NOTES

Surveillance Technology and Graymail in Domestic Criminal Prosecutions

CHARLES M. BELL*

ABSTRACT

Following World War II, the expansion of the bureaucratized intelligence services and the Federal Bureau of Investigation resulted in the development and refinement of evidentiary privileges to protect intelligence and law enforcement sources and methods from disclosure at trial. In cases involving the intelligence services and the national security establishment, the clash between these evidentiary privileges and defendants' discovery rights resulted in "graymail"—the trial tactic of forcing prosecutors into a dilemma between dismissing charges or disclosing sensitive or classified information about their sources and methods. The Classified Information Procedures Act has, for the most part, solved the problem of graymail with regard to classified information by prescribing workable procedures for its disclosure in evidence. However, law enforcement sources and methods that are sensitive but unclassified are protected by the law enforcement evidentiary privilege, and thus still subject to graymail. Law enforcement's increased use of secret surveillance technology like cell site simulators and zero-day vulnerabilities has exacerbated the problem of graymail in domestic criminal prosecutions. In the Playpen cases, a series of prosecutions arising from a sting of a child pornography ring, the FBI retroactively classified the source code of the Network Investigative Technique (NIT) the Bureau used to hack the Playpen dark web server. As a result, the Playpen cases offer a unique opportunity to observe graymail tactics in nearly identical cases both with and without CIPA's mechanism for controlled disclosure. CIPA's success in mitigating graymail in the Playpen cases argues that an analogous statutory mechanism for controlled disclosure would be the best way to mitigate the potential for graymail in other cases involving secret, but unclassified, law enforcement sources and methods.

TABLE OF CONTENTS

* J.D., Georgetown University Law Center, 2018.

INTRODUCTION

The Playpen cases are a series of prosecutions arising from an FBI sting of the eponymous child pornography website. During the sting, dubbed Operation Pacifier, the FBI operated the Playpen website for two weeks in early 2015.[1] The FBI altered the website's code to implant a malware on any computer used to visit the website. This malware, euphemistically termed a Network Investigative Technique (NIT), transmitted identifying details about the affected computers to the FBI.[2]

1. *See* Nicole Siino, *The FBI's "Operation Pacifier" Attempted to Catch Child Pornography Viewers but Courts Inquire into the Validity of the Search Warrant*, J. OF HIGH TECH. L. (Oct. 29, 2016), https://sites.suffolk.edu/jhtl/2016/10/29/the-fbis-operation-pacifier-attempted-to-catch-child-pornography-viewers-but-courts-inquire-into-the-validity-of-the-search-warrant/ [https://perma.cc/W2AU-6Q47].

2. *See* Susan Hennessey & Nicholas Weaver, *A Judicial Framework for Evaluating Network Investigative Techniques*, LAWFARE (July 28, 2016, 10:17 AM), https://www.lawfareblog.com/judicial-framework-evaluating-network-investigative-techniques [https://perma.cc/9WMU-9WWR].

FBI agents identified thousands of computers worldwide using this NIT. As of May 5, 2017, 350 have been arrested in the United States in connection with Playpen.[3] At least 137 Playpen users have been prosecuted.[4]

Some of these prosecutions have been stymied by graymail defenses.[5] A graymail defense seeks to disclose, or compel the government to disclose, information protected by classification or evidentiary privilege. If the government is unwilling to allow disclosure, the protected information may be inadmissible as evidence, requiring dismissal of some or all charges.

This note posits that the law enforcement evidentiary privilege that has enabled graymail in the Playpen cases has developed in parallel with a related privilege, the state secrets privilege. Part I will discuss the problem of graymail in cases involving the state secrets privilege and describe how the Classified Information Procedures Act (CIPA)[6] has mitigated the risk of graymail in such cases. Part II will discuss the problem of graymail in cases involving the law enforcement evidentiary privilege. Part III compares two Playpen cases, *United States v. Michaud* and *United States v. Tippens*, to illustrate how graymail defenses fare in cases where CIPA procedures allow for controlled disclosure and in cases where, in the absence of a statutory procedure, law enforcement evidentiary privileges alone do not. This note concludes by arguing that a statutory mechanism for controlled disclosure would be the best approach to limiting graymail in cases involving secret law enforcement methods.

I. THE PROBLEM OF GRAYMAIL IN CASES INVOLVING THE STATE SECRETS PRIVILEGE

A. The Reynolds *State Secrets Privilege*

The state secrets privilege is an evidentiary privilege that protects state secrets, whose disclosure would harm national security, from being divulged during trial. Though based on older legal doctrines, the state secrets privilege was first formally recognized by the Supreme Court in *United States v. Reynolds*.[7] As a result, the state secrets privilege is commonly known in the United States as the *Reynolds* privilege.

The *Reynolds* privilege may be invoked in any case in which the government might be compelled to disclose state secrets. The privilege may only be asserted or waived by the government, although the government may assert the *Reynolds* privilege to intervene to protect third parties from compelled disclosure.[8]

---

3. *See* FBI, *'Playpen' Creator Sentenced to 30 Years* (May 5, 2017), https://www.fbi.gov/news/stories/playpen-creator-sentenced-to-30-years [https://perma.cc/MH87-L39E].

