Every Corrupt Politician, Operative and Silicon Valley Campaign Financier Has Been Recorded Since 2007

- Every Email, Every Phone Call, Every Credit Card Transaction, Every Text, Every Voice-mail, Every toll booth transit, every restaurant conversation..everything that the Obama financiers did to break the law...is now held in archives by over 6 different law enforcement entities.

- They WILL be caught.

- Eric Schmidt's, Elon Musk's and John Doerr's election and government contract rigging fully documented

- Says a top DHS official: "Only a fool thinks that the entire contents of their company and personal email and files have not been hacked by now if they were involved in politics..."

- Revelation of all of the crimes is only one subpoena, one whistle-blower, or one hacker, away from becoming national news

U.S. courts: Electronic surveillance up 500 percent in D.C.-area since 2011, almost all sealed cases

By Spencer S. Hsu and Rachel Weiner

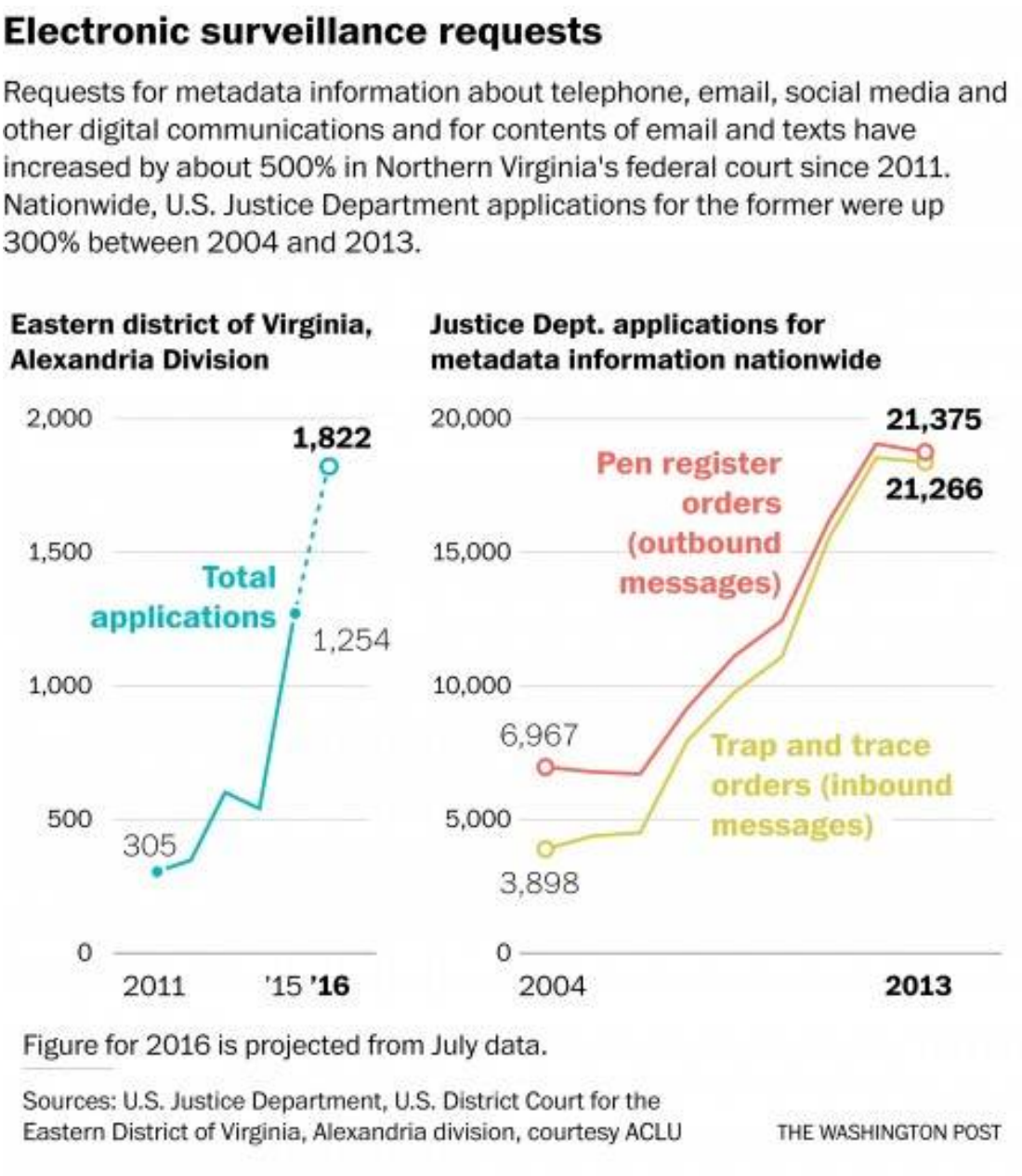
Secret law enforcement requests to conduct electronic surveillance in domestic criminal cases have surged in federal courts for Northern Virginia and the District, but only one in a thousand of the applications ever becomes public, newly released data show.

