Gagged, Sealed & Delivered: Reforming ECPA's Secret Docket

*Stephen Wm. Smith**

What is the most secret court docket in America? Many would point to the Foreign Intelligence Surveillance Act (FISA) court, set up during the Carter Administration to oversee requests for surveillance warrants against suspected foreign intelligence agents.[1] Due to the sensitive nature of its business, FISA proceedings and records are closed to public view. Since 1979, that court has processed over 28,000 warrant applications and renewals,[2] a rate of nearly one thousand secret cases a year.

But the FISA court is not number one in the secrecy parade, not by a long shot. According to a recent study by the Federal Judicial Center, there is another federal docket that handles tens of thousands of secret cases every year.[3] That docket is presided over by federal magistrate judges in United States district courts around the country. Most of its sealed cases are classified as "warrant-type applications," a category that includes not only routine search warrants but also various forms of electronic surveillance, such as the monitoring of electronic communications and data transmitted by the cell phones, personal computers, and other digital devices that now dominate our everyday lives. This type of electronic surveillance is regulated principally by the Electronic Communications Privacy Act of 1986 (ECPA).[4] Although the ECPA has often been amended, most changes have been technical tweaks to the existing framework.[5]

Some are now pushing for an update of the ECPA, which after all was enacted over two generations ago, long before Google or the smart phone was even conceived. Numerous hearings have been held in both the House and the Senate,[6] and last year several new bills were introduced in response

* United States Magistrate Judge, Southern District of Texas, Houston Division. Special thanks are due to my chambers staff—law clerks Patty DeLaney and Robert Morales, and case manager Jason Marchand—for invaluable assistance at various stages of this Article.

[1] *See* Foreign Intelligence Surveillance Act, 50 U.S.C. § 1803 (2010).

[2] Patricia L. Bellia, *Designing Surveillance Law*, 43 ARIZ. ST. L.J. 293, 341 (2011).

[3] TIM REAGAN & GEORGE CORT, FED. JUDICIAL CTR., SEALED CASES IN FEDERAL COURTS (2009) [hereinafter FJC STUDY], *available at* http://www.fjc.gov/public/pdf.nsf/lookup/sealcafc.pdf/$file/sealcafc.pdf.

[4] JAMES G. CARR & PATRICIA L. BELLIA, THE LAW OF ELECTRONIC SURVEILLANCE § 4:7 (2012).

[5] The primary exception was the USA PATRIOT ACT, which enacted several significant changes. Bellia, *supra* note 2, at 333. R

[6] *See Electronic Communications Privacy Act Reform: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 29 (2010) [hereinafter *ECPA Reform Hearing*]; *ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 81, 85, 93–94 (2010); *Electronic Communications Privacy Act: Government Perspectives on Protecting Pri-*

to concerns raised by industry and privacy groups.[7] Even the Department of Justice has weighed in with its own wish list of proposals to amend the ECPA in law enforcement-friendly ways.[8] Most proposals deal with substantive questions generated by new technology, like cell phone-location tracking or cloud computing.[9]

Less attention has been given to reforming more structural aspects of the ECPA.[10] One of the most neglected topics has been the regime of secrecy surrounding ECPA court orders. Through a potent mix of indefinite sealing, nondisclosure (i.e., gagging), and delayed-notice provisions, ECPA surveillance orders all but vanish into a legal void. It is as if they were written in invisible ink—legible to the phone companies and Internet service providers who execute them, yet imperceptible to unsuspecting targets, the general public, and even other arms of government, most notably Congress and the appellate courts.

Lack of transparency in judicial proceedings has long been recognized as a threat to the rule of law and roundly condemned in ringing phrases by many Supreme Court opinions.[11] According to the Court, transparency performs at least three vital functions in our judicial system: (1) it discourages misconduct among litigants and witnesses; (2) it checks the potential abuse of judicial power; and (3) perhaps most importantly, it has the "significant community therapeutic value" of promoting public confidence in the judicial system.[12] The Court elaborated on the unbroken Anglo-Saxon tradition of public access to criminal proceedings in *Richmond Newspapers, Inc. v. Virginia*: "Even without such experts to frame the concept in words, people sensed from experience and observation that, especially in the administration of criminal justice, the means used to achieve justice must have the support derived from public acceptance of both the process and its results."[13]

---

vacy in the Digital Age: Hearing Before the Senate Comm. on the Judiciary, 112th Cong. (2011) [hereinafter *Senate Judiciary 2011 ECPA Hearing*].

[7] *See* S. 1011, 112th Cong. (2011); S. 1212, 112th Cong. (2011); H.R. 2168, 112th Cong. (2011).

[8] *See Senate Judiciary 2011 ECPA Hearing*, *supra* note 6, at 6–11 (statement of Hon. James A. Baker, Associate Deputy Att'y Gen. of the United States). R

[9] *See Our Principles*, DIGITAL DUE PROCESS, http://www.digitaldueprocess.org/index.cfm?objectid=99629E40-2551-11DF-8E02000C296BA163 (last visited Mar. 28, 2012) (listing the proposed standards of the Digital Due Process Coalition, a diverse group of major companies, privacy advocates, and think tanks) (on file with the Harvard Law School library).

[10] Professor Patricia Bellia has termed these "second-order design questions," and has emphasized their impact on the quality of legislative and judicial oversight of executive surveillance techniques. Bellia, *supra* note 2, at 333. *See also* Paul Ohm, *Probably Probable Cause: The Diminishing Importance of Justification Standards,* 94 MINN. L. REV. 1514, 1549 (2010) (arguing that too much attention is paid to amending ECPA's "justification standards" and that Congress should seek other ways to balance police needs with privacy). R

[11] *See, e.g.*, Gannett Co. v. DePasquale, 443 U.S. 368, 412 (1979) (Blackmun, J., concurring in part and dissenting in part) ("[S]ecret judicial proceedings would be a menace to liberty."); Sheppard v. Maxwell, 384 U.S. 333, 349 (1966) ("[J]ustice cannot survive behind walls of silence . . . ."); Craig v. Harney, 331 U.S. 367, 374 (1947) ("What transpires in the court room is public property.").

[12] Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555, 556 (1980).

[13] *Id.* at 570–71.

Of course, some measure of temporary secrecy for electronic surveillance orders during a criminal investigation is both reasonable and necessary. Premature disclosure to the target or the general public could jeopardize the integrity of the ongoing investigation and encourage the target to flee or destroy evidence. The problem is that these surveillance orders remain secret long after the criminal investigation comes to an end.[14] This means that, unless the investigation results in criminal charges, targets who are law-abiding citizens will never learn that the government has accessed their emails, text messages, twitter accounts, or cell phone records. How often does this happen? No publicly available records answer the question, but information disclosed in a recent Freedom of Information Act case suggests that it happens thousands of times every year.[15]

Even if all ECPA targets were real criminals, the apparent size of ECPA's secret docket is by itself enough to give pause. Assuming the calculations in the next section are close to the mark, the number of ECPA cases filed in a single year surpasses the entire output of the FISA court since its creation in 1978.[16] More troubling still, this huge segment of the federal docket is not subjected to the discipline of appellate review routinely applied to the rest of that docket. For reasons explained in Part Three below, ECPA surveillance rulings are almost never challenged on appeal. Two very unfortunate consequences flow from this fact: magistrate judges are given no guidance in how to interpret or apply ECPA's complex provisions, and law enforcement is given free rein to push its surveillance power to whatever limits it chooses to recognize.[17]

This is not to say that there are no other potential constraints on this executive power. Congress, as the branch of government most responsive to public opinion, has the oversight power to enact laws responsive to new

---

[14] *See In re* Sealing and Non-Disclosure of Pen/Trap/2703(d) Orders, 562 F. Supp. 2d 876, 878 (S.D. Tex. 2008). This case is discussed in more detail *infra* note 68 and accompanying text. **R**

[15] *See* ACLU v. U.S. Dep't of Justice, 655 F.3d 1, 4 (D.C. Cir. 2011). This case is discussed in more detail *infra* note 83. **R**

[16] It should also be kept in mind that these calculations exclude state court surveillance orders. No data is available regarding state use of pen/trap devices, although data is available for state wiretaps. *See* Paul M. Schwartz, *Reviving Telecommunications Surveillance Law*, 75 U. CHI. L. REV. 287, 297. Based on the comparative wiretap data, the author infers that "there is currently more state use of these [pen/trap] devices than federal." *Id.*