4. Joseph Cox, *Dozens of Lawyers Across the US Fight the FBI's Mass Hacking Campaign*, MOTHERBOARD (Jul. 27, 2016), https://motherboard.vice.com/en_us/article/dozens-of-lawyers-across-the-us-fight-the-fbis-mass-hacking-campaign-playpen [https://perma.cc/343D-33FA].

5. *See* Hennessey & Weaver, *supra* note 2.

6. 18 U.S.C. app. 3 §§ 1–16.

7. *See* United States v. Reynolds, 345 U.S. 1 (1953).

8. This typically occurs in cases involving government contractors. *See, e.g.*, Mohamed v. Jeppesen Dataplan, 614 F.3d 1070 (9th Cir., 2010).

Asserting the privilege is a two-step process. First, "[t]here must be formal claim of privilege, lodged by the head of the department which has control over the matter, after actual personal consideration by that officer."[9] The court must then determine, typically in camera, whether the asserted privilege is appropriate. If so, disclosure of the protected information cannot be compelled.

A related doctrine known as the *Totten* bar precludes courts from trying civil cases in dispute in which the underlying matter of the case is a state secret.[10] In *Totten v. United States*, the Supreme Court upheld dismissal of a suit involving a contract between President Lincoln and the plaintiff for the latter to spy on the Confederates. Suits in which *Totten* bars justiciability are rare, but generally involve either the intelligence services or military contractors.[11] Unlike the *Totten* bar, a successful assertion of the *Reynolds* privilege "does not automatically require dismissal of the case. In some instances, however, the assertion of privilege will require dismissal because it will become apparent during the *Reynolds* analysis that the case cannot proceed without privileged evidence, or that litigating the case to a judgment on the merits would present an unacceptable risk of disclosing state secrets."[12]

Although its formal recognition of the state secrets privilege dealt with military secrets, the 1953 *Reynolds* decision roughly coincided with two events that would increase its subsequent importance. The first event was the beginning of the Cold War as the victorious allies of World War II fractured into rival Western and Eastern blocs.[13] The second was the 1947 establishment of the Central Intelligence Agency. The CIA organized and institutionalized human intelligence activities that had previously been undertaken largely by individual officials, acting on their own, since the beginning of the republic.[14] In addition to cultivating human intelligence sources, the CIA developed its own specialized surveillance technologies and adapted technical surveillance methods from the military, which also continued to develop surveillance technologies for military intelligence purposes. As the superpowers waged the Cold War not only with strategic nuclear détente and proxy war but also with espionage and covert action, the state secrets held by the growing intelligence community—its sources and methods—came to rival those held by the military.

---

9. United States v. Reynolds, 345 U.S. 1, 7–8 (1953).

10. Totten v. United States, 92 U.S. 105 (1876); *see also, e.g.*, Tenet v. Doe, 544 U.S. 1 (2005).

11. *See, e.g.*, *Totten*, 92 U.S. at 105; *Tenet*, 544 U.S. at 1; General Dynamics Corp. v. United States, 563 U.S. 478 (2011); El-Masri v. United States, 479 F.3d 296 (4th Cir. 2007).

12. *Jeppesen Dataplan*, 614 F.3d at 1079.

13. The beginning of the Cold War has been dated to Churchill's 1946 "Sinews of Peace" speech or the 1947 Truman Doctrine. *See generally* Winston Churchill, The Sinews of Peace, Address at Westminster College (Mar. 5, 1946), *in* SOURCES OF WORLD HISTORY 298–302 (Mark A. Kishlansky ed.,1995); H.R. Doc. No. 171 (1947).

14. Notably, George Washington and Abraham Lincoln both employed spies. *See generally* ALEXANDER ROSE, WASHINGTON'S SPIES: THE STORY OF AMERICA'S FIRST SPY RING (2006); *Totten*, 92 U.S. at 105.

B. The Disclose or Dismiss Dilemma in State Secrets Cases

The *Reynolds* privilege may be invoked in both civil and criminal trials. This presents a dilemma in criminal prosecutions where charges are based on state secrets. If the government invokes the state secrets privilege to avoid disclosure, there would be insufficient evidence for the prosecution to proceed, requiring dismissal. This "disclose or dismiss" dilemma occurs in two types of cases. The first type of case is when the crime itself involves state secrets. This might be, for example, a crime involving unauthorized disclosure of classified information.[15] Alternately, it might involve misconduct by members of the military or the intelligence community, or other national security officials acting in their official capacities.[16] In these types of cases, defendants are generally "insiders" who already have access to the state secrets at issue.[17]

The second type of case occurs when the crime is detected using secret sources or methods. These methods are often not only the best, but the only available techniques to detect certain crimes. The classic example of such crimes is a terrorist conspiracy revealed by, for instance, a human intelligence source or signals intelligence. In contrast to defendants in the first type of case, these defendants are generally "outsiders" who do not have access to the state secrets at issue.

The disclose or dismiss dilemma gives rise in both types of cases to graymail defense tactics. In insider cases, a graymail defense seeks to force the prosecution to dismiss the case to prevent the defendant from disclosing state secrets already in his or her possession during trial. This was the type of graymail employed by Oliver North during his prosecution for crimes in the Iran/Contra affair[18] and I. Lewis "Scooter" Libby during his prosecution for leaking the covert identity of CIA officer Valerie Plame Wilson.[19]

In outsider cases, a graymail defense seeks to force the prosecution to dismiss the case by compelling the government to disclose state secrets. Criminal defendants have several discovery rights available to compel such disclosure.[20] Under *Brady v. Maryland*, due process requires prosecutors to disclose material exculpatory evidence to the defense.[21] *Giglio v. United States* extends this requirement

---

15. *See, e.g.*, United States v. Rosen, 557 F.3d 192 (4th Cir. 2009), in which the defendant provided classified defense information to Israel in violation of 18 U.S.C. § 793.

