hiring, they have received trainings and certifications for various related skills and areas of expertise. As a result of their education and hands on experiences, they can properly use digital forensics tools. Importantly, they have been qualified as experts in courts and can counter NYPD and prosecution expert witnesses.³⁶

Without the knowledge to operate the various software and hardware processes and an understanding of how they work, access to these tools will lose its value. It is important to have qualified staff for three primary reasons: (1) they will be successful in achieving the goals of using the tools for clients' cases; (2) they can properly review data created or preserved – either from their own work or as provided in discovery by the prosecution; and (3) they can be qualified as experts to testify on behalf of the defense.

Staffing not only relates to digital forensics experts and DNA attorneys but also relates to information technology employees, management of information systems employees, investigators, and e-discovery staff.

³⁵ Hon. Alan D. Scheinkman and Shen Guo, *Tech in the Courtroom*, New York State Bar Association Journal, Mar./April 2018.

³⁶ *Hinton* at 276 (“Prosecution experts, of course, can sometimes make mistakes. Indeed, we have recognized the threat to fair criminal trials posed by the potential for incompetent or fraudulent prosecution forensics experts... This threat is minimized when the defense retains a competent expert to counter the testimony of the prosecution's expert witnesses; it is maximized when the defense instead fails to understand the resources available to it by law.”)

B. Technology Changes at a Rapid Pace and Scientific Innovation Will Never Cease

Highly qualified individuals who can be testify as experts in criminal proceedings must be paid accordingly. Furthermore, their certifications must be renewed and their knowledge must be constantly updated. Innovation in technology happens on a daily basis and significant changes happen so frequently it takes dedication to always stay apprised of the all that is occurring. As a result, digital forensics examiners and analysts must continuously attend trainings and conferences to remain experts. This is similar to how attorneys are required to attend Continuing Legal Education courses to maintain their license to practice law except the pace in which changes occur in the digital world far surpasses the changes that take place in the legal realm.

While there may be ground principles of science that never change or rarely have changed, science itself is an ever-improving and evolving field of study. Breakthroughs occur, theories are proven, unknowns are resolved, and sometimes as a result they generate a new set of unanswered questions. Initial training is important but an ongoing commitment to provide sufficient funding and resources for regular trainings and conferences are vital.

VII. ADDITIONAL RESOURCES AND CONTINUED FUNDING IS NECESSARY TO EFFECTIVELY REPRESENT OUR CLIENTS

A. Additional Resources

Though we have nationally renowned specialized Units, part of that attention is because of the rarity of a public defense office that even has that resource at all. Our resources and funding still do not compare to those of the District Attorneys' Office or the NYPD. There are still gaps in acquiring tools, staff, and training.

There are additional tools that public defenders need access to that we either know prosecutors and the NYPD have access to or we suspect that they do. These include e-discovery tools that can be connected to or be part of a cloud storage system and analytics programs to

review and analyze large amounts of digital data (especially when it is from multiple different sources, i.e. multiple phones, social media accounts, etc.).

As we move to cloud storage systems and as case files become more digital and less paper, we need the appropriate funding to maintain the cloud storage and to retain files in compliance with our ethical obligations. The rules of ethics and common sense require us to keep files for designated long term periods. It will cost money to keep those files in “cold storage” or “archived storage” in the cloud and that cost will increase each year as we are required to retain more cases and more data from those cases.

We also have to ensure the security of the systems being used or that will be used in the future. I think both sides would agree that there is significant private information contained in case files and discovery. Like most law firms, we are also concerned about malware, ransomware,³⁷ and general security issues. We also must protect the systems from failures by having backups and redundancy³⁸ built-in.

Additionally, our electronic devices, internal computer networks, and internet bandwidth must be capable of handling the discovery of the present and of the future. With that, there also must be better file transfer resources to allow files to be shared more smoothly between the public defender offices and the prosecution offices, as part of the need to comply with each other’s discovery obligations. Lastly, members of public defender offices need to be able to access the data related to their cases wherever they may be, including in court, at a Department

³⁷ “A type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid. More modern ransomware families, collectively categorized as crypto-ransomware, encrypt certain file types on infected systems and forces users to pay the ransom through certain online payment methods to get a decrypt key.” *Ransomware - Definition*, TrendMicro, available at <https://www.trendmicro.com/vinfo/us/security/definition/ransomware> [last accessed Jan. 28, 2020].

³⁸ “Having a secondary peripheral, computer system or network device that takes over when the primary unit fails.” *Definition of Redundancy*, PCMag, available at <https://www.pcmag.com/encyclopedia/term/redundancy> [last accessed Jan. 27, 2020].

of Corrections facility, in an office, or at home. The best way to accomplish that goal is a combination of cloud storage, internet access, and tablets to view the materials.

B. Regular Continued Funding

Funding and adequate resources are going to be required annually. As discussed throughout my testimony, this is the future and we are all already falling behind. There will be a need for regular trainings for both experts and non-experts alike. Almost all of the programs and other tools we currently have, are looking to purchase, and likely will be available in the future have recurring licensing fees and upgrade costs. Many of them require training in order to use them properly.

CONCLUSION

Proper funding and sufficient resources are required to close the technology gap between the prosecution and public defense offices. Failure to do so will lead to ineffective assistance of counsel, false convictions, and an exacerbation of the already disparate treatment of indigent defendants. This applies to all public defender offices, not just the Legal Aid Society. The City Council has the ability to act and it must do so. It would set a positive example for the rest of the country, many of whom are already looking to us for guidance, and ensure that all defendants are fairly represented.



TESTIMONY OF:

**Elizabeth Daniel Vasquez
Special Forensic Science Counsel**

BROOKLYN DEFENDER SERVICES

**Presented before
The New York City Council Committee on Justice System**

**Oversight Hearing on The Technology Gap
between Public Defenders and DAs**

January 29, 2020

My name is Elizabeth Daniel Vasquez. I am the Special Forensic Science Counsel at Brooklyn Defender Services (BDS) and lead the Forensic Science Practice within the Criminal Defense Practice. I have practiced as a criminal defense lawyer and as a civil rights attorney in New York, Washington, DC, and in federal courts across the country. The Forensic Science Practice's mission is to provide resource and support counsel services to trial attorneys facing complex forensic issues in misdemeanor, felony, and homicide cases in Brooklyn Criminal and Supreme Court. In that role, the Unit monitors the development of emerging scientific, technical, digital, and surveillance techniques, educates our trial lawyers regarding those techniques, and analyzes the legal and scientific or technical issues raised by the techniques themselves as well as their use or misuse.

