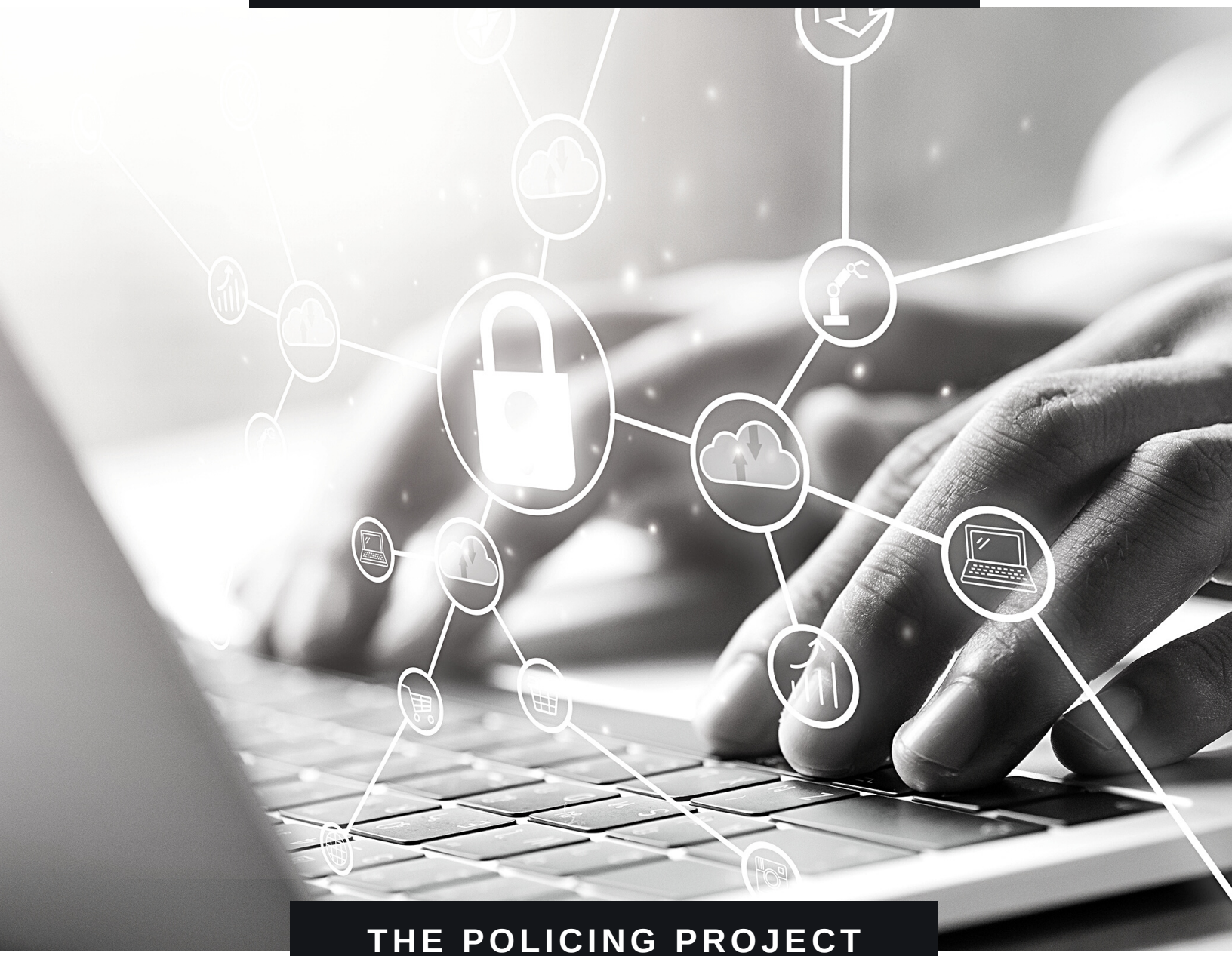
TUESDAY, MARCH 16, 2021

CONVERSATIONS ON POLICING TECH:

TRANSPARENCY ISSUES IN ELECTRONIC SURVEILLANCE

2020-2021 SALON SERIES



THE POLICING PROJECT

About the Policing Project Salon Series

As part of our ongoing work to help promote the ethical use of policing technology, the Policing Project is hosting a series of closed-door salons to work through some of the most difficult questions we face. Made possible through support from Microsoft, the salons enable us to vet our projects and discuss pressing issues around law enforcement's use of technologies with a diverse set of experts, including privacy advocates, technology vendors, police chiefs, academics, legal experts, community leaders, and government officials.

