Criminal Law Practitioner

Volume 2 | Issue 2 Article 13

2015

The Fourth Amendment in the Digital Age Symposium

Braxton Marcela
American University Washington College of Law

The Fourth Amendment in the Digital Age Symposium

by: Braxton Marcela[1]

On April 3, 2015, the National Association of Criminal Defense Lawyers and American University Washington College of Law's *Criminal Law Practitioner* hosted a symposium entitled **"The Fourth Amendment in the Digital Age,"** which featured various practitioners and policy experts to discuss the growing digital and technological advancements and the impact they will have on the Fourth Amendment protections, national security, and criminal justice. Claudio Grossman, Dean of the American University Washington College of Law, which hosted the event, began by noting that privacy is a right recognized by international covenants and custom. The current President of the National Association of Criminal Defense Lawyers, Theodore Simon, followed stating that the goal of the symposium was to explore how government surveillance programs, digital searches, etc. are impacting the Fourth Amendment in practice, and guide those "on the front lines" of criminal defense. He further stated that "Electronic surveillance and digital searches go to the heart of the Fourth Amendment and fundamental freedoms, including how citizens are investigated, charged, and tried. It directly impacts criminal defenders' work to represent their clients.

Panel 1

The symposium's first panel, entitled **"New Developments in Surveillance Technology: How the Government Collects, Searches, Stores, and Shares Information,"** focused on the technological advances that law enforcement, both state and federal are currently utilizing to investigate crimes and monitor suspects. It also included an in-depth discussion of how the legal system has adapted to new technologies and the implications they have for criminal defense. It was moderated by Jennifer Daskal, an Assistant Professor of Law at AU WCL. Panelists included Catherine Crump, an Assistant Clinical Professor of Law at the University of California at Berkley School of Law and the Associate Director, Samuelson Law, Technology and Public Policy Clinic, also serving as counsel to the American Civil Liberties Union in their challenge to the NSA metadata collection programs; Liza Goltein, Co-Director of the National Security Project, Brennan Center for Justice; Joseph Lorenzo Hall, Chief Technologist, Center for Democracy and Technology; and Eric Winger, Director of Cybersecurity and Privacy Policy for Global Government Affairs at Cisco Systems.

Daskal introduced the panel by stating that there has been a "tectonic shift" in how data is collected, stored, and used, and asking Hall to elaborate on the newer technologies the State currently utilizes to investigate and monitor suspects. Hall responded stating that surveillance has ballooned extraordinarily, going

1 Braxton Marcela is a rising 2L at American University Washington College of Law and is the incoming Associate Publications Editor for the Criminal Law Practitioner. His primary interest is criminal law, as well as secondary interests in national security law and immigration law. He is originally from North Carolina.

from being as passive as mere eavesdropping to assertive muscular data collection and storage. Surveillance has moved from being targeted to increasingly bulk—and "shockingly intrusive." Hall even cites an example of a quantum program that can "cut a hole" in a user's computer browser and collect passwords, keystrokes, and other data. He particularly notes that the NSA was using mass metadata collection long before the tech industry caught up to it. Hall cited a main severe that arises from these problems is the amount of false positives, or targeting people that should not be targeted, data targeting can implicate others who would not otherwise be implicated simply by nature of proximity or "being on the same train."

After Hall's overview, the panel began discussing the legal system's adaptation to the mass surveillance technologies. Goltein began by saying there has been a sea change in the law moving in favor of mass surveillance. Most troubling to the panel was the seeming eroding of the traditional "golden rule" that surveillance of a target required reasonable *suspicion* of criminal activity. This change begins with Section 215 of the United States of America Patriot Act,[2] which allows the government to get a Foreign Intelligence Surveillance Act (FISA) Court order for information on an individual based on *relevance* to a criminal act. The FISA Court interpreted the statute broadly. Secondly, Section 702 of the FISA Court Amendments Act of 2007[3] Congress removed requirement of individualized suspicion of wrongdoings for any foreign target overseas and in America. Finally, Executive Order 12333—most expansive of government authority—allows surveillance companies to collect foreign intelligence without any judicial involvement. Goltein also asserts that these changes make the distinction between foreign and domestic targets a legal fiction. Particularly, the government assumes if it has no information about a target, it is probably foreign. The government has also utilized backdoor searches, in which they use foreign targets to locate American citizens attached to a foreign target. The NSA used this method over 2,000 times against American citizens. The data ended up being used in local criminal prosecutions and by local government agencies throughout the country.

Crump also further elaborated on the surveillance technologies being used on the local level to monitor and investigate suspects. Crump stated there is a "pot of money" available to local police departments to access surveillance technology such as "Stone Gardens," a technology putting cameras and audio recorders in rocks, as well as "sting ray" devices which attach to a car, and license plate readers. Additionally, automatic license plate readers can take pictures of every car and enter the pictures into a larger database; aerial surveillance drones can track suspects and cars; local police departments track suspects on social media, as well as additional biometrics technology that has been used by local police departments. Further, localities have been able to pursue and arrest suspects at the local level based on nationally collected data.