BDS provides multi-disciplinary and client-centered criminal, family, and immigration defense, as well as civil legal services, social work support and advocacy, for over 30,000 clients in Brooklyn every year.

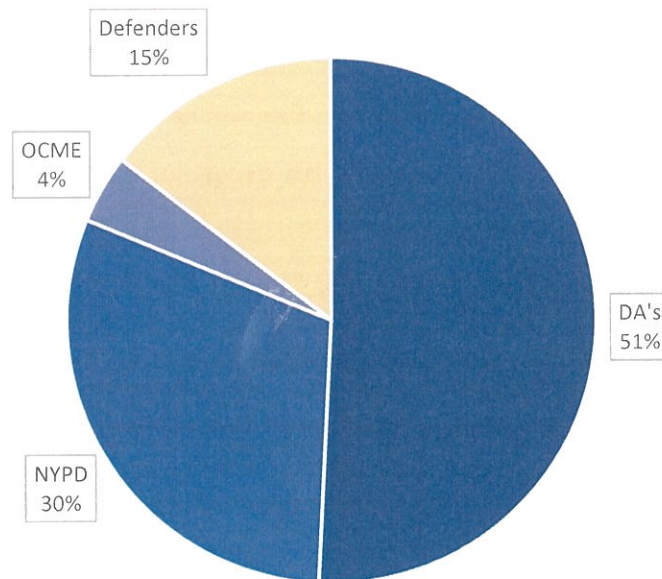
I thank the Committee on Justice System and Chairman Rory Lancman for inviting us to testify today about the technology gap between the City's public defenders and district attorneys.

Background

Over the last decade, technology has expanded and permeated our society to a remarkable degree. Tracking alongside that expansion, new investments have been required within the legal system—both civil and criminal. Funding to meet these challenges largely has funneled to the prosecution’s side of our adversary criminal system.

The New Year brought with it momentous and positive changes to New York’s discovery regime. The new discovery laws—much needed and integral—also brought with them an accelerated push within New York City’s system to digital discovery. The technological opportunities opened by this switch to digital discovery make the timing of this hearing both serendipitous and essential. The technology gap extends not only to questions of forensic tools and gadgets, but also to baseline technical capabilities to manage the expanding currency of data within the system.

Mayor Di Blasio’s recently proposed 2021 budget provides data with which the technology gap can be clearly seen. Specifically, the proposed budget outlines allocation for discovery reform implementation.¹ The numbers are stark:



In real terms, proposed funding related to criminal justice reform implementation reflects at worst a 6 to 1, and at best a 3.5 to 1, disparity in dollars invested.

¹ “A \$175 million investment — much of which was announced back in November — includes \$104 million for supervised release programs, \$35 million for district attorneys, \$21 million for the NYPD, \$10 million for indigent defense providers, \$2.9 million for the Office of the Chief Medical Examiner, \$857,000 for the fire department and \$487,000 for the law department.” Emma Whitford, “Mayor blames state deficit in ‘cautious’ \$95.3B budget preview,” The Brooklyn Eagle (Jan. 17, 2020), at <https://brooklyneagle.com/articles/2020/01/17/mayor-blames-state-deficit-in-cautious-95-3b-budget-preview/> (last accessed Jan. 28, 2020).

By another metric, the Mayor’s proposed budget also indicated that 1,006 total new staff were needed among the DA’s offices, NYPD, and OCME to implement the reforms.

Outside this particular budget-year, the NYPD has robust partnerships with technology giants, including Microsoft and IBM.² The OCME’s equipment and software budget is fed by federal grants, in addition to local and state funding.³ The DA’s Offices, which have direct access to the NYPD and the OCME, have separately built their own state-of-the-art digital labs, hired expert teams, and outfitted their firms with needed equipment.⁴

In Brooklyn, in addition to the hardware/software advantage, the King’s County District Attorney’s Office (“KCDA”) also has internal access to a former OCME analyst on staff, as well as digital forensics analysts. Furthermore, like the City itself, the KCDA has a data team that is part of its Crime Strategies Unit. In our increasingly data-driven world, access to a team of professionals with computer science analytics backgrounds allows an office to more readily identify and implement big data analytics solutions to data problems—a tremendous advantage at the height of digital discovery.

Meanwhile, indigent defense providers have been forced to get creative—a challenge that the offices in this City have met forcefully. However, the technology gap is real, and adversely affects criminal defendants in our system daily. What’s more: the gap is growing. Year over year failures in large-scale funding for investment only expand the widening technology gap between the City’s indigent defense providers and prosecutors.

Minding the Gap: What It Would Take to Create Parity

The technology gap can be seen across several spectra. This testimony will address four critical areas that prominently display the technology gap, and in which investment would be essential to close it: people, hardware needs, advanced data processing, and advanced forensics tools.

People

While the New York Time’s article “Imagine Being on Trial. With Exonerating Evidence Trapped on Your Phone” did an excellent job of describing the gadget and software disparity that constitutes a portion of the technology gap, a critical and consuming element of that gap was largely unarticulated: people.

² Schectman, Joel, “The NYPD is Microsoft’s New Business Partner,” The Wall Street Journal (Aug. 8, 2012) at <https://blogs.wsj.com/cio/2012/08/08/the-nypd-is-microsofts-new-business-partner/> (last accessed Jan. 28, 2020); Joseph, George and Lipp, Kenneth, “IBM Used NYPD Surveillance Footage to Develop Technology That Lets Police Search by Skin Color,” The Intercept (Sept. 6, 2018) at <https://theintercept.com/2018/09/06/nypd-surveillance-camera-skin-tone-search/> (last accessed Jan. 28, 2020).

³ See, e.g., Report of the Finance Division on the Fiscal 2018 Preliminary Budget and the Fiscal 2017 Preliminary Mayor’s Management Report for the Office of the Chief Medical Examiner, at <http://council.nyc.gov/budget/wp-content/uploads/sites/54/2017/03/OCME-2.pdf>, at 3. (last accessed Jan. 28, 2020).