[17] For example, district courts have repeatedly ruled that a probable cause warrant is required to obtain post-cut-through dialed digits (PCTDD) revealing content information such as bank account and Social Security numbers. *See In re* Application of the U.S. for Orders (1) Authorizing the Use of Pen Registers & Trap & Trace Devices & (2) Authorizing Release of Subscriber Information, 515 F. Supp. 2d 325 (E.D.N.Y. 2007); *In re* Application of the U.S. for an Order: (1) Authorizing the Installation & Use of a Pen Register & Trap & Trace Device, & (2) Authorizing Release of Subscriber and Other Information, 622 F. Supp. 2d 411, 419–22 (S.D. Tex. 2007); *In re* Application of the U.S. for an Order Authorizing (1) Installation & Use of a Pen Register & Trap & Trace Device or Process, (2) Access to Customer Records, & (3) Cell Phone Tracking, 441 F. Supp. 2d 816, 818–27 (S.D. Tex. 2006). The DOJ has never appealed such rulings, yet the FBI continues to seek such data in its pen register applications. *See, e.g.*, *In re* Application, No. 4:10-mj-01038 (Doc. 1) (S.D. Tex. Oct. 29, 2010); *In re* Application, No. 4:09-mj-00493 (Doc. 1) (S.D. Tex. June 25, 2009).

technology. But Congress often reacts slowly, if at all. A case in point is location tracking of cell phones, an issue which first came to Congress's attention in 1994.[18] Eighteen years have now passed without any amendment to the ECPA clarifying the appropriate legal standard for law enforcement to obtain that information. One likely reason for this lack of oversight is that Congress rarely has current, accurate data on the nature and extent of electronic surveillance by law enforcement due to inadequate reporting mechanisms in the ECPA itself.[19] With Congress on the sidelines, appellate courts not engaged, and the public in the dark, the results are predictable enough—surveillance tends to flourish and privacy to diminish, not by reasoned decision but by default.

The burden of this Article is to demonstrate that rooting out unnecessary secrecy should be a primary goal of any ECPA reform. The Article will proceed in four Parts: Part One will examine the extent of electronic surveillance secrecy in federal courts; Part Two will examine the existing statutory provisions in ECPA that foster such secrecy; Part Three explains how this secrecy regime has choked off appellate review, leaving law enforcement free to define the limits of its own power; and the final Part suggests ways to reduce secrecy and thereby ensure that, whatever bill Congress enacts as the twenty-first century version of the ECPA, the balance it strikes between privacy and law enforcement will endure.

I. Secret Federal Dockets: The FJC Study

One of the foremost opponents of judicial secrecy is Judge Frank Easterbrook, now Chief Judge of the U.S. Court of Appeals for the Seventh Circuit. Upon elevation to that post in 2006, Judge Easterbrook became a member of the Judicial Conference of the United States, the policy-making body for administering U.S. courts. Apparently at his instigation,[20] the Judicial Conference in 2008 directed the Federal Judicial Center (FJC) to conduct a study of sealed cases in the federal courts. The results of the study were published the following year.[21]

The study examined all cases filed in federal courts in 2006. On the surface, its conclusions were somewhat heartening. Of 245,326 civil cases filed that year, only 576 (0.2%) remained completely sealed in 2008. On the

[18] *See* Communications Assistance to Law Enforcement Act, Pub. L. No. 103-414, § 103, 108 Stat. 4280 (1994) (codified at 47 U.S.C. § 1002(a)(2) (2006)). The legislative history of the relevant CALEA proviso, which specified only that location information was not accessible solely pursuant to the Pen/Trap Statute, is discussed at *In re Application for Pen Register & Trap/Trace Device With Cell Site Location Auth.*, 396 F. Supp. 2d 747, 762–64 (S.D. Tex. 2005).

[19] *See* Schwartz, *supra* note 16, at 294–99. R

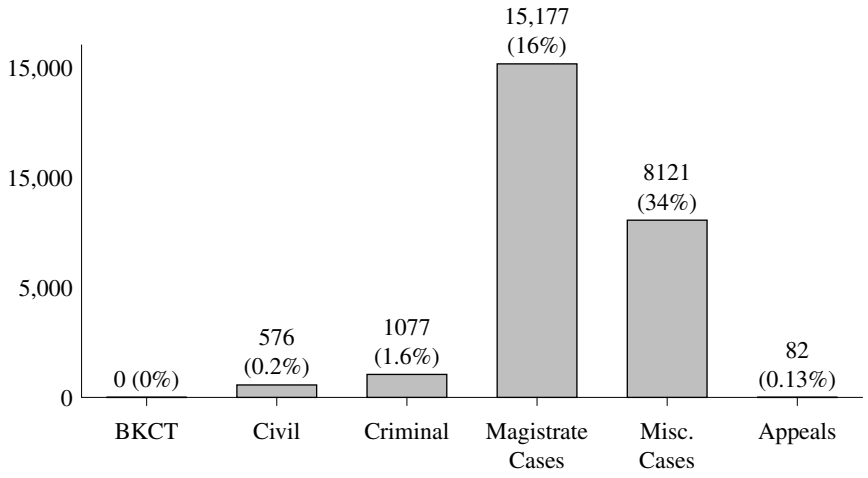
[20] *See* Carlyn Kolker, *Judges to Judges: Stop Sealing Cases*, Thompson Reuters News & Insight (Sept. 15, 2011), http://newsandinsight.thomsonreuters.com/New_York/News/2011/09_-_September/Judges_to_judges__stop_sealing_cases/ (on file with the Harvard Law School Library).

[21] FJC Study, *supra* note 3. R

criminal side, the numbers were slightly higher, though still not cause for alarm: of 66,458 criminal cases filed, 1,077 (1.6%) were completely sealed.[22]

These numbers do not tell the whole story, however. "Civil" and "criminal" are not the only recognized case classifications used by federal district courts.[23] Two other categories are also used: magistrate judge cases (designated "mj"), and miscellaneous cases (designated "mc" or "ms").[24] Magistrate judge cases consist of various kinds of independent proceedings, usually *ex parte*, typically assigned to magistrate judges by the district courts. These include warrant-type applications (such as search warrants, seizure warrants, pen registers, trap and traces, tracking devices, and permissions to compel information such as emails, telephone records, and tax returns), as well as other matters such as criminal complaints, Criminal Justice Act (CJA) appointments, extraditions, letters rogatory, and forfeitures. Miscellaneous cases usually consist of a variety of other matters often handled by district judges, including wiretaps.

FJC STUDY
SEALED FEDERAL CASES BY CASE TYPE 2006[25]



[22] 22 *See* SEALED CASES SUBCOMM. FOR THE JUDICIAL CONFERENCE COMM. ON RULES OF PRACTICE & PROCEDURE, REPORT ON SEALING CASES (2010), *available at* http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/jc09-2010/2010-09-Appendix-E.pdf. Note that the Sealed Cases Subcommittee worked with the FJC to specifically research sealed cases.

[23] Bankruptcy courts also have a distinct numbering system for their cases. However, the FJC study found no instance of an entirely sealed bankruptcy case in 2006. *See* FJC STUDY, *supra* note 3, at 31. R

[24] *Id.* at 2. As the study points out, some courts use additional categories, and classification criteria are not uniform across all districts.

[25] Cases filed in 2006 and still sealed at time of study in 2008. *Id.* at 21–30.

As the bar graph shows, the incidence of completely sealed magistrate judge cases was very high: 15,177 cases, or 16% of all 97,155 magistrate judge cases filed that year. The great bulk (83%)[26] of these sealed cases were warrant-type applications. Based on these numbers alone, it appears that a significant volume of law enforcement warrant activity—more than 12,000 cases annually—was handled out of public view. But on closer look this figure is a severe undercount, for several reasons.

A. Undercount Due to Inconsistent Case Designation

Part of the problem is that, as the FJC study found, district courts are not consistent in their designations of magistrate judge and miscellaneous cases. For example, many districts categorized a warrant-type application as a miscellaneous case; in fact, such applications were given miscellaneous case numbers one-third as often as magistrate judge case numbers.[27] Thus, magistrate judges frequently preside over cases identified as sealed miscellaneous cases, most of which are warrant-type applications.[28] While the miscellaneous category is the smallest in terms of volume, it also contains the largest percentage of sealed cases—34%. The combined total of sealed magistrate judge and miscellaneous cases was 23,298, representing about one out of every five cases in those two categories.[29] Of this combined total, more than 17,000 were warrant-type cases, according to FJC estimates.[30]

B. Undercount Due to Methodology

Sobering as these numbers are, they still understate the true extent of sealing in the federal courts. This is due to the study's methodology.[31] The Judicial Conference's subcommittee tasked the authors to study "completely sealed cases, not partially sealed case files."[32] To that end, they "consider[ed] a case sealed if the public is denied access to all docket information as well as all documents filed in the case."[33] Two types of sealed cases met this restrictive FJC criterion: (1) those not even entered on the Case Management and Electronic Filing System (CM/ECF),[34] and (2) those en-

[26] *Id.* at 21–22. This percentage was derived by a sampling technique described in the study, because the authors believed there were too many orders to be examined individually.