Both Goltein and Crump also assert that the Fourth Amendment is not seen as an adequate protection against these procedures. Particularly, the Fourth Amendment's reach is constricted by the "foreign intelligence exception," which is being both expanded and frequently invoked, as FISA courts have applied it broadly, ignoring prior courts' insistence that the target be a foreign national or foreign government. Particularly, according to Goltein, once the government identifies a foreign target, they take the opportunity to monitor and investigate all people in that individual's network. Goltein also cites the "Third Party Doctrine," which traditionally holds that when an individual transfers data to a third party, such as a telephone company, then there can be no expectation of privacy and the government can use the phone company's data on that individual. However, the panel noted that the "Third Party Doctrine" is eroding in courts and eventually may be replaced. Subsequent panels also confirmed this. On the subject of the

2 115 Stat. 272, §215.
3 154 Cong. Rec. H. 5743, §702.

Fourth Amendment, Crump is more optimistic about the Fourth Amendment providing a remedy to mass surveillance and intrusion. In particular, she *cites Riley v. California*,[4] in which the Supreme Court held there is a difference between digital data and other personal effects that can be searched in their decision prohibiting a search of a suspect's cell phone pursuant to arrest. She also cited Justice Alito's concurring opinion in *United States v. Jones*,[5] which seemed to give some credence to importance of curtailing long-term surveillance of individuals and more protection. Crump also notes that there have been some state and local level victories invoking the exclusionary rule against advanced forms of technological surveillance.

Winger evaluated on companies involved in mass surveillance and how they have responded to the government's increased use of surveillance. He notes that the problem is largely a result of the public's general trust in the internet and companies such as Twitter, Yahoo, Google, and other companies. The economic and social reliance on the internet and the trust people place in its technologies empower and encourage data collection. However, some companies and providers are mounting legal challenges to data collection policies. These companies are particularly hoping to set a framework that can protect data and make surveillance more targeted and set a distinction between the content of individuals' calls and the metadata of calls held by the companies. Crump noted the companies' lawsuits as well, noting that it is encouraging that companies are starting to concern themselves with restricting data collection.

The panel ended with a discussion of the main challenges and important considerations panelists feel are important to practitioners. Hall noted that attorneys need to know what the government is doing, but also how network security and network operations work. There is a general need to invest in teaching attorneys how the technology works. Goltein states that attorneys' priorities should be identifying the stakes and the risks, as well as combatting the perception that the United States government won't misuse its national security power in its surveillance of Americans. She notes additionally that the slowness of American public opinion and the judiciary is much slower than the pace of technological development. Winger notes that attorneys should focus on broader debate about the scope of authorities that exist beyond the statutes that we have, particularly as it relates to trust between Americans companies, other nations and the US government. Crump concurs alleging that expanding the debate and expanding the public's education of the technology that is out there and its impact on both national security and criminal justice will be essential to addressing the various concerns involving mass surveillance and collection of suspects' data.

Panel 2

The second panel, entitled Challenges to the System: Prosecutors, Judges, and Defense Attorneys in the Digital Age, moderated by Gerry Morris, Esq., President-elect of the National Association of Criminal Defense Lawyers, focused on how digital surveillance and new technologies were directly impacting practitioners in the field. It featured Hanni Fakhoury, Senior Staff Attorney, Electronic Frontier Foundation; Neema Singh Guliani, Legislative Counsel, American Civil Liberties Union; Jim Harper, Senior Fellow, CATO Institute; Orrin Kerr, President and CEO, National Constitution Center, Professor of Law, George Washington University Law School.

Morris opened by asking the panel for general opening statements on the subject. Kerr began by asserting that *Riley v. California*[6] is a very good decision from the perspective of a defense attorney and should provide optimism about the judiciary's trust and allowance of digital surveillance. However, he also notes that the Courts have restricted the exclusionary rule further; thus, from a rights standpoint, the

4 134 S. Ct.1870 (2014).

5 132 S. Ct. 945 (2012).

6

rights are expanding, but this expansion will not likely benefit or aid clients. Harper also asserts that rights are expanding, particularly because the "reasonable expectation of privacy standard," originally set by *Katz v. United States*,[7] is slowly dissipating. A majority opinion of the Supreme Court has not cited to it or based a major decision off of it. Although attorneys can and probably should argue the "reasonable expectation of privacy" argument, it may be more relevant and practical for attorneys to argue a statutory-type, line-by-line analysis of whether there was indeed a search or seizure and then whether it was reasonable. Harper analogizes the standard to a mailed letter—when a letter is put in an envelope, one can reasonable expect the contents to be private, yet it can be more simply argued that opening the letter is a search/seizure, and property rights make opening it unreasonable. Harper further argues that this is likely good for defense practitioners and their attorneys, especially because this style of analysis can be analogously applied to the internet. He states that although the analysis is are very fact-specific, it will restore application of Fourth Amendment on its terms sufficient to protect privacy rights.