⁴ See, e.g., <https://www.manhattanda.org/da-vance-and-partners-celebrate-opening-new-manhattan-district-attorneys-office-cyber/> (last accessed Jan. 28, 2020).

Here in Brooklyn, the King’s County District Attorney’s staff includes a wide array of technical professionals with expertise in a variety of fields. For example, the KCDA has on staff a DNA analyst who not only “will assist in analyzing previous testing in cold cases and advise if additional tests are available and necessary,” but “will also review all DNA reports obtained by the Office, prepare expert witnesses and assist prosecutors in cross examining defense expert witnesses.”⁵ On the digital side, the KCDA has on staff a number of digital forensics analysts, as well as data analysts.

On the defense side, in addition to the Legal Aid Society’s digital forensic lab staff, the Public Defender Service in the District of Columbia (“PDS”)⁶ has been at the forefront of implementing this model in a defense office. PDS has two, on-staff forensic consultants, who both have advanced degrees in the forensic sciences, and are available to review casefiles in a variety of disciplines. Their presence on staff ultimately lowers the amount that PDS needs to spend on outside experts and increases the quality of PDS attorneys’ representation of their clients. Like the KCDA’s DNA analyst, PDS’s consultants assist with report review, expert witness preparation, motion practice, and cross-examination preparation.

Every defense organization should have this type of consultant on staff.

But merely hiring the people does not end the investment need. Those people, including the on-staff legal consultants on these issues like the members of my Practice, require ongoing training and licensing. Forensics and digital techniques are evolving year to year. To keep pace with the rapid rate of change, we need to maintain up-to-date training opportunities for our attorneys and specialists and to renew the licenses of any on-staff consultants we add.

Finally, any expansion of staff—even expansions as essential as these—comes with an additional cost. We must have space to seat those additional people, and to house the equipment that serves their work.

Hardware Needs

In addition to the funding disparity discussed above, the essential discovery reforms implemented this year highlight a different technology deficiency at public defender offices that pre-dates January 1, 2020. The shift to digital discovery, as well as overall greater volumes of data that we are increasingly receiving in our cases, requires hardware upgrades to allow us to effectively work with these materials.

This increase in data volume has arisen from many sources, including footage from body-worn cameras, private surveillance cameras, and “dumps” of our client’s cell phones,⁷ computer hard

⁵ <http://www.brooklynda.org/forensic-science-unit/>

⁶ Prior to joining Brooklyn Defender Services, I was a staff attorney at PDS. My description of PDS’s model is based on my personal experience there.

⁷ We are seeing a huge increase in the number of cases in which judges have granted search warrants for the phone a client has on their person at the time of arrest. We are particularly seeing these increases in situations where there is no allegation that the phone had any involvement in the crime with which the client is charged.

drives, and social media histories. We expect that these volumes will continue to increase in the future.

On top of the materials we receive from the prosecution, and consistent with our Constitutional and ethical obligations, our investigators often find and create additional materials—such as recorded interviews with witnesses or surveillance videos overlooked by the police⁸—that we also need to store and manage.

Most basically, increases in the data we receive require commensurate increases in our own data storage capacity. Brooklyn Defender Services recently added large amounts of data storage capacity with a cloud-based application, but this type of storage comes with limitations on functionality—for example, the inability to play many video and audio formats—and cybersecurity concerns that affect our ability to best utilize the materials being turned over. We, as an organization, are continuing to explore options for data storage that will meet our needs, now and in the future.

In the courtroom, we encounter additional limitations. Right now, our criminal defense attorneys do not have laptop computers, so most of our notes about appearances continue to be taken by hand (as they have been since the inception of the New York State Unified Court System), even as our cases move to an increasingly digital format. In addition, lack of laptops means that most attorneys cannot bring the voluminous digital discovery received or generated with them to court appearances.

And we find that courtrooms are not always outfitted with working technology sufficient to meet our needs. For example, a colleague of mine was recently on trial and entered a video taken by an investigator into evidence. The courtroom did not have a working DVD player. My colleague had brought a laptop with her, but it would not connect to the courtroom's projector system. She was put in the awkward position of having to borrow the prosecutor's laptop so that she could play the video for the jury.

The DA's offices routinely have courtroom presentation equipment, including laptops that connect to the courtroom's projector systems, smartboards, and speakers, that demonstrate yet another dimension of the technology gap between us.

The pace of technological change we are currently experiencing suggests to us that we will be hamstrung in effectively representing our clients unless we, and the courtrooms in which we try our cases, keep pace with technology.

Advanced data processing

Along with basic hardware needs, the move to electronic discovery—which has been appropriately accelerated by the new (and much needed) discovery statute—brings additional implementation opportunities and challenges.

⁸ Balko, Radley, "Video completely undercuts former NYPD officer about alleged assault," The Washington Post (Nov. 20, 2019) at <https://www.washingtonpost.com/opinions/2019/11/20/video-completely-undercuts-former-nypd-officer-about-alleged-assault/> (last accessed Jan. 28, 2020).

As discussed above, the volume of discovery is increasing. For example, video systems, including body-worn cameras and surveillance cameras, and digital data repositories, like cell phones and social media sites, dramatically increase the amount of discovery that a defense attorney is both constitutionally and ethically obligated to review. In a single case, an attorney may be required to review and digest hundreds of hours of video and tens of thousands of images and text messages.

A disparity also exists between the DAs and the defense community in access to robust e-discovery tools. On the civil side, many software and databasing solutions have been developed to help civil attorneys manage and process the massive amounts of digital discovery produced in complex cases. Licenses for programs of that type are extraordinarily expensive.

However, these robust e-discovery tools allow attorneys (and/or investigators) to process, organize, digest, and manage data received in discovery. Artificial intelligence, machine learning and algorithmic processing can combine to help defenders quickly identify key files, frames, or images in a case.

Additionally, e-discovery tools can also assist attorneys (and/or investigators) to visualize the data received. Data visualization tools could be essential to case presentations at trial, in hearings, or within a mitigation advocacy report, which we traditionally call a pre-pleading investigation (“PPI”), used to advocate for pleas.

As discussed above, the need for robust e-discovery tools dovetails with the importance of installing a complete data team⁹ and arming public defenders with computer science and data professionals to assist with the management and investigation of cases.