[27] *Id.* at 23. The study observed that some districts "use magistrate judge case numbers for one type of warrant-type application, such as search warrants, and miscellaneous case numbers for other types of warrant-type applications, such as pen registers." *Id.*

[28] The FJC study estimated that 58% of sealed miscellaneous cases were warrant-type, based on a limited sample of cases from each district. *Id.*

[29] *Id.* at 21, 23.

[30] *Id.* at 22–23.

[31] This is not intended as a criticism of the authors' work, which is a very valuable and timely study of a difficult problem.

[32] FJC STUDY, *supra* note 3, at 1. **R**

[33] *Id.* at 28.

[34] CM/ECF is the online docketing system used in federal courts. The Southern District of Texas converted to this system in 2004, and according to the Administrative Office of U.S.

tered on CM/ECF with only a docket number and the notation "sealed."A case with every document sealed would *not* be counted as sealed, so long as there was *some* public information about the case, even in highly redacted form.[35] In other words, this study looked at sealed *cases*, not sealed *orders* granting (or denying) the requested relief.

Plainly, the number of sealed orders greatly exceeds the number of sealed cases as counted by the FJC study; the question is by how much? An actual search of all ninety-four district court dockets is beyond the scope of this Article (and the patience of this author), and the FJC may wish to consider such a study. In the meantime, there is another way to plausibly estimate the size of this hidden docket.

C. Estimating the Number of Sealed Orders

Although the FJC study is a severe undercount, it does provide a useful starting point. To arrive at an overall number, it ought to be possible to combine the FJC tally of completely sealed cases with a projected number of sealed orders based on a representative sample of publicly available CM/ECF docket sheets. The sum of these two numbers should put us within shouting range of the true number, until more exacting research comes along.

However, this simple additive approach runs the risk of double counting, because the FJC tally of completely sealed cases includes both CM/ECF ("online") and non-CM/ECF ("offline") cases. In other words, a projected number of sealed orders based on a sample review of online CM/ECF docket sheets may count as sealed an order already counted as sealed under the FJC's stricter standard. Fortunately, the FJC study gives us the means to elude this trap, because it discloses the relative percentages of sealed cases not entered into CM/ECF: 39% of magistrate judge cases and 42% of miscellaneous cases.[36] So the number of sealed, offline magistrate judge cases, per the FJC's count, is 5,919 (15,177 x .39); the number of sealed, offline miscellaneous cases is 3,411 (8,121 x .42); the combined total (per the FJC) of sealed offline cases on both dockets is 9,330.

Having computed the offline total, the next step in the calculation is to examine a sample of CM/ECF docket sheets to determine how many sealed orders the magistrate judge and miscellaneous dockets contain. Unlike the FJC study, this approach would count as sealed an order granting or denying the requested relief, regardless of what other case information, such as filing date or case type, might be publicly available.

Courts, 99% of all federal courts are now using the system. *See About CM/ECF*, ADMIN. OFF. U.S. CTS., http://www.uscourts.gov/FederalCourts/CMECF/AboutCMECF.aspx (last visited Apr. 11, 2012) (on file with the Harvard Law School library).

[35] FJC STUDY, *supra* note 3, at 1–2. For example, a case with a docket sheet consisting of the notation "Sealed Event" for each filing date would not be counted as sealed for purposes of the study. **R**

[36] *Id.* at 21, 23.

A review of Houston's CM/ECF docket sheets reveals that, out of 895 Houston magistrate judge cases filed in 2006, there were 418 sealed orders. This is 47% of the docket,[37] which is obviously a very high percentage. Is it representative of district courts as a whole? A spot check of 2006 online records for two other randomly selected districts suggests that Houston's ratio is certainly in the ballpark: the District of New Jersey shows 628 sealed magistrate judge orders out of a total of 1,581 (40%);[38] the Southern District of Florida shows 1,014 sealed magistrate judge orders out of a total of 2,170 (47%—exactly the same as Houston's).[39]

Even if the lowest of these percentages held nationwide, the number of sealed magistrate judge orders reported online would exceed 36,000.[40] Adding that figure to the 5,919 offline magistrate judge cases, we reach a total of more than 42,000 sealed orders in magistrate judge cases.

But this estimate is not yet complete, because it does not include miscellaneous cases. Based on a similar analysis of the 2006 Houston CM/ECF miscellaneous case docket, the percentage of sealed orders was 24%. Applying that percentage nationwide results in 4,965 sealed online miscellaneous orders;[41] added to the non-CM/ECF miscellaneous cases, the total of miscellaneous sealed orders rises to 8,376.

Putting all these numbers together—miscellaneous docket and magistrate judge docket, online and offline—we reach a grand total of over 50,000 sealed orders, or 42% of all cases filed on these two dockets in 2006. This is more than double the rate of sealing found by the FJC study.

D. Estimating the Size of the ECPA Docket

What percentage of these 50,000 secret orders are electronic surveillance orders[42] under the ECPA? Again, the FJC study does not really answer

[37] Other divisions in the Southern District of Texas followed a different classification procedure than Houston (e.g., pen register cases were classified as miscellaneous cases, or were not included in CM/ECF at all), precluding any consistent computation across the entire district.

[38] D. N.J. CM/ECF data on file with author. The number of sealed cases includes fifty cases for which no documents are available electronically despite an unsealing order.

[39] S.D. Fla. CM/ECF data on file with author. The number of sealed cases includes thirteen cases for which no documents are available electronically despite an unsealing order.

[40] The calculation is as follows: (97,155 – 5,919) x .40 = 36,494; that is, (total number of mj cases – offline-CM/ECF mj cases) x (percentage of orders sealed) = sealed online CM/ECF magistrate judge orders. *See* FJC STUDY, *supra* note 3, at 21. R

[41] The calculation is (24,099 – 3,411) x .24 = 4,965; that is, (total number of mc cases – offline-CM/ECF mc cases) x (percentage of orders sealed) = sealed online CM/ECF miscellaneous judge orders. *See id.* at 23.

[42] For purposes of this Article, the term "electronic surveillance order" covers all types of orders related to the ECPA, including wiretaps, tracking devices, pen registers, trap and trace devices, cell site data, stored wire and electronic communications such as email and text messages, as well as account information and other customer records held by electronic service providers, such as means of payment, activity logs of telephone, email, and Internet use, and the like.

the question.[43] However, a review of sealed cases on the 2006 Houston magistrate judge docket showed that more than 60% were ECPA related.[44] If this ratio applies across the board,[45] the number of electronic surveillance orders issued by federal courts in 2006 exceeds 30,000.

SEALED ORDERS: U.S. MAGISTRATE JUDGE AND MISCELLANEOUS DOCKETS 2006

		Sealed Orders			
	Cases	Offline (Non-CM/ECF)	Online (CM/ECF)	Combined (Offline + Online)	ECPA Orders
MJ docket	97,155	5,919	36,494	42,413	25,448
MS docket	24,099	3,411	4,965	8,376	5,025
Totals	121,254	9,330	41,459	50,789	30,473

The table above summarizes the results of the calculations described above. To recap: The first column shows the number of magistrate judge and miscellaneous cases filed in all federal courts during 2006. The second column shows the number of sealed final orders in cases not reported online, according to the FJC study. The third column shows the number of sealed final orders in cases for which at least some information is available on CM/ECF; these numbers are projections, based on the estimate that 40% of all online cases had sealed final orders. The 40% sealing ratio was the lowest among three sample districts examined by my chambers staff. The fourth column simply adds the number of sealed orders (online and offline) from columns two and three. Finally, the last column projects the number of sealed ECPA orders issued by all magistrate judges in 2006, assuming that 60% of the sealed cases in column four were ECPA surveillance orders. The 60% ratio was based on our review of Houston CM/ECF docket sheets.

[43] The FJC did not attempt to classify cases as ECPA or non-ECPA related. The study did attempt an estimated breakdown of cases according to warrant type, but this was based on a limited sample rather than an actual count. Due to the large volume of sealed cases, FJC researchers were unable to examine every one, and instead merely sampled two sealed magistrate judge cases and five sealed miscellaneous cases from each district. FJC STUDY, *supra* note 3, at 3. This limited sample size undermines the persuasive power of the FJC's warrant-type projections. R

[44] That is, government applications for pen registers, trap/trace, tracking devices, stored electronic communications, email and phone records, customer account and other information under the ECPA. The review was conducted by the author's chambers staff based on publicly available CM/ECF information. The data is on file with the author.