16. *See, e.g.*, United States v. North, 910 F.2d 843 (D.C. Cir. 1990).

17. John D. Cline & K.C. Maxwell, *Criminal Prosecutions and Classified Information*, L.A. LAWYER 35 (Sept. 29, 2006). Author John D. Cline was defense counsel for both Oliver North and Scooter Libby, among other graymail defendants, and is an amicus curiae to the Foreign Intelligence Surveillance Court.

18. *See North*, 910 F.2d at 898–99; LAWRENCE WALSH, 1 FINAL REPORT OF THE INDEPENDENT COUNSEL FOR IRAN/CONTRA MATTERS 108–111 (1993), available at https://archive.org/details/WalshReport [hereinafter WALSH REPORT] [https://perma.cc/5RDJ-K2NT].

19. *See generally* United States v. Libby, 467 F. Supp. 2d 1 (D.D.C. 2006).

20. *See generally* Jonathan M. Fredman, *Intelligence Agencies, Law Enforcement, and the Prosecution Team*, 16 YALE L. & POL'Y REV. 331 (1998).

21. *See* Brady v. Maryland, 373 U.S. 83, 87–88 (1963).

to evidence that could impeach government witnesses.[22] The Jencks Act requires prosecutors to disclose witnesses' statements made in direct examination for cross-examination by the defense.[23] Federal Rule of Criminal Procedure 16 requires the government to disclose any statements made by the defendant in the government's possession.[24]

A typical graymail defense in an outsider case involves a motion to compel discovery of information that is classified or otherwise protected by the *Reynolds* privilege. This motion might be based on a good faith belief by the defense that the information requested is both material and exculpatory, or it might merely be a tactic calculated to force the government to assert the state secrets privilege.[25] In either case, the graymail is equally effective: the court is placed in the untenable position of balancing the defendant's discovery rights against the government's *Reynolds* privilege. The only way to protect both without compromising either is for the court or the prosecution to dismiss the charges.

C. The Classified Information Procedures Act

The Classified Information Procedures Act (CIPA) was designed to counter the effectiveness of graymail by establishing procedures for the controlled disclosure of classified information during criminal trials. CIPA features two sets of procedures for the disclosure of classified information: one for disclosure by the defense of classified information in its possession, the other for compulsory disclosure by the prosecution. After indictment, the court holds a pretrial conference, on motion by any party, to consider matters related to classified information. The court then issues a protective order that generally prohibits disclosure of classified information, subject to later exceptions; establishes case-specific procedures for handling classified material and filing classified pleadings; and appoints a Court Security Officer to assist both sides with access to classified information.[26] These procedures may include requirements for members of the defense team to obtain security clearances and for classified material to be stored and viewed in a secure Sensitive Compartmentalized Information Facility (SCIF).[27]

CIPA Section 4 governs the defendant's discovery of classified information. Rather than barring disclosure of classified information entirely, as if the *Reynolds* privilege were invoked, the court has several options to permit full or partial disclosure of classified information to the defense. The court can permit the government to provide redacted documents with classified information

22. *See* Giglio v. United States, 405 U.S. 150, 154 (1972).

23. 18 U.S.C. § 3500.

24. FED. R. CRIM. P. 16(a)(1)(A)–(B).

25. *See* S. REP. NO. 96-823, 4296–97 (1980) ("It would be a mistake, however, to view the 'graymail' problem as limited to instances of unscrupulous or questionable conduct by defendants since wholly proper defense attempts to obtain or disclose classified information may present the government with the same 'disclose or dismiss' dilemma.").

26. Cline & Maxwell, *supra* note 17, 37–38; 18 U.S.C. app. 3 § 3.

27. Cline & Maxwell, *supra* note 17, at 38.

deleted. Alternately, the court can allow the government to provide an unclassified summary of the classified information sought, or to stipulate the relevant facts that the classified information sought would tend to prove.[28] These procedures limit the effectiveness of outsider-style graymail by allowing a conditional, controlled disclosure of classified information.

CIPA Sections 5 and 6 provide procedures for the defense to disclose classified information. The defense must provide notice to the court. On motion by the government, the court must hold a hearing in camera to determine the information's use, relevance, and admissibility using ordinary evidentiary standards. If the court finds the classified material admissible, it may permit the government to substitute an unclassified summary or stipulate the facts the classified information would tend to prove.[29]

Paradoxically, CIPA also codifies the disclose or dismiss dilemma. Section 9A of CIPA requires prosecutors to coordinate the prosecution with other federal agencies that might be affected by disclosure of classified information. This coordination entails initial and subsequent briefings to "keep the senior agency official concerned fully and currently informed of the status of the prosecution."[30] Section 12 requires the Attorney General to promulgate guidelines for "rendering a decision whether to prosecute a violation of Federal law in which . . . there is a possibility that classified information will be revealed."[31] If the required coordination indicates that prosecution could involve disclosure of classified information, the Justice Department determines, in accordance with the Attorney General's guidelines, whether the risk to national security from that potential disclosure is too great to continue the prosecution.

