The New York Times

I'm a Judge. Here's How Surveillance Is Challenging Our Legal System.

Prosecutors have stepped into the void left by Congress's failure to say how far the police can go in using investigative technology.

By James Orenstein
Mr. Orenstein is a federal magistrate judge.

June 13, 2019

On most weekdays in the federal courthouse in Brooklyn, prosecutors will ask the magistrate judge on duty to issue lots of sealed orders authorizing them to use all sorts of investigative technologies or requiring technology companies to keep tech-based searches secret.

But that typically won't happen when I'm the judge on duty. When it's my turn, the docket gets awfully quiet as prosecutors wait for another judge. That's not because the prosecutors or other judges are doing something they shouldn't. It's because prosecutors think they'll stand a better chance of getting what they want from another judge. This waiting game is a symptom of how new surveillance technologies are challenging a legal system that hasn't figured out how to handle them. (The views here are my own, not those of the federal courts.)

Congress is way behind in determining how far the police can go in using technology to invade people's privacy, and many of the legal disputes arising from this collision have not reached the Supreme Court. For the public, as a practical matter, the rules of the road are being decided by prosecutors. Your privacy is not their highest priority.

Here's an example. Last summer, the Supreme Court decided in Carpenter v. United States that when the police want to get records of a mobile phone's prior locations over extended periods — basically, to track a suspect's whereabouts at every moment over weeks or months in the past — the Constitution requires them to persuade a judge to issue a warrant based on probable cause. But for several years before that, savvy prosecutors were able to proceed without a warrant by seeking out judges they thought would rule their way. This tactic helped delay the legal question from reaching the Supreme Court for years.

Those decisions are best made in Congress, but if Congress fails to do so, judges should at least hear opposing views and give a public account of the reasoning behind their decision. These choices should not be left to the secret deliberation of a judge, handpicked by prosecutors, who sits on the lowest tier of the judiciary.

And ultimately, that's the problem: A Congress that has failed to keep pace with the times, not prosecutors aggressively using new technological tools. Congress has not enacted any thorough updates of the digital privacy laws that govern law enforcement investigations since the early days of the internet — long before we entrusted virtually every bit of information about our lives to our electronic devices and to the cloud. (That's why the Justice Department relied on a law written in 1789 when it tried to force Apple to help search an iPhone by disabling the device's password protection. I ruled against the government in that case.)

It is impossible to measure the cost in privacy losses and years spent behind bars suffered by people who could have successfully raised the issue decided in the Carpenter case if it hadn't taken so many years to reach the Supreme Court. It is likewise impossible to know how many investigations and prosecutions have been stymied because prosecutors lacked clear rules and could not take the risk that a particular investigative technology could undermine an important case.

If Congress won't write laws for this century's technology, courts must craft rules that ensure a fair and orderly review of new investigative methods. For example, the Foreign Intelligence Surveillance Court (which also confronts the tension between effective investigations and privacy) has a system for bringing in independent lawyers called "amici curiae" to argue novel or significant legal issues that occasionally arise when the government asks for technology-based surveillance orders. Those amici can argue in favor of the target's presumed privacy interests but don't represent him and can't give him information about the investigation.

Magistrate judges occasionally do the same on an ad hoc basis, but in those cases the amici don't have the same access to information as is allowed in the surveillance court, and, like the amici there, they can't appeal a lower-court ruling. Giving these independent lawyers the information they need to argue about the legality of novel law enforcement requests, as well as the right to appeal, would at least provide for a more balanced assessment of new surveillance technologies and a quicker way for questions about them to be decided on a national basis.

I don't presume that any of my rulings have struck the right policy balance between law enforcement and personal privacy. That's not even a question a judge like me should try to answer. But as the pace of technological advancement increases, the need becomes more