The bare-bones release by the courts leaves unanswered how long, in what ways and for what crimes federal investigators tracked individuals' data and whether long-running investigations result in charges.

Yet the listings of how often law enforcement applied to judges to conduct covert electronic surveillance — a list that itself is usually sealed — underscore the exponential growth in the use of a 1986 law to collect data about users' telephone, email and other Internet communications.

[Federal judges balking at law enforcement requests for electronic evidence]

Unsealing basic docket information "is an important first step for courts to recognize that they have been enabling a kind of vast, secret system of surveillance that we now know to be so pervasive," said Brett Max Kaufman, a staff attorney at the ACLU's Center for Democracy.



The two federal courts are among the most active in the country, with investigations that can span the country — and are the only ones known to make even modest disclosures about their surveillance dockets.

Peter Carr, a spokesman for the Justice Department, said “there are no broad generalizations or presumptions about when matters are sealed or not sealed,” and that such decisions are “an individualized process.”

When courts choose to share information “on the use of these investigative tools, the Department [of Justice] has worked with them” to preserve “the integrity of ongoing investigations,” and shield witnesses and the reputations of targets who are never charged, Carr said.

[A U.S. judge just disclosed how often law enforcement secretly tracks electronic records]

In Northern Virginia, electronic surveillance requests increased 500 percent in the past five years, from 305 in 2011 to a pace set to pass 1,800 this year.

Only one of the total 4,113 applications in those five years had been unsealed as of late July, according to information from the Alexandria division of the U.S. District Court for the Eastern District of Virginia, which covers northern Virginia. Kaufmann's group obtained the Northern Virginia data in July and shared it with The Washington Post.

The federal court for the District of Columbia had 235 requests in 2012, made by the local U.S. attorney's office. By 2013, requests in the District had climbed 240 percent, to about 564, according to information released by the court's chief judge and clerk.

Three of the 235 applications from 2012 have been unsealed.

The releases from the Washington-area courts list applications by law enforcement to federal judges asking to track data — but not eavesdrop — on users' electronic communications. That data can include sender and recipient information, and the time, date, duration and size of calls, emails, instant messages and social media messages, as well as device identification numbers and some website information.

Electronic exchanges, even absent what was said or written, can help investigators map a wide range of a target's relationships and the timing and pattern of activities.

The Virginia list also includes surveillance requests made since 2011 under a separate law that permits authorities to obtain the contents of emails.

The listings identified the case number of each surveillance application, the date it was filed and the name of the judge who reviewed it. Left undisclosed is information including the crime under investigation, any associated criminal case or charged defendant, or whether an investigation is ongoing or has ended. With rare exceptions, it also is not possible to determine whether a judge limited or denied an application, or whether a target or service provider challenged the government's request.

The information about what are known as pen register and trap and trace orders was made public after litigation by the ACLU, the Electronic Frontier Foundation, journalists and others, including some service providers. The ACLU has urged disclosures by all courts so the public and lawmakers can learn whether public safety gains outweigh privacy trade-offs.

"It's hard to understand whether this surveillance is necessary or whether there is overreach without basic information about how often these orders are sought or granted, or who is granting them. Even judges themselves do not know," Kaufman said.

[Edward Snowden comes forward as source of NSA leaks]

Recent years have witnessed explosive revelations about surveillance of Americans' electronic activity, focused on actions approved by a secretive federal court under the Foreign Intelligence Surveillance Act.