CIPA was designed to alter the *procedures* used by courts to handle classified information in criminal trials, not the substantive rights of defendants or the government's state secrets privilege.[32] As such, there are a number of problems CIPA does not purport to address. First, CIPA does not apply in civil cases.[33] Second, in criminal cases, CIPA does not apply to all state secrets, but only to classified information, defined as "any information or material that has been determined by the United States Government pursuant to an Executive order, statute, or regulation, to require protection against unauthorized disclosure for reasons of national security and any restricted data, as defined in paragraph r. of section 11 of the Atomic Energy Act of 1954."[34] Finally, and most importantly, CIPA does not

28. 18 U.S.C. app. 3 § 4.
29. *Id.* § 6(c)(1).
30. *Id.* § 9A.
31. *Id.* § 12.
32. *See, e.g.*, United States v. Anderson, 872 F.2d 1508, 1514 (11th Cir. 1989); United States v. Smith, 780 F.2d 1102, 1106 (4th Cir. 1985); United States v. Collins, 720 F.2d 1195, 1199 (11th Cir. 1983).
33. The State Secrets Protection Act of 2008, S. 2533, would have established a CIPA-like framework for controlled disclosure of classified information in civil suits.
34. 18 U.S.C. app. 3 § 1(a) (internal citations omitted).

attempt to balance statutorily the interests between the defendant's discovery rights and the government's state secrets privilege.

Even CIPA's critics concede that it has been effective at preventing graymail, though the full extent of its success is unclear.[35] The extent of the graymail problem before and after the passage of CIPA is difficult to measure because it is in neither the defendant's nor the government's interest to publicize that a prosecution has been discontinued due to graymail.[36] At the time of its passage, CIPA's advocates estimated that there were only five to ten graymail cases per year.[37] Moreover, CIPA procedures are chiefly useful in preventing graymail by outsiders, not insiders. Because defendants in insider cases already possess classified information, they can still mount a graymail defense by threatening to disclose the classified information outside of the judicial system through, for instance, congressional testimony or anonymous leaks.[38] Graymail by an insider defendant can also overwhelm the court's ability to process the defense's requests to disclose classified information. This latter tactic was successful in the trial of Oliver North, whose defense team sought to introduce classified information the mere description of which was 265 pages.[39] Ultimately, the prosecution dropped the most serious charges against North due to classification problems.[40]

II. THE PROBLEM OF GRAYMAIL IN CASES INVOLVING LAW ENFORCEMENT EVIDENTIARY PRIVILEGE

A. The Roviaro *Informer's Privilege*

Unlike the relatively monolithic *Reynolds* state secrets privilege, which protects both intelligence sources and methods, the law enforcement evidentiary privileges that protect confidential informants and investigative techniques have developed separately but in parallel. In *Roviaro v. United States*, the Supreme Court recognized the government's privilege to withhold the identities of confidential informants.[41] Citizens have a constitutional right, and a moral obligation, to report known criminal activity to law enforcement.[42] The informer's privilege, "by preserving their anonymity, encourages them to perform that obligation."[43] The *Roviaro* privilege is far from absolute, however; all that is required to overcome the privilege is a showing that the information sought would be "relevant

35. *See* Cline & Maxwell, *supra* note 17, at 41.

36. *Use of Classified Information in Federal Criminal Cases: Hearings on H.R. 4736 Before the Subcomm. on Civil and Constitutional Rights of the House Comm. on the Judiciary*, 96th Cong., 2d Sess. 3 (1980) (statement of Philip Heymann), cited in Richard P. Salgado, *Government Secrets, Fair Trials, and the Classified Information Procedures Act*, 98 YALE L.J. 427, 429–30 n.20 (1988).

37. Salgado, *supra* note 36, at 429–30 n.20.

38. *See* United States v. Pappas, 94 F.3d 795, 800 (2d Cir. 1996).

39. WALSH REPORT, *supra* note 18, at 108–111. Judge Gesell noted that CIPA "was ill-suited to a case of this type." United States v. North, 713 F. Supp. 1452, 1452 (D.D.C. 1989).

40. WALSH REPORT, *supra* note 18, at 110.

41. *See generally* Roviaro v. United States, 353 U.S. 53 (1957).

42. *Id.* at 59.

43. *Id.*

and helpful" to the defense.[44] The purpose of the *Roviaro* informer's privilege is not to protect law enforcement investigative techniques, but to protect individual informers who might suffer retaliation if their identities were known.[45] However, the informer's privilege and the "relevant and helpful" standard of admissibility delineated in *Roviaro* have shaped subsequent decisions recognizing a privilege for law enforcement techniques.

B. The Freedom of Information Act Law Enforcement Exemption

Besides *Roviaro*, another major influence on the development of a law enforcement evidentiary privilege was the Freedom of Information Act of 1966 (FOIA) and its subsequent amendments.[46] FOIA aims to increase government transparency by giving citizens the right to obtain information from government agencies. Like the state secrets privilege, the passage of FOIA may be attributed to the post-World War II expansion of the federal bureaucracy, particularly the bureaucratized intelligence services.[47] FOIA requires executive branch agencies to provide certain information on request, subject to a number of exceptions listed in paragraph (b).