[45] The Houston docket sheets for sealed miscellaneous cases do not specify the type of case sealed, so a similar analysis was not done for such cases. Even so, it is not unreasonable to apply the 60% ratio here as well. The FJC study estimated that 70% of sealed miscellaneous cases consisted of pen registers, trap and traces, tracking devices, wiretaps, and the like. FJC STUDY, *supra* note 3, at 23. R

Thus, by combining the FJC survey with these projections, we conclude that in 2006 magistrate judges issued more than 30,000 ECPA orders. To put this figure in context, magistrate judges in one year generated a volume of secret electronic surveillance cases more than thirty times the annual number of FISA cases; in fact, this volume of ECPA cases is greater than the combined yearly total of all antitrust, employment discrimination, environmental, copyright, patent, trademark, and securities cases filed in federal court.[46]

These figures are of course tentative, and further study is certainly warranted. Even so, it is plain that the FJC study has charted just the tip of a very large iceberg. Some litigants are now attempting to probe beneath the surface to discover its true dimensions, but the going is tough; much time and effort is required merely to learn basic docket information such as case names and numbers.[47] According to the calculations above, federal magistrate judges were presented with over 30,000 secret ECPA applications in 2006. There is no reason to believe these numbers have abated in recent years; quite the contrary, in fact.[48] How did we reach this troubling pass? To answer that we must take a closer look at the structure of the Electronic Communications Privacy Act.

II. The ECPA Secrecy Regime

The first thing to understand is that ECPA surveillance orders are hedged in by secrecy rules not typically applicable to ordinary search and seizure warrants issued under Rule 41 of the Federal Rules of Criminal Procedure. That rule makes no reference to sealing. On the contrary, Rule 41(i) directs the judicial officer to forward all papers relating to the search warrant to the clerk's office, presumably to be placed on the court docket for public inspection.[49] The rule also requires that the officer executing the warrant

---

[46] *See* James C. Duff, Admin. Office of the U.S. Courts, Judicial Business of the U.S. Courts 2006, at 168–73 tbl.C-2 (2006), *available at* http://www.uscourts.gov/uscourts/Statistics/JudicialBusiness/2006/front/completejudicialbusiness.pdf.

[47] *See* ACLU v. U.S. Dep't of Justice, 655 F.3d 1 (D.C. Cir. 2011) (upholding a FOIA request for a list of docket numbers, courts, and names of prosecutions in which defendants were subject to warrantless cell phone tracking); *In re* Application of the United States for an Order Pursuant to 18 U.S.C. § 2703(d), Misc. Nos. 1:11-DM-3, 2011 WL 5508991 (E.D. Va. Nov. 10, 2011) (denying motion for public docketing of all § 2703(d) orders relating to WikiLeaks investigation).

[48] According to the latest disclosed figures by the DOJ, new pen register and trap/trace orders requested by four federal agencies (FBI, DEA, USMS, and ATF) more than doubled between 2006 and 2009. *Compare* U.S. Dep't of Justice, Report on the Use of Pen Registers and Tap and Trace Devices by the Law Enforcement Agencies/Offices of the Department of Justice for Calendar Year 2009 (2009), *available at* http://www.justice.gov/criminal/foia/docs/2009penreg-anlrpt.pdf, *with* U.S. Dep't of Justice, Report on the Use of Pen Registers and Tap and Trace Devices by the Law Enforcement Agencies/Offices of the Department of Justice for Calendar Year 2006 (2006), *available at* http://www.justice.gov/criminal/foia/docs/2006penreg-anlrpt.pdf.

[49] *See In re* Search Warrant for Secretarial Area Outside Office of Gunn, 855 F.2d 569, 573 (8th Cir. 1988) ("[S]earch warrant applications and receipts are routinely filed with the clerk of court without seal."); *In re* Application of Newsday, Inc., 895 F.2d 74, 79 (2d Cir.

give a copy of the warrant to the target of the search, though this notice can be delayed at the request of law enforcement if a statute so permits.[50] Therefore, even though the process of issuing search warrants entails an *ex parte* application by the government and *in camera* consideration by the magistrate judge, affected parties are ultimately notified and search warrant papers are generally available for public scrutiny.

By contrast, ECPA surveillance orders are kept under wraps in three ways: sealing of court records, delayed notice to the target, and nondisclosure ("gag") orders directed to service providers and their agents. Interestingly, the statute does not take a uniform approach to secrecy for all types of electronic surveillance orders.

A. Wiretaps

Title I of the ECPA[51] amended the Wiretap Act to authorize interception of electronic communications. Wiretap orders and applications "shall be sealed" by the district judge[52] and may be disclosed "only upon a showing of good cause."[53] No time limit for sealing is stated. As the authors of the leading treatise on electronic surveillance law have observed, "the effect . . . is to close files to public scrutiny long after any need for secrecy has passed."[54] The statute does require post-surveillance notice to the target "within a reasonable time but not later than ninety days" after the surveillance ends, although that notice may be postponed upon a showing of good cause.[55] In practice, the ninety-day maximum period has come to be seen as a minimum, and further postponements are granted as a matter of routine.[56] Finally, only the targets of the investigation are entitled to notice; other parties to the intercepted communication have no right to notice under the statute.[57]

1990) ("[T]here is a common law right to inspect what is commanded thus to be filed."). *See generally*, WRIGHT ET AL., FEDERAL PRACTICE AND PROCEDURE, CRIMINAL § 673, at 332–33 (3d ed. 2004) (noting that sealing of search warrant affidavits is "an extraordinary action" to be taken only in exceptional cases).

[50] *See* FED. R. CRIM. P. 41(f)(1)(C), (f)(3).

[51] Pub. L. No. 99-508, § 101, 100 Stat. 1848 (1986) (codified at 18 U.S.C. §§ 2510–2511, 2520–2521 (2006)). Another portion of this title authorizes tracking devices moving across state lines. 18 U.S.C. § 3117 (2006). Tracking devices are covered by recent amendments to Rule 41.

[52] Magistrate judges are not authorized to issue wiretap orders. *See* 18 U.S.C. § 2510(9)(a) (2006); *In re* United States, 10 F.3d 931 (2d Cir. 1993).

[53] 18 U.S.C. § 2518(8)(b) (2006).

[54] CARR & BELLIA, *supra* note 4, § 4:70. R

[55] 18 U.S.C. § 2518(8)(d) (2006).

[56] *See* CARR & BELLIA, *supra* note 4, § 5:45. R

[57] 18 U.S.C. § 2518(8)(d). These non-targets have been described as "conversational passersby." *Id.* § 5:46.

B. Pen Registers and Trap & Trace Devices

Title III of the ECPA (referred to as the Pen/Trap Statute) covers pen registers and trap/trace devices.[58] The Pen/Trap Statute also provides for sealing and nondisclosure, but on its face allows for more judicial discretion than in the case of wiretaps. The statute directs that pen/trap orders be sealed "until otherwise ordered by the court."[59] No particular sealing period is given, although presumably sealing ought to last at least as long as the surveillance authorized by the order itself—a period of sixty days.[60] No specific showing is required to justify unsealing. The statute also authorizes a gag order directing the service provider and its employees not to disclose the existence of the pen/trap or the underlying investigation to any other person, "unless or until otherwise ordered by the court."[61] Again, no particular showing by the government is required to obtain the gag order, and no maximum (or minimum) time period is imposed or suggested.[62] Unlike wiretap orders (as well as ordinary search warrants), there is no requirement that the pen/trap target ever be given notice of the order or the investigation; by the same token, nothing in the statute precludes such notice at the court's discretion. In sum, a judge issuing a pen/trap order is required to seal the order for some unspecified period, but the duration of the sealing and any accompanying gag order is left to that court's essentially unguided discretion.

C. Stored Communications and Subscriber Information (2703(d) Orders)

Title II of the ECPA is known as the Stored Communications Act (SCA)[63] and prescribes requirements and procedures under which the government can obtain court orders (known as § 2703(d) orders) compelling access to stored wire and electronic communications, as well as related subscriber and customer account information. Unlike the Pen/Trap Statute, the SCA makes no provision for sealing such court orders. Even so, the government is generally not required to provide notice to the subscriber or customer before compelling disclosure from the provider via a 2703(d) order .[64]

---

[58] Pub. L. 99-508, 100 Stat. 1848, 1868 (1986) (codified at 18 U.S.C. § 3121 (2006)). Historically, a pen register recorded the phone numbers dialed by a target phone, whereas a trap and trace device recorded incoming phone numbers, like a caller ID device. In 2001, the USA PATRIOT Act expanded the definitions to include other non-content "dialing, routing, addressing, or signaling information," such as email addresses. CARR & BELLIA, *supra* note 4, § 4:82. R

[59] 18 U.S.C. § 3123(d)(1) (2006).

[60] *Id.* § 3123(c)(1), (c)(2). Extensions up to sixty days can be granted upon reapplication to the court.

[61] *Id.* § 3123(d)(2).