Advanced Forensics Tools

“Imagine Being on Trial. With Exonerating Evidence Trapped on Your Phone” effectively described a number of digital forensics tools and gadgets that all defense offices should have. The list of advanced forensics tools vital to the defense role is not confined to digital forensics, however.

As the article explained, an effective digital forensics laboratory set up needs to invest in both hardware and software tools that allow a consultant/analyst to extract, preserve, analyze, and report digital data, specifically cellphone data, in a usable form. These types of tools include solutions sold by Cellebrite, as well as Magnet Forensics.

⁹ It is also worth noting that defense organizations like BDS do not *only* advocate for individual defendants, but also give voice to broader community concerns. Our role in advocating for system accountability and informing policy decisions at the City and state levels would both be greatly enhanced by the establishment of a data team, with real data analytics expertise, and access to comprehensive data visualization tools. In addition, practice areas beyond our criminal practice, including immigration defense, family defense, community defense, and civil legal services would benefit immensely from these same staff members and tools.

When a case situation requires examination of records, instead of a physical device, such a lab must also have tools that allow the digesting, plotting, and visualization of cell site location information.

Additionally, our cases are demonstrating a dramatic uptick in the number of data dumps received from social media sites like Facebook. The files we regularly receive from government Facebook warrant returns are tens of thousands of unsorted pages. Such a lab must also have tools that allow the digesting and organization of social media dumps, like Magnet's Axiom tool. Currently, to deal with these disclosures, we must hire an outside expert to process the data for us. Each case consultation can cost us tens of thousands of dollars, merely to be able to *review* the disclosed materials.

Beyond data generated by cellphones and social media, defenders also now regularly receive large volumes of digital images, including photographs and screenshots. Embedded in those images is often detailed information about that image, including the precise location at which the image was created, the date and time of its creation, and the device type that created it (e.g. an iPhone or a digital camera). This "exif data" is accessible via specialized tools that allow its viewing.

Outside digital forensics and within more traditional forensic methods, the same tools and gadget needs arise. In the area of DNA analysis, defenders need access to software like GeneMapper, which is a software program that reads and displays the electronic raw data generated by DNA testing, STRMIX, which is a probabilistic genotyping software that purports to deconvolute complex mixtures and calculates likelihood ratios for case propositions, and PACE, which is a software plug-in that estimates the number of contributors to a complex DNA mixture. In the area of fingerprint and ballistics comparison, defenders need access to software like MIDEO, which provides evidence image comparison platforms and image storage. In the area of crime scene review, defenders need access to gadgets like LEICA, which creates and displays a 3-D laser scan of physical spaces like crime scenes providing more robust imaging than can be created by traditional cameras.

The set of available and necessary advanced forensic tools expands and changes every day. Defender access to up-to-date tools is essential to the defense role.

The Gap's Real Justice Cost

The technology gap is real and is growing, but its cost is hard to see in real terms. The cost redounds to expenses both monetary and social. Essentially, the true cost of the technology gap is fundamental injustice. A few examples help to demonstrate this reality:

Innocence hidden in plain sight. The sheer volume of video surveillance footage and other video footage makes imperative that participants in the criminal justice system have the support and resources to meaningfully review that footage for relevant and potentially exculpatory material.

In a recent case in our office, the prosecutor turned over body-worn camera footage from multiple officers. The prosecutor obviously had not reviewed every minute of the hours-long set of videos. Thankfully, the assigned BDS lawyer on this case had both the time and dedication to review each and every minute of that footage. That lawyer's review revealed a shocking reality: the footage from one of the officers clearly showed that the arresting officer was planting a stun gun in our client's vehicle. The case was dismissed.

In our minds, this case of uncovering a police officer blatantly planting evidence is not merely a success story, but more a warning call. What about the cases where both the prosecution and defense are deluged by surveillance footage and other forms of video discovery? There is only so much triage that defense lawyers can perform before critical evidence of a client's actual innocence is missed in a mountain of data.

Sifting the Facebook mountain. Another example of data overload in discovery are the massive dumps of Facebook pages that the prosecution has extracted from our client's social media accounts. Defense lawyers can receive dumps of 20,000 pages or more to look through; sometimes it is not known which of those thousands of pages will be entered into evidence by the government against our clients. The district attorney's office has several critical advantages in sifting through these massive data sets:

(A) The DA's office has the software to efficiently search through thousands of Facebook pages or pages from other social media sites; and

(B) The DA's office has the trained and experienced personnel to perform these searches, and then collect and organize this data for presentation at trial.

Again, there are cases and there will be cases where there is evidence of actual innocence for defendants who are falsely accused of crimes. Defense lawyers need the resources and support to find that evidence, to represent everyone zealously, and to bring evidence of actual innocence to the judge, to the prosecution and to the jury.

Innocence hidden in genetic code. Even in an area of forensics like DNA, our office has learned that extra resources and support are critical for meaningfully representing our clients. In a recent case, the OCME compared an old, incomplete profile of the client against a crime scene sample – the result was a statistic that tended to exclude the client from the DNA, but the lab still called it uninformative or inconclusive.

Our office had to contract with an outside vendor to obtain a more updated, more complete DNA profile of the client to show that he was truly excluded from the crime scene DNA. Public defender offices like ours need interpretative software to make preliminary decisions about such cases so that we can make sure that innocent clients don't slip through the cracks in the system.

Conclusion

BDS is grateful to the Committee on Justice System for hosting this critical hearing and shining a spotlight this issue. Thank you for your time and consideration of my comments. If you have any questions, please feel free to reach out Elizabeth Daniel Vasquez at (718) 254-0700 x 413 or evasquez@bds.org.



Testimony of
Sergio De La Pava
Legal Director
New York County Defender Services

Before the
Committee on Justice System
Oversight Hearing: The Technology Gap between Public Defenders and DAs

January 29, 2020

My name is Sergio De La Pava and I am the Legal Director of New York County Defender Services (NYCDS), a public defense office that represents tens of thousands of New Yorkers in Manhattan's criminal courts every year. I have been representing clients accused of crimes in this city for more than twenty years. Thank you to Chair Lancman for holding this hearing on the wide technology gap between public defenders and prosecutors.