About the Policing Project

We partner with communities and police to promote public safety through transparency, equity and democratic engagement.

Our work focuses on front-end, or democratic, accountability — meaning the public has a voice in setting transparent, ethical, and effective policing policies and practices before the police or government act. The goal is to achieve public safety in a manner that is equitable, non-discriminatory, and respectful of public values.

For more information, visit **www.PolicingProject.org**

The report was written by Policing Project Staff Attorney Katie Kinsey and Student Fellow Claire Groden.

Event Description and Review

As Americans increasingly conduct their lives online, the technology companies that own these digital platforms have become de facto warehouses of personal information. This information includes intimate details about people, from their financial habits, to their relationships to others, to their movements. This trove of digital information has not escaped the notice of law enforcement, whose requests to electronic service providers for user records and information have been steadily on the rise. These law enforcement requests can set up an awkward dynamic for tech companies – making them active participants in law enforcement processes and gatekeepers of user information. They also entirely cut out the individual citizens whose information actually is implicated by these requests. Yet, at the moment, it is hard even to evaluate the informational dynamics of these law enforcement requests because they often are hidden from public view via gag orders or other secrecy measures. As part of our Tech Salon Series, the Policing Project invited experts from diverse backgrounds—including representatives from the tech industry, academics, civil liberties advocates, prosecutors, and members of law enforcement—to discuss transparency issues with law enforcement requests to internet and digital providers for customer digital information.

Hosted by **Policing Project Faculty Director Barry Friedman** and **Texas A&M Associate Professor of Law Hannah Bloch-Wehba**, the salon sought to parse out what we actually know and still need to learn about these requests.

Discussion Overview

To start, participants confirmed both that there has been a rise in law enforcement requests for information to digital service providers, and that secrecy has become the norm for these requests. Several reasons were offered to explain these trends. As to why there's been an increase in requests for electronic surveillance, one participant offered a simple explanation: that's where the information lives. As people conduct their personal and professional lives online, digital data has become the dominant informational currency. Law enforcement representatives confirmed this explanation and added that they merely were following the lead of individuals who increasingly use the internet and digital tools to perpetrate and conceal criminal activities. Although agreeing that necessity accounted for some portion of the increase, others attributed the rise to the relative ease with which digital information can be obtained and organized—it comes in an indexable and searchable format—as compared

to physical or analog evidence. In addition, electronic surveillance involves fewer investigational risks than physical surveillance: previously, accessing information about the target of an investigation, such as through a physical search, could risk tipping off the target to the government's scrutiny. By contrast, with electronic surveillance, law enforcement agencies now can access information about targets from third-party providers in the early stages of an investigation without making any observable contact with the target. There was debate about whether the cost of electronic surveillance contributed to its prevalence, with some in law enforcement arguing that electronic surveillance actually could be more expensive than its physical equivalent.

There also was general agreement that secrecy has become business as usual for law enforcement requests to digital providers. Explanations for this culture of secrecy varied. One government official emphasized that secrecy simply is necessary for certain investigations, such as cybercrimes, in which investigators often may not know the targets' identities. In these cases, if the targets are tipped off to an investigation, the anonymity of the internet enables individuals to disappear and forces investigators back to square one. Still, several participants emphasized that this secrecy often arises from institutional or administrative inertia rather than necessity. In other words, secrecy has become the default setting even when the integrity of the investigation does not require it. For example, some jurisdictions' rules allow requests for e-surveillance to remain sealed indefinitely unless prosecutors affirmatively move for unsealing, which creates friction to obtain transparency. Several participants also highlighted the role played by investigators' use of model forms containing boilerplate requests for secrecy – a sort of copy-and-paste directed secrecy.