In contrast, the Washington court disclosures concern domestic law enforcement activities governed by the 1986 Electronic Communications Privacy Act — a federal law that has been copied by many states for their courts. The law has drawn less public attention than the act covering foreign intelligence gathering. But the 1986 act has attracted scrutiny in legal circles over whether its legal protections remain adequate in an era of increasingly sophisticated surveillance methods and data storage.

[A Maryland court is the first to require a warrant for covert cellphone tracking]

To get a traditional wiretap to listen in on a landline phone call, law enforcement authorities have to meet the legal standard of probable cause and prove to a judge that their search will probably yield evidence of a specific crime and that alternatives to a wiretap are unavailable.

But under the 1986 law, judges must approve requests for pen register orders upon a statement by government investigators that the information they are seeking is relevant to an investigation. Once in place, those orders typically remain sealed and bar companies from telling customers that law enforcement has requested their information.

The Justice Department alone obtained more than 42,000 such orders in criminal investigations in 2013 — the most recent year for which statistics are available — a sixfold increase since 2004 that coincided with the growth in smartphones, text messaging and social media applications such as Facebook.

[Justice Department: Agencies need warrants to use cellphone trackers]

Under another type of request, authorities can obtain contents of emails by showing a judge the information is “significant” to an investigation. The Virginia listings includes some requests for email content under that standard. But for more than two years, Carr said, the Justice Department in practice has generally used search warrants to obtain the content of emails.

U.S. Magistrate Stephen Wm. Smith of Houston, a leading voice for more openness, has said that encouraging courts to electronically file and publicly docket sealed surveillance requests using a standard form would help courts, Congress and the public debate legal reforms. Without a public docket, surveillance cases “all but vanish into a legal void . . . as if they were written in invisible ink,” Smith wrote in a 2012 article in the Harvard Law and Policy Review. U.S. District Chief Judge Beryl A. Howell of the District last month disclosed electronic surveillance requests made in 2012 in that court. The release for that year was arranged as part of a public records petition to unseal all government surveillance applications and orders in closed investigations that was brought by Vice News journalist Jason Leopold and joined by the Reporters Committee for Freedom of the Press.

The office of U.S. Attorney Channing D. Phillips of the District worked on the plan to disclose select information and said it agreed in principle that surveillance cases did not necessarily need to be permanently sealed.

The three unsealed District cases are related to a pending case against five defendants accused of heroin trafficking.

[Meet the judge who just released 200 secret government surveillance requests]

One still sealed District case docket states the request was denied by a judge on Feb. 14, 2012. Another sealed filing on June 22, 2012, was docketed with the words, " — v. United States of America," suggesting that it led to litigation by a company or person challenging the government's request.

U.S. Magistrate Theresa C. Buchanan in Virginia announced the change to the Alexandria court division's docketing disclosure in 2011 after three individuals represented by the EFF and ACLU challenged a secret government attempt to track their Twitter communications, connection records and account information.

[WikiLeaks, free speech and Twitter come together in Va. court case]

The government had allowed Twitter to notify the individuals of the request, which was part of a federal criminal investigation into the anti-secrecy group WikiLeaks' role in a mass release of U.S. diplomatic documents. The request remains the only unsealed application listed in the Virginia records.

A pending court case before a federal judge in Maryland illustrates how disclosures may spark public debate.

[Government rule change to catch pedophiles may mean more mass hacking]

The ACLU has asked the court to unseal the docket of a July 2013 search warrant in a national child pornography investigation. The ACLU says the warrant appeared to authorize the FBI to secretly place code, or malware, on all computers that logged in to an anonymous email service but could have captured information not only of suspects but also of individuals such as dissidents or journalists who also use the email service.

[From Playpen to TorMail: Did a government hack in a child porn probe sweep up data of innocent people?]

Carr said the warrant authorized access only to computers accessing specific email accounts and child porn websites on a specific hosting server, not all visitors, saying in a statement that "Any assertion otherwise is based on Internet rumor and not substantiated facts."

The ACLU's Kaufman said that, whether the warrant was broad and legally questionable or narrower, "the government should disclose it and related materials so the public can decide for itself whether this kind of operation was lawful or wise."