Singh opened by pointing out that there is a "bizarre tension" in federal government. Although government is unable to keep up with growing technology, as current debates over surveillance technologies involves technology that is a decade old, the federal government is very good at getting this technology to state and local law enforcement technologies. She advocated a federal policy that policy prohibits the federal government from asking states/localities to hide or conceal use of surveillance technologies. For example, she states that the Department of Justice has asked prosecutors and police departments to cite "confidential sources" in cases, offer plea deals before challenges to evidence arose, or dismiss cases involving data collected via certain surveillance devices. The goal of these directives is to directly keep information on surveillance technologies away from judges. She also states that Congress needs to exert further oversight over federal funding of surveillance technologies by local governments, describing the Department of Justice's grants as a "blank check." She sees the main problem being that Congress does not act on privacy concerns until there is a problem, leaving them "fifteen to twenty years behind." For Singh, an expansion of congressional oversight and regulatory change from the Department of Justice is crucial to addressing the Fourth Amendment as we move through the digital age.

Fakhoury opened by saying the important thing to remember about surveillance and privacy issues is that they are universally occurring in the criminal justice system throughout the nation. For example, he cites a judge in Baltimore who asked a police officer to disclose information about a stingray device, and the prosecutor decided to interrupt the questioning and concede on a motion to suppress evidence collected by the device. Fakhoury says that defense attorneys should value stories and "wins" such as this because they allow attorneys to say "We're not crazy. This is an actual problem." He particularly encourages each defense attorney to seek their "Riley Moment," named for *Riley v. California*,[8] which he identifies as the moment which shows the existence of a search/seizure using intrusive technology. Fakhoury states four reasons why *Riley* is very significant to defense practice, particularly when it comes to digital search and surveillance: 1) Court did not feel they had to apply the *Robinson v. United States*[9] decision allowing containers in proximity to arrestee incident to arrest; (2) quantitative and qualitative difference between cell phone [and phone data] and other items that can be searched incident to arrest; (3) cell phone data goes back to even before you bought the phone; and (4) phones are so pervasive in society now that they justify higher scrutiny than other levels. He states that the best practice coming from *Riley* and other cases that have challenged digital searches and surveillance is to frequently and actively make discovery requests and vigorously ask questions, both in

7 389 U.S. 347 (1967).
8
9 414 U.S. 218 (1973).

court and to the prosecutors, about where certain information is coming from and what technology is being used. He advocates this course particularly, because of his belief that the reliability of evidence gathered by digital or technological surveillance should be as relevant to the proceeding as evidence gathered from other less intrusive and more arcane means.

Panel 3

The third panel was entitled, **Law and Policy: A Path Forward for the Constitution, Courts, Congress, and Law Enforcement**, and was moderated by Jeff Rosen, President and CEO, National Constitution Center, Professor of Law, George Washington University Law School. It featured Ahmed Ghappour, Visiting Professor at the University of California Hastings College of the Law, and Director or the Liberty, Security and Technology Clinic; David Lieber, Senior Privacy Policy Counsel at Google; Greg Nojeim, Senior Counsel and Director of the Freedom, Security and Technology Project at the Center for Democracy and Technology; and Kenneth Wainstein, Partner at Cadwalader, Wickersham & Taft LLP, Former Homeland Security Advisor, Former Assistant Attorney General for National Security, and Former United States Attorney for the District of Columbia.

Rosen began the discussion by asking each panelist if it would be constitutional for President Barack Obama to announce a policy involving multiple miniature drones that would ubiquitously and continuously monitor and survey regular citizens and keep data that could be accessed by national security agencies and law enforcement. Ghappour claims that it depends on the particular scope of the program, the size of the drones, the types of surveillance, and the storage of the data. However, he was quick to highlight that there are some forms of ubiquitous surveillance in many public areas already. Ghappour also cites the First Amendment as a barrier to twenty-four hour drone monitoring, as such surveillance would cause people to self-censor their words, activities and associations, which would violate the First Amendment. Lieber says that such a policy would not be constitutional, as "the Fourth Amendment protects people not places." Throughout this panel, each panelist once again reiterated that the "reasonable expectation of privacy test" is likely to be abandoned as a means of Fourth Amendment analysis. Nojeim is also very skeptical of the twenty-four hour drone policy, particularly as it deviates from the court's holding in *Jones*, which held that a twenty-eight day surveillance using a GPS tracking violated the 4th Amendment. Wainstein also claimed the twenty-four hour drone surveillance would be likely unconstitutional because of the rule in Jones.