Classified information is exempt from FOIA disclosure under (b)(1). Law enforcement information is exempt from FOIA disclosure under (b)(7) to the extent that it would, among other things, reveal the identity of a confidential source or law enforcement techniques and procedures, if disclosure would risk circumvention of the law.[48] These reasons for exempting law enforcement information from FOIA disclosure are strikingly similar to the reasons underlying the *Reynolds* privilege's protection of intelligence sources and methods whose disclosure would harm national security. Although the law enforcement exemption to FOIA does not create a judicial rule of evidence, it became a cornerstone of the judicially created law enforcement privilege.[49] Kenneth Graham notes that the FOIA exemption "marks the outer limits of the [law enforcement] privilege" since it would be absurd to exclude information from use in court when it could be obtained for any other purpose via FOIA.[50]

C. The Law Enforcement Evidentiary Privilege[51]

In *Black v. Sheraton Corp. of America*, the D.C. Circuit became the first federal appellate court to recognize the law enforcement evidentiary privilege as a distinct subspecies of the executive privilege protecting law enforcement sources

---

44. *Id.* at 60–61.

45. Stephen Wm. Smith, *Policing Hoover's Ghost: The Privilege for Law Enforcement Techniques*, 54 AM. CRIM. L. REV. 233, 258 (2017).

46. 5 U.S.C. § 552.

47. Smith, *supra* note 45, at 247.

48. 5 U.S.C. § 552(b)(7).

49. KENNETH W. GRAHAM, JR., 26A FED. PRAC. & PROC. EVID. § 5683, Westlaw (1st ed.).

50. *Id.* § 5681.

51. See generally Smith, *supra* note 45, for a thorough exploration of the history and development of the law enforcement privilege.

and methods from disclosure.[52] In *United States v. Green*, the D.C. Circuit extended the law enforcement privilege to criminal proceedings.[53] Notably, *Green* blurs the line between protecting confidential informants and secret investigative techniques. The information sought by the defendant in *Green* was the location of a hidden police observation post, disclosure of which would have revealed the identity of the property owner who cooperated with police by permitting them to occupy the observation post. In analogizing a "surveillance location privilege" from the *Roviaro* informer's privilege, the *Green* opinion misconstrues *Roviaro*'s holding by making too much of *Rovario*'s policy argument.[54] In *Roviaro*, the informer's privilege serves to protect the informant from retaliatory harm rather than to protect his future usefulness to police. The *Roviaro* court considers the risk of harm to future investigations only to the extent that, if there were no informer's privilege, and prosecutors were compelled to disclose the identities of confidential informants, no one would inform out of fear of violent reprisal.[55] In *Green*, on the other hand, the risk to future investigations is of first importance:

> Like confidential informants, hidden observation posts are often useful law enforcement tools, so long as they remain secret. Just as the disclosure of an informer's identity may destroy his future usefulness in criminal investigations, the identification of a hidden observation post will likely destroy the future value of that location for police surveillance.[56]

In *United States v. Van Horn*, the Eleventh Circuit adopted the *Green* law enforcement evidentiary privilege for secret surveillance techniques, this time involving electronic surveillance by means of microphones hidden in the defendant's own office.[57] Since the surveillance did not implicate a third party's cooperation, as did the observation post in *Green*, the court's reasoning in *Van Horn* did not rely on the informer's privilege at all. The court's policy rationale for a law enforcement evidentiary privilege was to protect the efficacy of police surveillance techniques: "Disclosing the precise locations where surveillance devices are hidden or their precise specifications will educate criminals regarding how to protect themselves against police surveillance. Electronic surveillance is an important tool of law enforcement, and its effectiveness should not be unnecessarily compromised."[58]

---

52. *See* Black v. Sheraton Corp. of America, 564 F.2d 531, 541 (D.C. Cir. 1977); Smith, *supra* note 45, at 259.

53. *See* United States v. Green, 670 F.2d 1148, 1150 (D.C. Cir. 1981); Smith, *supra* note 45, at 260.

54. *Green*, 670 F.2d at 1155.

55. *See* Smith, *supra* note 45, at 258 ("[T]he *Roviaro* informer's privilege has little to do with safeguarding law enforcement techniques for future use. . . . Rather, the concern is to protect this particular John Doe 'from those who would have cause to resent his conduct[,]' or, as the dissent more bluntly puts it, 'Dead men tell no tales.'").

56. *Id*.

57. United States v. Van Horn, 789 F.2d 1492, 1507 (11th Cir. 1986).

58. *Id*. at 1508.

Judge Stephen Smith credits J. Edgar Hoover as the father of the law enforcement privilege.[59] Hoover modernized the FBI to use the most scientific and advanced methods of crime detection—the best surveillance technology of his day. He also used those methods illegally to surveil public figures and political dissidents, activities he wished to keep out of the public view. These practices, combined with the Bureau's dual role as law enforcement and domestic counter-intelligence, made the extension of a state secrets-like privilege to law enforcement a natural and perhaps foreseeable result of law enforcement's adoption of intelligence methods. Coincidentally, the law enforcement technique at issue in *Black v. Sheraton Corp. of America*, the case which first recognized a privilege protecting law enforcement techniques, was an illegal FBI wiretap.[60]

The use of secret surveillance techniques has not been limited to the FBI, nor even to federal law enforcement generally. Since the September 11, 2001 terrorist attacks on the United States, police militarization has trickled down to local law enforcement.[61] Local police have adopted not only military armored vehicles and weapons, but also military signals intelligence and surveillance techniques.[62] In response, savvy criminals have begun to adopt equally sophisticated counter-surveillance techniques, such as strong encryption. This trend has created what has become known as the "going dark" problem, in which law enforcement can obtain the necessary legal authority to intercept communications and access stored digital information but lacks the technical ability to do so.[63] Police find themselves in a digital arms race as surveillance technologies, in turn, innovate to overcome technical surveillance countermeasures.