[62] In fact, the "unless" clause implies that the court may refuse to enjoin disclosure even in the first instance.

[63] Pub. L. No. 99-508, 100 Stat. 1848, 1860-61 (codified at 18 U.S.C. § 2701–2703 (2006)).

[64] The exception to the rule is when the government seeks a 2703(d) order to compel disclosure of the contents of certain electronic communications. 18 U.S.C. § 2703(b)(1)(B). Prior notice to the subscriber or customer is required in that instance, although delayed notice

The SCA does authorize the court to issue a gag order (called "preclusion of notice") to service providers, commanding them not to notify any other person of the existence of the court order.[65] Unlike the related non-disclosure provisions of the Pen/Trap Statute, however, an SCA gag order is not automatic. As a predicate to issuance, the court must find reason to believe that notification "will" result in one or more of the following adverse consequences: "(1) endangering the life or physical safety of an individual; (2) flight from prosecution; (3) destroying or tampering with evidence; (4) intimidation of potential witnesses; or (5) otherwise seriously jeopardizing an investigation or unduly delaying a trial."[66] The duration of notice preclusion under § 2705(b) is "for such period as the court deems appropriate."[67] So once again, Congress defers to the discretion of the issuing judge.

Thus, the secrecy provisions of the SCA are less stringent than other forms of ECPA surveillance such as wiretaps or pen registers. The default rule is that a 2703(d) order will not be sealed, nor will it be accompanied by a gag order absent a showing of one of the special circumstances listed in 2705(b). However, in many districts the government routinely avoids these weaker SCA secrecy provisions by the simple expedient of combining its requests for a 2703(d) order and a pen/trap order into a single application and order. The combined order is then automatically sealed and gagged by authority of the Pen/Trap Statute. Although neither statute appears to contemplate such combined orders, no published court opinion has challenged the practice.

D. Indefinite Sealing = Permanent Sealing

One might readily concede that ECPA orders ought not be made public while the criminal investigation is ongoing. The problem is that temporary sealing orders almost always become permanent. More often than not, judges set no expiration dates on these orders, but merely direct that they be sealed and not disclosed "until further order of the court."[68] The reality is that magistrate judges almost never have occasion to revisit these cases, so the "further order" lifting the seal rarely arrives.

My own division is a case in point. From 1995 through 2007, federal magistrate judges in Houston issued a total of 3,886 electronic surveillance orders that were sealed "until further order of the court." As of 2008, 99.8% of those orders remained sealed, long after the underlying criminal investiga-

of up to ninety days may be allowed upon a showing that notice may trigger one of the adverse results listed in 18 U.S.C. § 2705(a)(2).

[65] 18 U.S.C. § 2705(b) (2006). The use of the verb "notify" rather than "disclose" raises the question whether the notice preclusion order would prohibit the provider from responding to an unsolicited customer inquiry. No case has yet addressed this issue, however.

[66] *Id.* § 2705(b)(1)-(5).

[67] *Id.* § 2705(b).

[68] *E.g.*, *In re* Sealing & Non-Disclosure of Pen/Trap/2703(d) Orders, 562 F. Supp. 2d 876, 877–78 (S.D. Tex. 2008).

tion was closed.[69] Based on anecdotal conversations with other magistrate judges around the country, I have no reason to believe the Houston experience is unique.

This phenomenon is troubling for a number of reasons. First, secret court records violate the centuries-old common law tradition of public access.[70] Second, a compelling argument can be made that gag orders of indefinite duration violate the First Amendment.[71] Finally, excessive secrecy effectively shields electronic surveillance orders from appellate review, thereby depriving the judiciary of its normal role in shaping, adapting, and updating legislation to fit changing factual (and technological) settings over time. This point is elaborated in the next Section.

III. Missing in Action: ECPA and the Courts of Appeals

It is commonly recognized that statutes dominate the law of electronic surveillance. As Professor Bellia has observed, "[t]here is surprisingly little judicial constitutionally-based regulation of surveillance tactics."[72] Even apart from constitutional issues, remarkably few appellate court opinions delve into ECPA's complexities as a matter of ordinary statutory interpretation. Although an empirical study of this claim is beyond the scope of this Article, a few illustrations may suffice.

- During its twenty-five year history, the ECPA has been the subject of only two Supreme Court decisions.[73] By comparison, over a similar period the Supreme Court decided thirty-seven cases involving the Employee Retirement Income Security Act of 1974,[74] a statute of comparable range and complexity but generating far fewer cases filed.[75]
- Until 2010, no appellate court had ever addressed the legal standard applicable to cell phone-tracking orders, even though magistrate judges were issuing tens of thousands of such orders every year without appellate guidance. One federal circuit court

[69] *Id.* at 895. To avoid this problem, I now set a time limit of 180 days for sealing and gag orders, with extensions granted if the investigation is still ongoing, or for other good cause.

[70] *See* Stephen Wm. Smith, *Kudzu in the Courthouse: Judgments Made in the Shade*, 3 Fed. Cts. L. Rev. 177, 181–202 (2009).

[71] *See In re Sealing*, 562 F. Supp. 2d at 881–87. The argument is that an electronic surveillance gag order is a content-based prior restraint on speech, which bears a heavy presumption against its constitutional validity. The government does have a compelling interest in maintaining the integrity of its ongoing criminal investigation, but that interest expires when the investigation ends. *See also* Butterworth v. Smith, 494 U.S. 624, 632–33 (1990).

[72] Bellia, *supra* note 2, at 298. R

[73] *See* City of Ontario, Cal. v. Quon, 130 S. Ct. 2619 (2010); Bartnicki v. Vopper, 532 U.S. 514 (2001). Neither case involved a criminal investigation.

[74] John H. Langbein, David A. Pratt & Susan J. Stabile, Pension and Employee Benefit Law xix–xxxix (5th ed. 2010).

[75] The number of new ERISA filings in 2006 was only one-third the number of ECPA filings as calculated above. *See* Duff, *supra* note 46, at 162 tbl.C-2. R

finally considered the issue in that year,[76] but its decision raised as many questions as it answered.[77]

- The first (and to date the only) appellate case reaching the constitutionality of ECPA provisions on government access to emails was finally decided in 2010, and was commenced only after a magistrate judge unsealed the underlying ECPA orders.[78]

There is no real mystery to this unusual state of affairs. Appellate review cannot happen unless one of the parties has both the opportunity and the incentive to appeal. But when it comes to electronic surveillance orders, the poet's maxim prevails: "In this world, who can do a thing, will not / And who would do it, cannot, I perceive."[79] To see this, consider the strategic perspective of the three parties who might be aggrieved by an adverse ruling on an electronic surveillance application—the targeted individual, the provider, and the government.

A. Browning's Maxim in Action

Of the three, the targeted individual certainly has the most incentive to challenge an electronic surveillance order. Not only might such an order intrude upon personal privacy, it might also yield inculpatory evidence. Yet the target has no opportunity to challenge the order before its execution. He is extremely unlikely to know about the application because it is submitted *ex parte*, without notice, and subject to the sealing and gag orders already mentioned. Even if he somehow did learn about it, the ECPA affords him no statutory right to challenge the validity of a 2703(d) order prior to execution.[80] If later charged with the crime under investigation, he may collaterally attack the order via a motion to suppress under the Fourth Amendment, although prospects of success are not very high.[81] This also assumes that the

---

[76] *See In re* Application of U.S. for an Order Directing Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304 (3d Cir. 2010). The issue is now before the Fifth Circuit. *See In re* Application of the U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827 (S.D. Tex. 2010), *appeal filed*, COA number 11-20884 (Dec. 12, 2011).

[77] For an analysis by one of the *amici curiae* who participated in oral argument to the Third Circuit, see Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 682–89 (2011).

[78] *See* Warshak v. United States, 490 F.3d 455, 460–61 (6th Cir. 2007), *vacated in part*, 532 F.3d 521 (6th Cir. 2008) (en banc), *appeal after remand*, 631 F.3d 266 (6th Cir. 2010).

[79] ROBERT BROWNING, *Andrea Del Sarto*, *in* MEN AND WOMEN 184, 189 (1856).

[80] *In re* Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d), Misc. No. 1:11–DM–3, 2011 WL 5508991 (E.D. Va. Nov. 10, 2011) (holding that subjects of 2703(d) orders have no statutory right to notice or pre-execution hearing to vacate 2703(d) order for non-content Twitter records). The SCA authorizes a pre-execution challenge only to an order under § 2704 directing the service provider to create a backup copy of certain communication contents. 18 U.S.C. § 2704(b) (2006).