Late last year, the N.Y. Times ran a story about the Legal Aid Society's first-in-the-nation defender technology lab. To their great credit, Legal Aid invested in achieving greater defense access to police forensic technology to improve their ability to represent their clients. This involved gaining access to forensic devices and software from companies including Cellebrite, Magnet Forensics, and Guidance Software.¹ According to the article, the unit has invested more than \$100,000 in just technology that allows defenders to make precise copies of computer drives or a person's phone and do so in a format that holds up in court. This technology is critical to preserve evidence that may exonerate an accused person. But smaller defender offices like ours, who still represent thousands of clients every year but operate on a far lesser budget, do not currently have access to such tools.

¹ Kashmir Hill, *Imagine Being on Trial. With Exonerating Evidence Trapped on Your Phone*. N.Y. TIMES, Nov. 22, 2019, available at <https://www.nytimes.com/2019/11/22/business/law-enforcement-public-defender-technology-gap.html>.

So the technology gap this hearing refers to is real. Worse, it threatens to grow over time as history tells us that reliance on technology and concomitant technological advancement are relentless. And this is especially true in the world of law enforcement and criminal prosecution. Meaning institutional defenders are not only behind but also falling more behind every day the problem goes unaddressed.

We call on City Council to address this problem, because it threatens to deny entire swaths of our most vulnerable citizens their constitutional right to due process and to the effective assistance of counsel. The Council should ensure that all of New York City's six public defense offices receive the resources we need to staff and outfit our own in-house technology units. All people accused of crimes in our five boroughs deserve to have defenders who are equipped to not only vigorously represent them in court with their legal skills, but who also have the technological wherewithal to scrutinize the prosecution's case and establish possible defenses. While the legal burden remains with the prosecution to prove our client's guilt beyond a reasonable doubt, it is our constitutional obligation to hold them to that burden in every aspect of the prosecution. This certainly includes those increasingly common instances where the police and prosecution have relied on forensic or other technology. An accused person's outcome in their case should not depend on the luck of the draw as to whether Legal Aid was in arraignment the day the case begins. Every defender office must be on equal footing in this critical area.

We also strongly believe that these technological resources must be available in-house for each individual defender office and not via a shared system. New York City relies on multiple public defender offices in part because of ethical guidelines set out in the New York State Unified Court System Rules of Professional Conduct (Rules 1.7 through 1.10) that govern conflicts of interest in legal representation. By having multiple defense providers in the courtroom at every arraignment shift, the city ensures that co-defendants each receive an attorney who is able to represent only their interests. Because of these conflicts, it would be unethical for NYCDS to go to Legal Aid and ask them to share their equipment or expertise on a case where they represent the co-defendant or where there is any danger of one of their clients being implicated or harmed in any way.

So we do not believe that an independent citywide defender technology lab is the solution to the prosecutor/defender technology gap. Such a lab invites many questions. How would the lab prioritize which cases are reviewed first? How would the lab handle conflicts involving co-defendants? Could the lab actually be independent? Would we be reluctant to have evidence tested if we thought it might corroborate the prosecution's accusations? We also expect that, like other crime labs, a technology lab would be immediately backlogged, requiring our clients to wait for long periods of time, during which our clients might be incarcerated, as we wait to secure the evidence necessary to prove their innocence.

If NYCDS had its own lab, we could prioritize for ourselves which cases are most urgent. All of the analysis would remain in house, and if evidence came back, for instance, confirming our client's guilt, we could safely share that information with our client and the without fear of that evidence coming to light in violation of our ethical and professional obligations. All of the testing, because conducted by us, would fall within the attorney-client privilege. We would not

need to negotiate with other defender offices about whose case goes first, or worry that sensitive information might come to light.

In terms of actual costs, we will be following up with a specific budget request that will detail the funding needed to be operational as soon as possible. But note that while a significant expense will be the purchasing of equipment, there will be other financial considerations. A technology unit would require constant training and staffing, not just the one-time expense of purchasing goods. But while the details need to be honed, it is self-evident that every defender office must have a significant technology budget that it is free to use as it sees fit in the best interests of its clients and to the benefit of our entire criminal justice system.

Finally, as this Committee considers securing funding for defender offices to bridge the technology gap, we also urge you to pass the POST Act (Int. 487-2018), which would require NYPD to disclose to the public the types of surveillance technology that they use against New York City residents. Passage of the POST Act would ensure that defenders know what kinds of technology NYPD relies upon so that we may consider investing in and training our staff on the same. If we remain in the dark about what kinds of technology the other side has, our criminal justice system can never truly be fair.

If you have any questions about my testimony, please contact me at sdelapava@nycds.org.



**New York City Council
Committee on Justice System**

**Hearing re: The Technology Gap Between Public Defenders and DAs
January 29, 2020**

**Written Testimony of The Bronx Defenders
By Olivia Scheck, Forensic Practice Group, Criminal Defense Practice**

Chairman Lanceman, my name is Olivia Scheck, and I am an attorney in the Criminal Defense Practice of The Bronx Defenders and a member of our office’s Forensic Practice Group.

The Bronx Defenders (“BxD”) is a public defender non-profit that is radically transforming how low-income people in the Bronx are represented in the legal system, and, in doing so, is transforming the system itself. Our staff of over 350 includes interdisciplinary teams made up of criminal, civil, immigration, and family defense attorneys, as well as social workers, benefits specialists, legal advocates, parent advocates, investigators, and team administrators, who collaborate to provide holistic advocacy to address the causes and consequences of legal system involvement. Through this integrated team-based structure, we have pioneered a groundbreaking, nationally-recognized model of representation called holistic defense that achieves better outcomes for our clients. Each year, we defend more than 20,000 low-income Bronx residents in criminal, civil, child welfare, and immigration cases, and reach thousands more through our community intake, youth mentoring, and outreach programs. Through impact litigation, policy advocacy, and community organizing, we push for systemic reform at the local, state, and national level. We take what we learn from the clients and communities that we serve and launch innovative initiatives designed to bring about real and lasting change.

I. Introduction

When it comes to forensic science, there is a huge gap in resources and information between public defender offices and prosecutors in this city. That gap leads to an imbalance that undermines our ability to adequately represent clients. Moreover, people charged with crimes who have the means to hire experts, utilize technology, and run tests receive better outcomes than those who do not. This is not justice. The Council should take action to provide public defenders with increased access to information and resources so that they can adequately represent impoverished New Yorkers facing criminal charges.