In addition to answering this particular question, the panelists expressed some reason to be optimistic about Courts' handling of surveillance in the digital age. Nojeim relied particularly on *Jones* for this optimism. Most notably, no justices accepted the government's view that driving on public roads removes an individual's reasonable expectation of privacy. Further, Nojeim claims that the *Jones* opinion signals the judiciary's awareness of privacy rights and an inclination towards greater protection. Wainstein concurred on the claim that the Court post-*Jones* will be more protective of privacy rights, especially because of the slippery slope argument that is very pervasive in the legal questions about surveillance. In addition to the *Jones* opinion, Nojeim cites three additionals reasons to be optimistic about Court's and lawmakers' future handlings of surveillance and technology: (1) SCOTUS embrace of the notion that technology is changing the nature of privacy and it is insufficient to apply less advanced technologies that don't include as large an amount of data—for example, the holding in *Riley* based, in part, because cell phones are different in that they store such a large amount of data; (2) business has emerged as a key constituency by engaging in the privacy debate in a way that they had not in previous years, including filing suits to protect consumers' data; and (3) there is increasing ease with which we can encrypt and protect data. Wainstein disagrees with the idea that data encryption will

hinder or curtail mass surveillance. However, he is concerned that mass encryption of certain types of data will make it harder to prosecute certain suspects and will put an amount of valuable data outside of the reach of law enforcement. Particularly he is concerned that, because of encryption, the government may go through the process to obtain a warrant for necessary information about a suspect, but such data will be unavailable because of encryption.

Wainstein, the symposium's only prosecutor, brought an interesting perspective to the discussion by speaking of the rationales behind surveillance and collection of data. He asserts that there are practical applications that justify the collection and the use of mass data. Particularly, he cited a list of names on a plane as a type of data. If there was a suspected or alleged terrorist on the boarding list of the plane, the government and the general public would want the government to be able to upload the flight's manifest and read through the list of passengers to thwart any possible terror plot. Nojeim questioned this hypothetical on the grounds that the other passengers, who had done no wrongs, will have still suffered a violation of their Fourth Amendment rights. He further stated that the Federal Bureau of Investigations is not required, by rule or statute, to destroy data collected on innocent persons, making violations of the Fourth Amendment against the innocent people on the flight list more likely.

The panelists further discussed what policy and legislative changes may possibly await the ongoing debate about surveillance and law enforcement, especially as the USA Patriot Act, Section 215 is set to expire in May. Wainstein points first to Congress, yet says that it is unlikely that Congress will significantly change the current surveillance regimes, as it is atypical for members of Congress to buck the Executive Branch on matters involving national security, including surveillance and technologies. For example, Wainstein does not expect the Patriot Act to be restored in its current terms after it expires. Lieber is more optimistic on Congressional action, citing the upcoming expiration of Section 215 of the Patriot Act as a reason to be optimistic. He claimed that there will be considerable pressure on lawmakers to tailor a new statute that takes into account considerable privacy concerns from privacy advocates, as well as private companies. Lojeim theorizes that the involvement of business as a constituency in privacy matters may further assist the search for a legislative solution to these issues. Overall, while there will be pressure on Congress to closely scrutinize and revise policies around surveillance, yet very intelligent minds differ on the likelihood of significant change. The panel was in general agreement that surveillance policies will be greatly impacted by shifts in the courts' interpretations of privacy, private companies' resistance to certain policies, and political pressures on Congress.

Conclusion

After the three panels, it was very clear that there are a series of complicated issues involved in the government's digital surveillance and monitoring practices. It is also very clear that there are significant problems that defense attorneys must address in order to adequately represent their clients. Moving forward from the symposium, it does seem as if there is reason to be optimistic, yet there must also be an awareness of the challenges and the difficulties involved in creating substantive change. If defense attorneys continue to educate themselves and their clients and advocate, both in courts and in Congress, the goals of the symposium and the goals of criminal defense in the digital age would surely be furthered. For more information, the symposium is available on-line from C-SPAN at http://www.c-span.org/search/?searchtype=All&query=Fourth+Amendment+and+Technology.

About the AUTHOR

Braxton Marcela is a rising 2L at American University Washington College of Law where he serves as the Associate Publications Editor for the Criminal Law Practitioner. Braxton also serves as a Senior Staffer on the National Security Law Brief. Additionally, he is Political Affairs Chair for the WCL Latino Law Students Association and the Political Director for the WCL Democrats. Prior to attending law school, he completed his Bachelor's degree at Hampden-Sydney College, where he double-majored in Government and Spanish. He formerly served as a Diamond Summer Intern at the American Israel Public Affairs Committee and worked as a field staffer for President Obama's 2012 campaign. He has always had a passion for public service and criminal law. After completing law school, he hopes to return to North Carolina and seek a career in criminal prosecution.