[81] Even if a constitutional violation is shown, relief may be denied if the officer acted in good faith. United States v. Leon, 468 U.S. 897 (1984). There is no statutory suppression remedy under the ECPA. 18 U.S.C. §§ 2510–2522 (2006). The Act does authorize a post-execution civil action against the provider, but good faith reliance on a court order is an absolute defense. 18 U.S.C. § 2707(e) (2006).

order has been disclosed by the government in pretrial discovery or at trial.[82] And of course, the suppression remedy is no consolation to the law-abiding citizen who is never charged with a crime and who never learns, even after the fact, that her emails and phone records have been obtained and reviewed by the government.[83]

The phone company or ISP on the receiving end of the order is in a different position. It certainly has the opportunity to challenge the order, as well as the accompanying gag provisions, if it chose to do so. But why should it? The provider's own privacy interests are not at stake, and it is compensated for most expenses of complying with the order. Costs of appeal would almost certainly outweigh any uncompensated inconvenience. Although there may well be instances in which a provider might "push back" against law enforcement in response to particular orders,[84] providers rarely appeal to a higher court.[85]

That leaves the government as the only viable appellant. As initiator of the *ex parte* proceeding, the government is immediately notified if the court denies its application, and has standing to appeal if it so chooses. Yet the government rarely so chooses. The reason is not hard to fathom. Why risk a loss on appeal that could make "bad law?" After all, a decision by a magistrate or district judge is not binding precedent.[86] Other magistrate judges in the district are available, so better to wait for a less obstinate judge on the duty rotation. An apparent example of this calculus is that, despite the multitude of magistrate (and district) judge decisions denying warrantless access to prospective cell site data, not one has been appealed to any federal circuit court.

[82] Given that so few of these orders are ever unsealed, it may be doubted whether they are routinely disclosed to defense counsel as a matter of practice.

[83] There are no good data on the number of persons targeted by these orders but never charged with a crime. However, the government's response to a recent FOIA request suggests the number is quite large. In *ACLU v. U.S. Dep't of Justice*, 655 F.3d 1 (D.C. Cir. 2011), the government was asked to provide docket information for any case in which an individual was prosecuted after the government obtained an order for cell phone location data without a showing of probable cause. In response, the DOJ produced a list of only 255 criminal prosecutions over a period of approximately seven years after September 11, 2001. *Id.* at 4. Given that thousands of such orders were issued by magistrate judges during this period, and that the first judicial decisions requiring probable cause for cell site information were not issued until 2005, it is reasonable to infer that far more law-abiding citizens than criminals have been tracked in this fashion.

[84] Albert Gidari Jr., *Companies Caught in the Middle*, 41 U.S.F. L. REV. 535, 546–47 (2007).

[85] *United States v. Apollomedia Corp.*, No. 99-20849, 2000 WL 34524449 (5th Cir. June 2, 2000), where an Internet service provider appealed a nondisclosure provision in a 2703(d) order, is perhaps the exception that proves the rule.

[86] *See* RLJCS Enters., Inc. v. Prof'l Benefit Trust Multiple Emp'r Welfare Benefit Plan & Trust, 487 F.3d 494, 499 (7th Cir. 2007).

B. No Bar to Government Appeal

Recently, some have floated the idea that the government faces a jurisdictional impediment when appealing the denial of an electronic surveillance application. A DOJ spokesman testified before the Senate Judiciary Committee that the ECPA should be amended to include a mechanism for the government to appeal the denial of *ex parte* orders in criminal investigations.[87] This proposal implicitly assumes that such a ruling is not a final decision subject to ordinary appellate review.[88] But no reported appellate case has ever denied jurisdiction over a government appeal on that basis. In fact, the government has an unbroken string of victories on the jurisdiction issue whenever it has been raised.[89] The reported decisions may be somewhat dated, but that merely confirms the issue is no longer worthy of serious debate.[90] The authors of the leading treatise on federal court practice, in a section collecting and summarizing the relevant case law, have concluded without qualification that denial of warrant applications are final decisions appealable by the government:

> Denial of a government application for a search warrant concludes the only matter in the district court. Nothing but airy speculation can predict whether there will be any subsequent criminal proceeding or other opportunity for appeal. . . . *Appeal is available as*

[87] *Senate Judiciary 2011 ECPA Hearing*, *supra* note 6, at 7 (statement of Hon. James A. Baker, Associate Deputy Att'y Gen. of the United States). The author has requested the DOJ to provide legal authority supporting its concerns, but to date has received no substantive response. **R**

[88] *See* 28 U.S.C. § 1291 (2006). The fallacy here is the assumption that a warrant application is necessarily part of some larger, on-going court proceeding. In reality, a warrant application is typically made during the investigation before a criminal case is filed, and so it is docketed as a separate, stand-alone case; when the court denies the requested relief, the case is over.

[89] *See In re* Application for Warrant to Seize One 1988 Chevrolet Monte Carlo, 861 F.2d 307, 308–09 (1st Cir. 1988) (denial of seizure warrants appealable under 28 U.S.C. § 1291); *In re* Grand Jury Subpoena Bierman, 765 F.2d 1014, 1017–18 (11th Cir. 1985), *vacated in part on other grounds*, 788 F.2d 1511 (11th Cir. 1986) (order denying motion to compel answer to grand jury question held appealable under both 28 U.S.C. § 1291 and 18 U.S.C. § 3731); *In re* Grand Jury Subpoena, 646 F.2d 963, 967–68 (5th Cir. 1981) (order quashing a grand jury subpoena appealable either as an order excluding evidence in criminal proceeding under 18 U.S.C. § 3731 or as final order under 28 U.S.C. § 1291); *In re* Grand Jury Empanelled Feb. 14, 1978, 597 F.2d 851, 854–57 (3d Cir. 1979) (same); *In re* Sealed Affidavit(s) to Search Warrants Executed on February 14, 1979, 600 F.2d 1256, 1257 n.2 (9th Cir. 1979) (order to unseal master affidavit in support of search warrant held appealable under 28 U.S.C. § 1291); *In re* Carlson, 580 F.2d 1365, 1372–73 (10th Cir. 1978) (denial of application for warrant to search and seize taxpayer assets held appealable under 28 U.S.C. § 1291); *In re* U.S. for an Order Authorizing the Interception of Oral Commc'ns, 563 F.2d 637, 640–42 (4th Cir. 1977) (denial of wiretap application appealable under 28 U.S.C. § 1291); *In re* United States, 427 F.2d 639, 642 (9th Cir. 1970) (order denying application to intercept wire communications appealable under 28 U.S.C. § 1291).

[90] For example, the Third Circuit accepted jurisdiction, without comment, over the government's appeal from a district court denial of a 2703(d) order for historical cell site data. *In re* Application of U.S. for an Order Directing a Provider of Electronic Commc'n Service to Disclose Records to the Gov't, 620 F.3d 304, 305 (3d Cir. 2010).

> *from a final decision.* Refusal to authorize use of electronic means to intercept communications is appealable for the same reasons.[91]

In short, the DOJ's proposal is a solution in search of a problem.

C. Standing Issues

That said, there is a serious standing problem when the government appeals such orders—who will argue the case for the other side? The surveillance application is typically an *ex parte* proceeding with no defendant yet charged. The target is rarely aware of these proceedings, which are sealed even when denied to avoid jeopardizing the ongoing investigation. Privacy groups are sometimes allowed to appear as *amicus curiae*, filing briefs in defense of the court's ruling. But this *ad hoc* measure is not entirely satisfactory; not every court can or will afford this opportunity, and even when such *amici* do appear, they do not have the same procedural rights as actual parties-in-interest, such as discovery, access to sealed filings, and the ability to raise claims not asserted by the parties. Unlike the DOJ's imaginary appealability concerns, this is a genuine problem in need of legislative attention.[92]

D. The Consequences of Avoiding Appellate Review

As we have seen, the parties in best position to challenge ECPA orders directly, the government and the providers, have little or no incentive to appeal. The party with the most incentive to appeal, the target, is largely prevented from doing so by ECPA's secrecy provisions. Targets never charged with a crime—that is, law-abiding citizens—will never learn of this government intrusion into their electronic lives.[93] Targets who later become

---

[91] CHARLES A. WRIGHT ET AL., FEDERAL PRACTICE AND PROCEDURE § 3919.9 (2d ed. 1992) (emphasis added) (footnotes omitted). Against this great weight of authority is one sentence of dicta by a district court dealing with a different issue. Denying a suppression motion by a defendant challenging the validity of a warrant on collateral estoppel grounds, the district court declared that "the government has no right to appeal if it believes the magistrate erred in denying the warrant." United States v. Savides, 658 F. Supp. 1399, 1404 (N.D. Ill. 1987), *aff'd on other grounds sub nom.* United States v. Pace, 898 F.2d 1218 (7th Cir. 1990). No authority was cited for this proposition, nor has this passage ever been cited by an appellate court—unsurprising, given that a district court opinion is not binding precedent. *See RLJCS Enters.*, 487 F.3d at 499. This would seem to be especially true of a trial court pronouncement on appellate court jurisdiction.