Next, participants were asked to consider what harms flow from this secrecy to various stakeholders, including criminal defendants, the judiciary, and legislative bodies. Almost all participants agreed that the harms were significant and spread across these diverse actors and institutions. For defense attorneys and advocacy groups, the use of gag orders means they lack insight into how law enforcement agencies may be developing novel uses for electronic surveillance, thus interfering with their ability to bring constitutional challenges to these practices. For judges, secrecy can hamper professional knowledge exchange as judges are forced to operate in a vacuum, unable to see how their peers are interpreting the law in sealed orders. At the policy level, secrecy means that legislators, including Congress, are hamstrung in understanding—and therefore addressing—the scope and contours of the issues presented by these requests.

Finally, participants turned to potential solutions to the prevalence of secrecy in electronic surveillance. One suggestion endorsed by many participants was for jurisdictions to

examine their unsealing practices and reset the default rule if necessary. For example, some judicial districts, such as the District of Arizona, unseal surveillance applications after a set period unless law enforcement agencies move to maintain the sealing order. This practice would cut against the institutional inertia that keeps surveillance requests and orders sealed indefinitely by default. Other suggested giving advocates more tools to defend customers' privacy interests, such as by allowing advocates to step in on behalf of targets' privacy in an amicus process modeled after the Foreign Intelligence Surveillance Act (FISA). Perhaps the most widely supported solution was the publication of aggregate surveillance order data, which would help Congress and the public better understand the volume and nature of law enforcement agencies' request to third parties for information. One participant urged Americans to take a page from countries like Britain and Belgium that have established independent privacy and civil rights oversight boards to track and report out these surveillance concerns. To cap off the session, at least one participant urged that a comprehensive response to the prevalence of electronic surveillance secrecy will require the deployment of all of these solutions. No matter the solution, there was significant agreement that the status quo has to change from a climate of secrecy to a culture of transparency. Barely regulated law enforcement access to people's digital information cannot remain the default setting.

LIST OF ATTENDEES

Roy Austin, *Vice President of Civil Rights and Deputy General Counsel*, Facebook

Sue Glueck, *Senior Director of Academic Relations*, Microsoft

Jennifer Granick, *Surveillance and Cybersecurity Counsel*, American Civil Liberties Union

Jerome Greco, *Supervising Attorney*, Digital Forensics Unit, The Legal Aid Society

Justin Herdman, *Partner*, Jones Day; former *U.S. Attorney*, Northern District of Ohio

Travis LeBlanc, *Partner*, Cooley LLP; *Board Member*, Privacy and Civil Liberties Oversight Board

Aaron Mackey, *Staff Attorney*, Electronic Frontier Foundation

Brian Owsley, *Assistant Professor of Law*, University of North Texas at Dallas College of Law

Riana Pfefferkorn, *Research Scholar*, Stanford Internet Observatory; former *Associate Director*, Surveillance and Cybersecurity, Center for Internet and Society

Timothy Plancon, *Assistant Administrator and Chief of Operational Support*, Drug Enforcement Administration

Monica Ryan, *Assistant U.S. Attorney*, District of Arizona

Roger Rogoff, *Legal Affairs*, Microsoft; former *Judge*, King County Superior Court

Richard Salgado, *Director*, Law Enforcement and Information Security, Google

Chris Soghoian, *Senior Advisor for Privacy & Cybersecurity*, Office of Senator Ron Wyden

Aravind Swaminathan, *Global Co-Chair*, Cybersecurity and Data Privacy, Orrick, Herrington & Sutcliffe LLP; former *Assistant United States Attorney*, Western District of Washington

James Vinocur, *Deputy Chief*, Cybercrimes and Identity Theft Bureau, Manhattan District Attorney's Office

Stephen William Smith, former *Magistrate Judge*, U.S. District Court, Southern District of Texas; former *Director of Fourth Amendment & Open Courts*, Center for Internet and Society

Andrew Weissmann, *Distinguished Senior Fellow and Adjunct Professor*, NYU School of Law; former *Chief*, Fraud Section, U.S. Department of Justice; former *General Counsel*, Federal Bureau of Investigation

HOSTS

Hannah Bloch-Wehba, *Associate Professor of Law*, Texas A&M University School of Law

Barry Friedman, *Faculty Director*, Policing Project; *Jacob D. Fuchsberg Professor of Law and Affiliated Professor of Politics*, NYU School of Law

Farhang Heydari, *Executive Director*, Policing Project, NYU School of Law

Katie Kinsey, *Staff Attorney*, Policing Project, NYU School of Law