At BxD, we have established a Forensic Practice Group in order to more effectively confront and utilize forensic science on behalf of our clients. The Forensic Practice Group (“FPG”) is a group of attorneys, each of whom is responsible for conducting trainings and consulting with others in

the office on a particular area of forensic science. The specialty areas within FPG are: digital forensics, DNA, pattern evidence (e.g. ballistics and fingerprints), toxicology, false confessions and eyewitness identification. As members of FPG, our role is often to assist attorneys in identifying forensic issues and then connect them to actual scientific experts. However, retaining experts (for consultation and/or live testimony) is an extraordinarily expensive undertaking for which we do not always have adequate funding.

In addition to the expense associated with hiring experts, there are other challenges that make it difficult to effectively confront and utilize scientific evidence. In some cases, neither we, nor the available experts, have access to the technologies that are being used by law enforcement. (This is true in the context of facial recognition technology, DNA analysis, and breath alcohol testing, all of which are discussed below.) Indeed, in the digital context, we do not even have a full understanding of what technologies are being used by law enforcement.

In order to ensure that the adversarial system functions properly, we are asking the City Council to do the following:

- ensure greater transparency among police and prosecutors regarding what technologies are in use and the methodologies being employed;
- provide additional funding for defender organizations to be able to hire experts and, where necessary, purchase the technologies that are being used, and;
- in cases where it is not possible for defender organizations or independent experts to purchase the technology ourselves (for example because the manufacturers refuse to sell them to us), require law enforcement to allow independent experts access.

The widening gulf between law enforcement and defenders in access to forensic technology undermines our ability to adequately represent our clients. In what follows, we identify topics of concern in the four FPG areas where access to forensic technology is most at issue: digital forensics, DNA, pattern evidence, and toxicology.

II. Digital Forensics

In anticipation of the new discovery reforms, the Mayor's Office of Criminal Justice ("MOCJ") provided our office with some additional funding for digital forensics. This critical infusion of resources allowed us to gain access to three computer programs, and will also allow us to hire a digital analyst who will have the skills and the time to run these and other programs as needed. These improvements, which are still being implemented, will make an enormous difference in our ability to adequately represent clients.

However, there are many digital forensic technologies being used by the NYPD and the Bronx DA, that we know little about and are unable to adequately confront, such as facial recognition technology. The City Council should provide the funding for us to license these technologies ourselves and hire experts to operate them. In addition, the City Council should take action to ensure greater transparency about what technologies are being used by police and prosecutors, as well as the protocols they are employing, and to provide an opportunity for examination of these technologies by independent experts.

A. Our recent digital acquisitions demonstrate how important closing the gap can be to our clients

To understand the importance of defenders being able to access forensic technologies, it is helpful to consider the case of Chris Shaw¹, who was arrested for robbery. Mr. Shaw immediately told his attorney that he was innocent and could not have committed the crime because he was playing basketball at the time it occurred. He was able to show his attorney his location on his phone, and the attorney took screenshots from the phone to submit to the grand jury. However the Assistant District Attorney assigned to the case refused to introduce the screenshots to the grand jury without some way of authenticating them. It might have been possible to hire an expert to extract the data and present the evidence, but it could not have been done within the timeframe required to have that evidence presented to the grand jury. As a result Mr. Shaw was unable to use the cell phone data to demonstrate his innocence.

Thanks to funding provided by the City, we will soon be in a position to ensure that this situation never happens to one of our clients again. Using one of the programs that we were recently funded to purchase, we will be able to download the information contained on our clients' phones, including their location information. Our digital analyst will then be able to serve as a witness to authenticate the data in court. This is just one way in which having these new resources will allow us to better represent our clients.

In addition to the program mentioned above, which will allow us to preserve and analyze all of the information contained on our clients' phones, we have also been able to license two other programs that will help us serve our clients. One of the programs will allow us to instantly analyze call data records. The third program will allow us to organize and analyze social media records. Having access to these programs is an extremely important step towards leveling the playing field.

B. Still, more transparency and resources are needed

While acquiring these programs will greatly improve the quality of our advocacy, there are many digital forensic tools that we do not have access to and, potentially, don't even know exist. For example, the NYPD is increasingly using facial recognition software in its investigations. Without access to the software, we are unable to fully probe its reliability or access information that could be exculpatory for our clients. For example, we know that NYPD's facial recognition software can produce hundreds of possible matches, called a "candidate list," for any given input photo and also that it assigns a "confidence ratio" to each of those results.² In a case where our client has been wrongly accused, these candidate lists could contain the identity of the actual perpetrator. Yet we have never received a candidate list as part of discovery, and we would have no way of identifying these alternate suspects since we do not have access to the facial recognition technology used by the NYPD.

¹ Pseudonyms used throughout to protect client confidentiality.

² For information on facial recognition technologies, see The Georgetown Law Center on Privacy and Technology website: <https://www.law.georgetown.edu/privacy-technology-center/>

In order to effectively represent our clients, we need to be able to understand and test law enforcement's technology. This point is well-made by the example of Stingray technology, which imitates cell towers in order to intercept cell phone users' location information. Defense attorneys did not know that this technology existed until it was discovered by a hacker in California.³ Similarly in New York, the NYPD used stingrays for years in secret until it was forced to disclose their use following litigation. Once the use of Stingrays became known, defense attorneys were able to challenge it as violating the Fourth Amendment. The courts agreed and concluded that law enforcement must obtain a warrant before employing Stingrays to collect people's information. As this example demonstrates, defense attorneys cannot challenge or be prepared to confront technologies that we do not know exist.

On this point, BxD reiterates its support for the POST Act, which would require the NYPD to disclose to the public information about the surveillance technologies it uses or seeks to acquire. If we do not compel law enforcement to disclose the technologies used against our clients and fund defenders adequately so that, where applicable, we can acquire licenses and hire experts to explore these technologies, people accused of crimes will simply not be in a position to confront the evidence against them.

III. DNA

We face an unprecedented expansion of the use of DNA evidence in our clients' cases. Police and prosecutors in the Bronx now test DNA in more cases than ever before. Instruments used for DNA testing have become far more sensitive in recent years, allowing for analysis of smaller and smaller quantities of DNA. In order to keep pace with technological and operational demands in cases involving DNA evidence, we need additional resources, including **access to STRmix**, the software that is used by the Office of the Chief Medical Examiner ("OCME") to analyze DNA samples, and a staff member who can operate it.