D. The Disclose or Dismiss Dilemma in Law Enforcement Privilege Cases

The appellate courts' recognition of an evidentiary privilege protecting law enforcement investigative techniques used to detect domestic crimes has brought with it the same kind of disclose or dismiss dilemma seen in *Reynolds* state secrets privilege cases. Cases such as *Green* and *Van Horn* avoided the disclose or dismiss dilemma in part by adopting stricter admissibility standards than the

---

59. *See* Smith, *supra* note 45, at 234.

60. Black v. Sheraton Corp. of America, 564 F.2d 531, 534 (D.C. Cir. 1977); Smith, *supra* note 45, at 259.

61. *See generally* Cadman Robb Kiker III, *From Mayberry to Ferguson: The Militarization of American Policing Equipment, Culture and Mission*, 71 WASH. & LEE L. REV. ONLINE 282 (2015).

62. *See, e.g.*, Jeffrey L. Vagle, *Tightening the OODA Loop: Police Militarization, Race, and Algorithmic Surveillance*, 22 MICH. J. RACE & L. 101 (2016).

63. *See* James Comey, Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course? (Oct. 16, 2014), https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course [https://perma.cc/NK6Z-7458]; *but see* BERKMAN CENTER FOR INTERNET & SOCIETY AT HARVARD UNIVERSITY, DON'T PANIC: MAKING PROGRESS ON THE "GOING DARK" DEBATE (2016), https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf [https://perma.cc/JB26-QW3L] (arguing that the "going dark" problem is not as serious as Director Comey suggested, because "[m]arket forces and commercial interests will likely limit the circumstances in which companies will offer encryption that obscures user data from the companies themselves").

"relevant and helpful" standard articulated in *Roviaro*.[64] However, the proliferation of law enforcement surveillance technology has the potential to exacerbate the disclose or dismiss dilemma in law enforcement privilege cases. Graymail, once a recourse useful only to spies and terrorists, has become a valid tactic for ordinary criminal defendants.

United States v. Rigmaiden illustrates the use of graymail in a law enforcement privilege case, outside of the context of national security.[65] Daniel Rigmaiden was jailed for tax fraud. Although the technology was not publicly known at the time, the FBI's investigation had employed a cell site simulator device, also known as a Stingray, which allows for geolocation and real-time interception of cellular communications devices such as mobile phones and the aircard Rigmaiden's laptop computer used to connect to the Internet.[66] Rigmaiden moved pro se to discover information in the FBI's possession regarding real-time and historical cellular geolocation and interception techniques, in particular technical specifications of the Stingray device.[67] The government asserted law enforcement privilege. Ultimately, the court held that the information Rigmaiden sought was protected by the law enforcement privilege, citing *Roviaro*, but found that Rigmaiden's defense was not hampered by the FBI's lack of disclosure.[68] *Rigmaiden* may seem like an outlier, but use of cell site simulators by law enforcement was widely unknown at the time. Since then, use of such devices, not only by federal law enforcement agencies, but also by state and local police, has become widespread.[69] It seems only a matter of time before other criminal defendants adopt graymail when police resort to these and similar surveillance technologies.

III. LAW ENFORCEMENT PRIVILEGE AND CIPA IN THE PLAYPEN CASES

The Playpen cases provide a unique opportunity to observe law enforcement privilege and CIPA procedures at work under nearly identical sets of facts involving the use of sophisticated surveillance technology by law enforcement.

A. The Playpen Investigation

Playpen was a so-called "dark web" Tor Hidden Service site. Ordinarily, police can locate computer crime offenders using their Internet Protocol (IP) addresses:

---

64. Smith, *supra* note 45, at 256–64.

65. *See* United States v. Rigmaiden, No. CR 08-814-PHX-DGC, 2013 WL 1932800, (D. Ariz. May 8, 2013).

66. *See* Eric Pait, *Find My Suspect: Tracking People in the Age of Cell Phones*, 2 GEO. L. TECH. REV. 155, 159–160 (2017) (describing cell site simulator technology).

67. Motion for Additional Discovery Due to Government Ignoring Defendant's Recent Discovery Requests, United States v. Rigmaiden, No. CR 08-814-PHX-DGC, 2013 WL 1932800 (D. Ariz. Nov. 10, 2011).

68. *See* United States v. Rigmaiden, No. CR 08-814-PHX-DGC, 2013 WL 1932800, *4 (D. Ariz. May 8, 2013).