[92] With government consent, one creative magistrate appointed CJA counsel to represent the unnamed cell phone user at a hearing on the government's application for prospective cell site data. *In re* Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register, 415 F. Supp. 2d 211, 212 (W.D.N.Y. 2006). Explicit statutory authority for appointed counsel in such situations would help resolve the difficulty.

[93] Even if the law-abiding citizen were to break through the barrier of secrecy, there is little remedy for a statutory violation that does not rise to the level of a constitutional wrong. There is no civil action against the United States for a statutory violation, 18 U.S.C. § 2707(a) (2006), and a provider's good faith reliance upon a court order is an absolute defense, *id.* § 2707(e).

criminal defendants might learn about the order after the fact, assuming the government deems the information material to the prosecution and turns it over; however, they have no reason to challenge the order post-execution because the statute provides no suppression remedy.[94] The inevitable result is that appellate courts are rarely presented with the opportunity to interpret and apply ECPA's complex provisions.

Lack of appellate review is unhealthy for any regulatory scheme, especially one designed to check executive power. Every statute has its rough edges of ambiguity and gaps of uncertainty. These flaws are brought to light and repaired, day by day, case by case, through lower court rulings subject to review and correction by the courts of appeal, and, ultimately, by the Supreme Court. If Congress deems the Supreme Court's handiwork contrary to the will of the people or the good of the nation, then it is free (within constitutional limits) to change course and amend the statute. The whole process then starts anew.[95]

Under ECPA's secrecy regime, law enforcement occupies a privileged position. As new surveillance technology is developed that pushes the boundaries of existing law, law enforcement is free to expand its scope of operation unimpeded by the normal process of adversarial adjudication. The careful balance between privacy and security set by Congress is inevitably washed away by a torrent of secret orders, unrestrained by the usual adversarial and appellate processes. The longer such surveillance tools are employed without effective judicial oversight, the more familiar they become; familiarity breeds acceptance;[96] and with such acceptance our reasonable expectations of privacy—and hence our Fourth Amendment protections—continue to shrink. With that in mind, we turn to possible ways to remedy the situation.

IV. A Prescription for Transparency

Perfect transparency in criminal investigations is neither practical nor desirable, but ECPA's present system of gagging and sealing is surely overkill. If my diagnosis—that ECPA's regime of secrecy has choked off the oxygen of appellate review necessary for a healthy regulatory scheme—is correct, then the cure is relatively straightforward: open up the information arteries. Greater transparency would enable meaningful oversight not only by appellate courts but also by Congress and the general public. The pre-

[94] A constitutional suppression remedy is available if the evidence was obtained in violation of the Fourth Amendment, of course. But the focus of such a challenge is not statutory interpretation, but rather the strictures of the Fourth Amendment and its relevant case law.

[95] *See generally* Adrian Vermeule, *Second Opinions and Institutional Design*, 97 Va. L. Rev. 1435, 1439–40 (2011) (noting that "judicial review is a mechanism for ensuring a 'sober second thought' in the law-making process" (quoting Harlan F. Stone, *The Common Law in the United States*, 50 Harv. L. Rev. 4, 25 (1936)) (citing Alexander M. Bickel, The Least Dangerous Branch 26 (2d ed. 1986))).

[96] *See* Kyllo v. United States, 533 U.S. 27, 40 (2001) (Fourth Amendment warrant protection limited to surveillance devices that are "not in general public use").

scription offered below would accomplish this in three ways: (a) notifying targets and affected individuals, (b) opening court files to the public, and (c) gathering better surveillance data for Congress.

A. Removing the Gag

Individuals targeted by electronic surveillance are kept unaware by the presence of gag orders silencing their service providers, and by the absence of any notice requirements. In these ways, law-abiding citizens never charged with a crime are prevented from ever learning of government intrusions into their electronic lives.

To remedy this defect, the ECPA should be amended to require notice to the target of any electronic surveillance order, including the customer, subscriber, or user of a targeted phone or Internet service. This proposal is not novel.[97] Such notice is already routine for ordinary search warrants under Rule 41, intercept orders under the Wiretap Act, and certain 2703(d) orders.[98] Delay of notice might be authorized in the limited circumstances already listed in the SCA,[99] although extension periods should be limited and repeat requests carefully scrutinized.

Routine gag orders should be eliminated. In the unusual case where such an order might be warranted, it should be justified on the same grounds as the delay of notification provisions described above.

Of course, notice to the customer or user will accomplish little if he has no standing to challenge electronic surveillance orders, whether pre- or post-execution. The ECPA should be amended to allow affected customers, subscribers, and users a meaningful opportunity to challenge orders issued in violation of ECPA's rules and procedures.[100] Only such an adversarial process will generate the appellate review necessary to enable the judicial branch to fulfill its institutional responsibility as a check on executive power.

---

[97] *See* Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now?: Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact*, 26 BERKELEY TECH. L.J. (forthcoming Mar. 2012) (proposing notice for those individuals whose location information is obtained by law enforcement agencies), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1845644.

[98] *See supra* text accompanying notes 14, 82, 87.

[99] 18 U.S.C. § 2705(b) (2006).

[100] Some have recommended a statutory suppression remedy. *See, e.g.*, Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9 (2004). This is fine for those eventually charged with crime, but does nothing for law-abiding citizens subjected to this governmental intrusion. At a minimum some form of statutory penalty would seem appropriate, perhaps coupled with injunctive relief and attorneys' fees.

B. Removing the Seal

The public has no way to evaluate, much less have confidence in, sealed court orders.[101] From the standpoint of the ordinary citizen, electronic surveillance is among the most intrusive governmental activities a court can authorize,[102] yet it is also the most likely to be hidden from public view.

Congress should amend ECPA to eliminate automatic sealing for electronic surveillance applications, orders, and docket sheets. This is already the law regarding docket sheets in general.[103] It is also already the law for 2703(d) orders under the SCA, which makes no provision for sealing.

Pen/trap applications and orders largely consist of many pages of boilerplate, with only a paragraph or two of factual detail (if that).[104] Redaction of target-identifying information would almost always suffice to avoid jeopardizing the particular surveillance or the investigation as a whole. In the unusual case where sealing a case file or document is necessary, a court should issue a sealing order that (1) contains findings to justify the sealing, (2) explains why narrower alternatives such as redaction or sealing only a single document would not be feasible or effective, and (3) sets a time limit or mechanism for lifting the seal when it is no longer justified.[105] At a minimum, however, basic information about the surveillance—such as the requesting agency, the type of crime under investigation, and other cover sheet data discussed in the next section—should almost always be accessible to the public.

---

[101] *See* Hicklin Eng'g, L.C. v. Bartell, 439 F.3d 346, 348 (7th Cir. 2006) (Easterbrook, J.) ("The political branches of government claim legitimacy by election, judges by reason. Any step that withdraws an element of the judicial process from public view makes the ensuing decision look more like fiat and requires rigorous justification.").

[102] *See* United States v. Jones, 132 S. Ct. 945, 955–56 (2012) (Sotomayor, J., concurring).

[103] Secret dockets have regularly been condemned as a violation of the public's right of access under the First Amendment. *See, e.g.*, United States v. Ochoa-Vasquez, 428 F.3d 1015, 1030 (11th Cir. 2005); Hartford Courant Co. v. Pellegrino, 380 F.3d 83, 93–96 (2d Cir. 2004).

[104] A few examples of unsealed applications from the Southern District of Texas, now available on PACER, are sufficient to make the point: Application for Order Authorizing Installation & Use of Pen Registrar & Trap & Trace Device, United States v. Pen Registrar, 4:10-mj-01004-1 (S.D. Tex. Nov. 13, 2010), ECF 1; Application for Order Authorizing Installation & Use of Pen Registrar & Trap & Trace Device, United States v. Pen Registrar, 4:10-mj-00374-1 (S.D. Tex. Apr. 29, 2010), ECF 1; Application for Order Authorizing Installation & Use of Pen Registrar & Trap & Trace Device, United States v. Pen Registrar, 4:09-mj-00493-1 (S.D. Tex. June 25, 2009), ECF 1; Application for Use of Pen Register & Trap & Trace Device, United States v. Pen Registrar, 4:09-mj-00282-1 (S.D. Tex. Apr. 10, 2009), ECF 1; Application for Use of Pen Register & Trap & Trace Device, United States v. Pen Registrar, 4:08-mj-00798-1 (S.D. Tex. Nov. 18, 2008), ECF 1.