A. Analyzing DNA mixtures is a complex task that relies on variable assumptions

Currently, much of the DNA evidence coming from the OCME involves poor quality mixtures of DNA from multiple contributors. For example, the DNA on a firearm may be from multiple different people whose DNA was deposited at different times either when various people touched the gun or when it was transferred to the gun through some other mechanism. Nevertheless, our clients face lengthy prison sentences based on OCME's analysis of this DNA.

Analyzing these mixtures in order to determine whose DNA may be present is an extremely complicated task. Indeed, analysts at crime labs were unable to analyze samples like this until a few years ago. Now, OCME uses a proprietary software known as STRmix, which was developed and marketed by a company from New Zealand to produce a statistic that is supposed to inform the court about how strongly the evidence shows whether or not a person's DNA is present in one of these complex mixtures. The software relies on advanced concepts in

³ How a Hacker Proved Cops Used Secret Government Phone tracker to Find Him, Cyrus Farivar, Politico.com: <https://www.politico.com/magazine/story/2018/06/03/cyrus-farivar-book-excerpt-stingray-218588>

computer science, mathematics, statistics, biology and probability to estimate how strong the support is for the proposition that a person's DNA is present or not.

This is far from a settled area of science. Notably, one federal court recently excluded STRmix DNA results from a criminal trial because of the degree of uncertainty in the analysis performed by the government.⁴ A New York State court excluded STRmix results in a case where the results appeared inconsistent with the results from a different software that was designed to perform the same analysis.

Experts in the field agree there is no "ground truth" or correct answer when it comes to determining how likely it is that a person contributed to a mixture of DNA. There is simply too much uncertainty in the complex analyses performed by the computer. STRmix and other similar systems can arrive at different results. Nonetheless, the statistic generated by STRmix is presented in court cloaked in the aura of infallibility associated with scientific testing.

B. To effectively represent clients in cases where DNA evidence is at issue, we need a copy of STRmix and a person who can operate it

In order to probe the reliability of the results offered by the prosecution's experts, defense attorneys need access to the same software that is used by the OCME. This is especially important since the experts who are available to consult with defense attorneys also do not have access to STRmix. Without this access, the defense cannot investigate DNA results to see if OCME's statistics should be challenged in court, or if different statistics — including statistics excluding a client — should be presented to a jury. Public defenders also need staff with training on STRmix and other software for DNA analysis, so that we can operate the technology ourselves, without always incurring the expense of hiring an expert.⁵

IV. Pattern Evidence

In the field of pattern evidence, which includes ballistics and fingerprints, the biggest challenge we face is being able to afford sufficient access to expert witnesses who can testify about the technology and methods that are being used by law enforcement. While technically the burden is placed on the prosecution to establish the reliability of the forensic evidence they are seeking to introduce in court, defense attorneys must work with experts to understand whether forensic techniques are reliable and then be able to challenge their introduction. Hiring experts in order to properly understand and litigate the reliability of a forensic discipline can cost tens of thousands of dollars. When we have sufficient resources to effectively challenge new types of forensic evidence, we create precedent others can rely on. However, when these issues are not properly litigated, it can open the floodgates to unreliable scientific evidence.

A recent Frye hearing jointly litigated by BxD and the Legal Aid Society is instructive. The first Frye hearing of its kind on the admissibility of firearms toolmarking identification evidence, it was imperative to litigate the hearing robustly. BxD and LAS were able to share the costs of the

⁴ United States v. Gissantaner, No. 1:17-CR-130, 2019 WL 5205464 (W.D. Mich. Oct. 16, 2019)

⁵ This approach has been successfully employed at the Sacramento County public defender's office, where they have a staff member with a science masters degree available to consult on DNA cases.

experts (since we represented co-defendants), and it was still only feasible because better funded public defender organizations — particularly, The Public Defender Service for the District of Columbia — had already paid for the experts to review all the relevant materials, dissect the studies, and prepare witnesses to testify. Indeed, even while sharing expert fees, it was only feasible to utilize these experts and properly litigate the admissibility of the forensic evidence properly because another organization happened to have already worked with the experts to prepare them in a different matter. Fortunately, as a result of having access to these resources, we were able to demonstrate to the court that the evidence the prosecution sought to introduce was not, in fact, generally accepted, and the court agreed that it could not be introduced at trial.

In order to ensure that we are in a position to properly litigate these issues going forward, we are asking the City Council to provide additional funding for us to be able to hire experts as these issues with new and untested technologies arise.

V. Toxicology

There is perhaps no area of criminal defense where public defenders are more hamstrung in their ability to meaningfully scrutinize scientific evidence than in the context of toxicology — in particular the use of breath alcohol test results in driving while intoxicated (“DWI”) cases. We need the help of the City Council to obtain access to the technologies that are currently being used by the NYPD so that we can adequately assess their reliability.

A. The technology gap is especially bad in Driving While Intoxicated cases

To prosecute DWI cases, DAs generally rely on the results of police-administered breath-alcohol tests. However, the manufacturers of breath alcohol testing devices, with the help of law enforcement, work hard to ensure that these devices never make it into the hands of independent experts. The result is that defense attorneys (particularly public defenders) often have no way to assess the reliability of the results that are used to convict their clients.

In November 2019, *The New York Times* published an exposé on the unreliability of commonly used breath-testing instruments and the challenges that defenders have faced in attempting to have them examined by independent experts.⁶ The *Times* concluded that these devices “generate skewed results with alarming frequency.” The report also recounted several instances in which independent experts have managed to gain access to breath-testing devices and uncovered serious problems. For example, the article notes that in 2007, the New Jersey Supreme Court ordered that defense experts be permitted to examine the Alcotest 7110, the breath test that was used by law enforcement at the time. The experts reported finding “thousands of programming errors” and the court ended up mandating “modifications” to the machine’s software in order for its results to be admissible as evidence.⁷ Similarly, in 2016, a Massachusetts court ordered law enforcement to turn over two of their Alcotest 9510 machines to defense experts for examination. The result of that investigation, which revealed glitches in the machine’s software

⁶ These Machines Can Put You in Jail. Don’t Trust Them., Stacy Cowley and Jessica Silver-Greenberg, *The New York Times*: <https://www.nytimes.com/2019/11/03/business/drunk-driving-breathalyzer.html>

⁷ State of New Jersey v. Chun, 943 A.2d 114 (N.J. 2008): <https://www.courtlistener.com/opinion/1989907/state-v-chun/>

as well as problems with the state's maintenance procedures, was the invalidation of more than two years worth of test results.⁸ As these examples make clear, breath-testing devices are not infallible and independent examination of the machines' inner-workings is necessary to ensure their reliability.