69. *See Stingray Tracking Devices: Who's Got Them?*, ACLU, https://www.aclu.org/map/stingray-tracking-devices-whos-got-them [https://perma.cc/E2GK-9UZQ].

numerical addresses which, like phone numbers, can be traced to specific devices, either using publicly-available search tools or by compelling Internet service providers to disclose records connecting IP addresses to particular users' accounts.[70] As a result, many child porn traffickers began using Tor, a network designed to anonymize users' IP addresses through a series of encrypted relays operating over the general Internet.[71] Using a specially-configured version of the Firefox browser, Tor users can anonymously browse ordinary websites, but can also reach Tor Hidden Services that are not available outside of the Tor network. Like users' IP addresses, a Tor Hidden Service's IP address is obscured; users reach a Tor Hidden Service site through a special .onion web address. Although Tor Hidden Services have legitimate, lawful uses, this dark web is frequently used by criminals to trade illegal goods and services.

The Playpen investigation began in 2014, when the FBI received a tip from a foreign law enforcement agency that the Playpen Tor Hidden Service site was, as a result of a temporary incorrect configuration, displaying its actual IP address.[72] The site's operators corrected the configuration, but not before the FBI could observe the IP address, which they traced to a computer physically located in Lenoir, North Carolina. The FBI seized the system and arrested its operators.[73]

Instead of keeping Playpen offline, the FBI applied for, and received, a warrant in the Eastern District of Virginia to operate the server from February 20 through March 4, 2015.[74] Any computer visiting the Playpen site during this period was infected with the FBI's NIT. The NIT transmitted identifying details about the affected computers to the FBI, including the computers' true IP addresses—a technique for which Tor's system of anonymizing relays would be no defense. Although technical details about the NIT have never been officially acknowledged, computer security experts have speculated that it relied on an unpatched code vulnerability in the Tor Firefox web browser.[75] Such vulnerabilities are known as zero-day vulnerabilities because, as they are known only to their discoverers, software publishers have had zero days to correct them and issue a patch to users.

---

70. 18 U.S.C. § 2703(c) allows police to obtain IP address records from service providers using a subpoena, court order, or warrant.

71. Like any measure of secrecy, Tor can, and is, used for purposes both noble and nefarious. Tor was originally developed by the U.S. government for military systems and has been adapted for use by, e.g., whistleblowers and dissidents against repressive regimes. *See* Kyle Swan, *Onion Routing and Tor*, 1 GEO. L. TECH. REV. 110, 110–11 (2016).

72. *See* FBI, *'Playpen' Creator Sentenced to 30 Years* (May 5, 2017), https://www.fbi.gov/news/stories/playpen-creator-sentenced-to-30-years [https://perma.cc/W6X9-NMPF]; Motion and Memorandum in Support of Motion to Suppress Evidence at 3, United States v. Michaud, No. 3:15-cr-05351-RJB, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016).

73. Complaint at 3, United States v. Ferrell, No. 1:15-cr-00331 (E.D.N.Y. Jul 08, 2015).

74. *See* Siino, *supra* note 1.

75. Nicholas Weaver, *The End of the NIT*, LAWFARE (Dec. 5, 2016), https://www.lawfareblog.com/end-nit [https://perma.cc/8GKG-NQNH].

The FBI's NIT collected identifying details about thousands of computers worldwide. The Bureau subsequently subpoenaed Internet service provider records identifying individual account holders for certain of those IP addresses and obtained and executed warrants to search for and seize evidence of child pornography at those account holders' locations.

To say the FBI's use of the NIT was problematic would be an understatement. There are the obvious ethical problems posed by the FBI distributing child pornography, a crime predicated on the continuing harm done to victims each time their likenesses are disseminated. Moreover, numerous challenges to the legality of the NIT warrant have arisen, attacking its territorial jurisdiction and specificity. At the time, Federal Rule of Criminal Procedure 41(b) permitted magistrate judges to grant warrants for searches only within their own districts.[76] Since the warrant authorized the NIT malware to search users' computers anywhere, the warrant was void *ab initio*, the search presumptively unreasonable, and the evidence obtained thereby inadmissible.[77] Since then, Rule 41(b) has been amended to allow magistrate judges to issue warrants authorizing remote searches of computers when their physical locations have been "concealed through technological means."[78] The extraterritoriality defense has succeeded in at least one case, *United States v. Levin*.[79] It has failed in others, such as *United States v. Werdene*, where the court found that suppression was not the correct remedy where officers had acted based on a good faith belief in the warrant's validity, and *United States v. Schuster*, where the court found that suppression was not the appropriate remedy because the subsequent amendment to Rule 41(b) eliminated the deterrent value of suppression by removing the possibility of violating Rule 41(b) in the same way.[80]

Attacks on the NIT warrant's specificity have focused on particularity: the Fourth Amendment requires that warrants particularly describe places to be searched.[81] The warrant did not specify particular computers, but only a general class of computers—those accessing the Playpen website during the duration it was kept online for Operation Pacifier. As such, defendants argue, the warrant lacks the required particularity, amounts to an unconstitutional general warrant, and the evidence obtained under it must be suppressed.[82]

---

76. FED. R. CRIM. P. 41(b) (as of 2015).

77. *See, e.g.*, United States v. Levin, 186 F. Supp. 3d 26, 33–36 (D. Mass. May 5, 2016).

78. FED. R. CRIM. P. 41(b)(6).

79. *See, e.g.*, *Levin*, 186 F. Supp. 3d at 44.