[105] The Judicial Conference of the United States recently adopted each of these requirements for the sealing of entire civil cases. *Conference Approves Standards & Procedures for Sealing Civil Cases*, U.S. COURTS (Sept. 13, 2011), http://www.uscourts.gov/news/Newsview/11-09-13/Conference_Approves_Standards_Procedures_for_Sealing_Civil_Cases.aspx (on file with the Harvard Law School Library). Another possible alternative to sealing would be limiting remote electronic access to the case file, as is currently done in Social Security and immigration cases. *See* FED R. CIV. P. 5.2(c).

C. Removing the Blindfold

The FJC study demonstrated not only that secrecy is a significant problem in warrant-type cases, but also that the true dimensions of the problem are concealed by the lack of systemic data. Blindfolded in this manner, neither Congress nor the public can accurately assess the breadth and depth of current electronic surveillance activity; as a result, legislative reforms are likely to be misguided, ineffective, or both. The ECPA should be amended to ensure that the blindfold is removed by requiring complete and accurate reporting about electronic surveillance cases.

Current law already mandates reporting of aggregated statistical data on certain forms of surveillance, such as wiretaps and pen registers.[106] As one commentator has noted, however, these statistics no longer reflect the full range of law enforcement surveillance activity.[107] The most glaring omission is data on the SCA, which law enforcement uses to obtain a broad spectrum of electronic communications data, including email and text messages, IP addresses, cell phone-location tracking, phone records, account records, and other customer and subscriber information. Some commentators have proposed expanding ECPA's reporting requirements to other forms of surveillance, such as location tracking.[108] This proposal contemplates that the Administrative Office of the United States Courts ("Administrative Office" or "AO") would be responsible for compiling and submitting the report to Congress, thereby providing a sound empirical basis for further legislative action.

The idea is a good one and long overdue, but the judicial branch need not await legislative permission to take such action. Aside from the intangible harm that secrecy does to the rule of law, secrecy also has a financial cost, because sealed records are more burdensome for clerk's offices to maintain than open records.[109] Simply as a matter of efficient court administration, therefore, the judiciary has a justifiable interest in gathering accurate docket data to better manage its case flow and monitor significant trends.

One valuable tool long employed for this purpose on the civil side is the "Civil Cover Sheet." This is a one page standard form (JS 44), approved by the Judicial Conference of the United States in 1974, which must be submit-

[106] *See* 18 U.S.C. § 2519 (2006) (wiretaps); 18 U.S.C. § 3126 (2006) (pen/traps). The DOJ has been less than diligent in providing the required pen/trap reports. It failed to make separate annual reports for the years 2004–2008, and issued a combined report in 2010 only after an inquiry by a Senate staffer. *See* David Kravets, *Congress Left in the Dark on DOJ Wiretaps*, WIRED (Feb. 13, 2012), http://www.wired.com/threatlevel/2012/02/congress-in-the-dark/. Something similar happened in 2004, when the DOJ submitted five years of reports in one "document dump." *See* Schwartz, *supra* note 16, at 297. R

[107] Christopher Soghoian, The Law Enforcement Surveillance Gap 3 (unpublished manuscript), *available at* http://ssrn.com/abstract=1806628 ("[M]ost modern surveillance now takes place entirely off the books and the true scale of such activities, which vastly outnumber traditional wiretaps and pen registers, remains unknown.").

[108] *See, e.g.*, Pell & Soghoian, *supra* note 97, at 55–59. R

[109] FJC STUDY, *supra* note 3, at 31. R

ted to the court clerk by any party wishing to initiate a civil action.[110] The form requests eight categories of basic information about the case. It is signed by the attorney initiating the proceeding. This information provides a valuable database for research and monitoring of civil court filings.

A similar cover sheet could readily be employed for warrant-type cases. Only a few basic categories of information need be included:

- Law enforcement agency filing the application
- Jurisdictional authority (i.e., Wiretap Act, SCA, Pen/Trap Statute, FRCP 41, etc.)
- Relief sought (i.e., search warrant, seizure warrant, wire interception, pen register, trap and trace, tracking device, prospective cell site data, historical cell site data, toll records, email contents, customer account records, etc.)
- Type of crime under investigation, if specified
- Recipient of order/warrant (phone company, ISP, etc.), if specified
- Sealing requested? For how long?
- Delayed notice requested? For how long?
- Initial request? If not, provide case numbers for previous or related cases.

This basic information would fit on a single page, to be filled out and signed by a prosecutor associated with the investigation. The burden of providing the information would thus be placed on the party in the best position to provide it. Because the information sought would be little more than a skeletal summary of the application itself, the burden would be minimal.

Data from the warrant cover sheet could be readily aggregated for periodic statistical reports to Congress, as the Administrative Office is already required to do for wiretaps. This data would provide a sounder and more accurate empirical basis for Congress to evaluate how its laws are being used, and how they should be changed.[111] Just as importantly, public disclosure of this data would enable researchers, academics, and other interested parties to study the actual practice under current law and make recommendations to Congress on how to make it more effective (or less abusive, as the case may be). Finally, and most importantly, publication of this data will allow the press and the public to better understand the extent of government intrusion into our digital lives, so that the balance between privacy and law

[110] The Civil Cover Sheet is available at http://www.uscourts.gov/uscourts/FormsAndFees/Forms/JS044.pdf.

[111] *ECPA Reform and the Revolution in Cloud Computing: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 130 (2010) (statement of Fred H. Cate, Professor, Director of Center for Applied Cybersecurity Research, Indiana University) ("Having [surveillance] statistics gives Congress a sound empirical basis on which to evaluate how its laws are being used and whether they need to be changed. It also provides that same information for people such as those of us gathered at this table when making recommendations to Congress. And it provides information to the public and the press so that they know how those laws are being used and to what effect.").

enforcement struck by our elected representatives will more likely reflect the informed will of the people.

V. Conclusion

Ordinary citizens are inclined to give the benefit of the doubt to our zealous and well-meaning officers of the law. But 30,000 secret surveillance orders a year generate a ton of doubt. Keep in mind that this number covers only federal law enforcement; it is unlikely that state and local law enforcement are less active than their federal counterparts.[112] At some point it becomes legitimate to question the proper limits of the modern surveillance state. When so much is done out of public view, how can we know when it has gone too far?

Equally significant is the impact of such secrecy on the judicial branch itself. Open court proceedings have long been considered a cornerstone of the rule of law: "People in an open society do not demand infallibility from their institutions, but it is difficult for them to accept what they are prohibited from observing."[113] Sealing of judicial records is a recent phenomenon in our legal history.[114] It was never a feature of English common law, and was unheard of in this country at the time our Constitution was adopted and for a hundred years thereafter.[115] The Supreme Court first encountered a sealing order in 1915.[116] Over the last quarter century, however, sealing orders have become as common as grass; in my experience, a civil case file without at least one sealed document has become the exception rather than the rule.[117]

The precise scope of the secrecy problem in U.S. courts awaits further study, but enough is known to raise concern. Each year, federal magistrate judges issue tens of thousands of orders allowing law enforcement to gain electronic access to the lives of our citizens—who we call, where we go, when we text, what websites we visit, what emails we send, etc. Yet, magistrate judges have no meaningful guidance from appellate courts on how to interpret ECPA's complex provisions. As we have seen, this is not the fault of the appellate courts—they cannot decide appeals never filed. And appeals cannot be filed when parties most affected by secret orders do not

[112] *See* Eric Lichtblau, *Police Are Using Phone Tracking as a Routine Tool*, N.Y. Times, Apr. 1, 2012, at A1 (noting the extensive use of cell phone tracking by local police officials, often without judicial oversight).

[113] Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555, 571–72 (1980).

[114] See Smith, *supra* note 70, at 197–207, for a general history of judicial sealing in the United States. R

[115] One of the first opinions to seal court proceedings was issued by the Rhode Island Supreme Court in 1893. *In re* Caswell, 29 A. 259 (R.I. 1893).

[116] *Ex parte* Uppercu, 239 U.S. 435 (1915) (granting writ of mandamus to allow access to discovery materials in another case sealed by court order with consent of the parties).

[117] *See also* Kristen Rasmussen, *Uncivil Secrecy*, 35 The News Media & the Law 30 (Fall 2011), *available at* http://www.rcfp.org/browse-media-law-resources/news-media-law/news-media-and-law-fall-2011/uncivil-secrecy.

know about them. The result is a statutory scheme bereft of the normal process of refinement and correction by appellate review. As new technology is developed, courts are inevitably presented with a one-sided view of how existing law should apply—the side of law enforcement. The outcome is not hard to predict.

Congress faces a formidable task in deciding which substantive reforms to the ECPA are necessary to keep up with new technology and to strike the appropriate balance between privacy and security for the new century. Equally important are the structural reforms needed to ensure that, going forward, Congress and the judiciary will be able to monitor and maintain the new line between privacy and law enforcement, wherever that line is drawn. That will require the elimination of ECPA's current gag, seal, and blindfold.