B. We need the City Council's help to be able to adequately assess results from the NYPD's new DWI breath testing device, the Intoxilyzer 9000

In late 2017/early 2018, the NYPD transitioned to using a new device for its stationhouse breath testing: the Intoxilyzer 9000, made by a company called CMI. Whereas the previous model used by the NYPD, the Intoxilyzer 5000EN, had been studied by independent experts, who published studies on potential sources of error, the 9000 has been shielded from this type of scrutiny. To our knowledge, CMI has not allowed any independent experts (who could be hired by defense attorneys) to examine the machine, attend their trainings on how it works, or review its internal programming. It appears there is only one independent expert who has been able to examine the machine and he did so over the course of only 10 hours at an undisclosed location under clandestine circumstances.⁹

This dearth of experts who have interacted with the Intoxilyzer 9000 makes it impossible for us as public defenders to adequately challenge the reliability of the results that are offered against our clients. For example, our office went to trial last year on a case where our client appeared on video to be completely sober, but registered a .10 BAC on the Intoxilyzer 9000. As it turned out, this client worked everyday with a chemical that had been shown to artificially inflate test results on a previous model of the Intoxilyzer. At the trial, we sought to introduce expert testimony regarding the possibility that exposure to this chemical had tainted the result; however, our expert was precluded from testifying on the grounds that he had never actually interacted with an Intoxilyzer 9000 and could not, therefore, testify about whether the previously-observed phenomenon was likely to persist in the 9000. The jury convicted our client on the charge that he had been driving with a blood alcohol concentration of .08 or more, based on the Intoxilyzer 9000 test result, which we were unable to controvert.

Our inability to gain access to the Intoxilyzer 9000 on behalf of independent experts prevents us from effectively representing clients and creates a high likelihood that innocent people will be wrongly convicted. To address this injustice, we are asking the City Council to facilitate access on behalf of independent experts to one or more of the Intoxilyzer 9000 devices that are currently in use by the NYPD. Additionally, we are asking that you require the NYPD to permit independent experts to attend their trainings on how to operate and maintain the machines.

VI. Conclusion

⁸ *Commonwealth of Massachusetts v. Evando Ananias, et al*, 2017 WL 11473590 (Superior Court of Massachusetts, Department of the Trial Court, Middlesex County, February 16, 2017): <https://int.nyt.com/data/documenthelper/1924-2017-commonwealth-v-ananias-decision/213c49d9b3baeabfb77c/optimized/full.pdf#page=1>

⁹ Performance Characteristics of the Intoxilyzer 9000, Jan Semenoff, *Counterpoint Journal*: https://www.counterpoint-journal.com/uploads/7/6/8/8/76880517/the_intoxilyzer_9000_iafs_2017.pdf

There is both the need and the potential for the City Council to alleviate the technology gap between public defenders and law enforcement. This can be accomplished in part through additional funding, which would allow public defenders to retain experts, license technologies (such as facial recognition technology and STRmix) and hire staff who could help us operate them. The City Council could also provide crucial assistance by requiring greater transparency from law enforcement. This means disclosing what technologies are being used, providing information about the protocols that are being followed, instructing criminalists to cooperate in providing information to defense attorneys, and, where necessary, permitting independent experts to examine technologies that are not otherwise accessible (e.g. in the case of the Intoxilyzer 9000). Only by closing this technology gap can the Council ensure that public defenders are prepared to uphold our adversarial function and effectively defend our clients.

**THE COUNCIL
THE CITY OF NEW YORK**

Appearance Card

I intend to appear and speak on Int. No. _____ Res. No. _____

in favor in opposition

Date: 1/29/20

(PLEASE PRINT)

Name: Jerome Greco

Address: _____

I represent: Legal Aid Society

Address: 49 Thomas Street, New York, NY 10013

**THE COUNCIL
THE CITY OF NEW YORK**

Appearance Card

I intend to appear and speak on Int. No. _____ Res. No. _____

in favor in opposition

Date: _____

(PLEASE PRINT)

Name: Elizabeth Vasquez

Address: _____

I represent: Brooklyn Defender Services

Address: 177 Livingston Street, Brooklyn

**THE COUNCIL
THE CITY OF NEW YORK**

Appearance Card

I intend to appear and speak on Int. No. _____ Res. No. _____

in favor in opposition

Date: 1/29/2020

(PLEASE PRINT)

Name: Sergio De La Pava

Address: 100 William St.

I represent: New York County Defender

Address: Services

◆ Please complete this card and return to the Sergeant-at-Arms ◆

**THE COUNCIL
THE CITY OF NEW YORK**

Appearance Card

I intend to appear and speak on Int. No. _____ Res. No. _____

in favor in opposition

Date: _____

(PLEASE PRINT)

Name: Joorge Camacho

Address: _____

I represent: Mayor's office of Criminal Justice

Address: 1 Centre Street, 10th Floor

**THE COUNCIL
THE CITY OF NEW YORK**

Appearance Card

I intend to appear and speak on Int. No. _____ Res. No. _____

in favor in opposition

Date: _____

(PLEASE PRINT)

Name: Scott Matthews-Novelli

Address: _____

I represent: Mayor's office of Criminal Justice

Address: 1 Centre Street, 10th Floor

**THE COUNCIL
THE CITY OF NEW YORK**

Appearance Card

I intend to appear and speak on Int. No. _____ Res. No. _____

in favor in opposition

Date: 1/29/20

(PLEASE PRINT)

Name: Olivia Schuch

Address: _____

I represent: The Bronx Defenders

Address: 360 E 161st St, Bronx, NY 10451

Please complete this card and return to the Sergeant-at-Arms