80. *See* United States v. Werdene, 188 F. Supp. 3d 431, 451–53; Order Denying Defendant's Motion to Suppress at 8–9, United States v. Schuster, No. 1:16-cr-00051 (S.D. Ohio May 18, 2016).

81. *See* U.S. CONST. amend. IV.

82. *See, e.g.*, Motion and Memorandum in Support of Motion to Suppress Evidence, United States v. Michaud, No. 3:15-cr-05351-RJB2016, 2016 WL 337263 (W.D. Wash. Oct. 30, 2015).

B. Law Enforcement Privilege Graymail in United States v. Michaud

Several Playpen defendants have successfully pursued a graymail strategy. One such defendant is Jay Michaud, a Seattle schoolteacher. In *United States v. Michaud*, the defense had failed to suppress evidence obtained by the NIT either on the basis that the warrant lacked particularity or that it violated Rule 41(b).[83] Michaud moved to compel discovery of the NIT source code, arguing that source code was relevant to the defense to

> determine the full extent of the information the Government seized from Mr. Michaud's computer when it deployed the NIT; whether the NIT interfered with or compromised any data or computer functions; and whether the Government's representations about the how the NIT works in its warrant applications were complete and accurate.[84]

Regardless of whether Michaud's counsel made this motion in good faith, it was classic outsider graymail.

Judge Robert J. Bryan found that the NIT source code was material to Michaud's defense—a potential "treasure trove of exculpatory evidence"—and granted the motion to compel discovery.[85] In response, the government refused to disclose the NIT source code, claiming that it was subject to law enforcement privilege.[86] As a compromise, Michaud offered to enter into a protective order that would limit review to defense counsel with a security clearance, at a secure government facility, and prohibit public disclosure—substantially the same conditions as might have been imposed by a protective order issued under CIPA Section 3. The court even offered to review the NIT evidence ex parte, in camera under Federal Rule of Criminal Procedure 16(d)(1).[87] The government did not relent.

At that point, the court was faced with a disclose or dismiss dilemma. As Judge Bryan wrote:

> [T]he defendant has the right to review the full N.I.T. code, but the government does not have to produce it. . . . What should be done about it when, under these facts, the defense has a justifiable need for information in the hands of the government, but the government has a justifiable right not to turn the information over to the defense?[88]

---

83. *See* Order Denying Defendant's Motion to Suppress Evidence at *8, United States v. Michaud, No. 3:15-cr-05351-RJB2016, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016).

84. Motion and Memorandum of Law in Support of Motion to Compel Discovery at 1–2, United States v. Michaud, No. 3:15-cr-05351 (W.D. Wash. Jul 23, 2015).

85. Order on Procedural History and Case Status in Advance of May 25, 2016 Hearing at 4, United States v. Michaud, No. 3:15-cr-05351 (W.D. Wash. May 18, 2016).

86. *Id.* at 3, 5.

87. *Id.* at 2.

88. *Id.* at 5.

The answer he arrived at was exclusion of the evidence derived from the NIT and the NIT warrant, and all the fruits thereof.[89] As the government had based its case against Michaud entirely on that evidence, the prosecution dismissed all charges after an unsuccessful interlocutory appeal.[90] The government's motion to dismiss explicitly recognized the disclose or dismiss problem inherent in balancing "the many competing interests that are at play when sensitive law enforcement technology becomes the subject of a request for criminal discovery. . . . The government must now choose between disclosure of classified information and dismissal of its indictment. Disclosure is not currently an option."[91] Michaud's graymail had succeeded.

Michaud highlights a particular graymail problem related to law enforcement hacking. Zero-day vulnerabilities like the one used in the FBI NIT are a scarce resource. They are difficult to discover and can be reused only as long as they remain secret.[92] Once exposed, they are quickly patched and become useless. As a consequence, live zero-day vulnerabilities are quite valuable and there is a thriving underground market in them.[93] The U.S. government both actively researches and purchases zero-day vulnerabilities.[94] Intelligence community documents declassified in 2016 reveal the existence of a formal interagency Vulnerabilities Equities Process (VEP) that controls use and disclosure of zero-day vulnerabilities throughout the executive branch.[95] It remains unclear whether the government's unwillingness to disclose the Playpen NIT source code resulted from this Vulnerabilities Equities Process.[96]

---

89. *See* Order Denying Dismissal and Excluding Evidence at 1, United States v. Michaud, No. 3:15-cr-05351 (W.D. Wash. May 25, 2016).

90. *See* Government's Unopposed Motion to Dismiss Indictment Without Prejudice at 1, United States v. Michaud, No. 3:15-cr-05351 (W.D. Wash. Mar. 17, 2017).

91. *Id.* at 2. By this time the NIT source code had been, as became relevant in later Playpen cases, retroactively classified by the FBI. *See* Government's Response to Defendant's Motion to Compel at 22 n.8, United States v. Darby, No. 2:16-cr-00036 (E.D. Va. Mar. 10, 2016).

92. For a thorough analysis of the life cycle of a zero-day vulnerability, see LILLIAN ABLON & ANDY BOGART, ZERO DAYS, THOUSANDS OF NIGHTS (2017).

93. *See* Vlad Tsyrklevich, *Hacking Team: A Zero-Day Market Case Study* (Jul. 22, 2015), https://tsyrklevich.net/2015/07/22/hacking-team-0day-market/ [http://perma.cc/DGH7-E88K]. Tsyrklevich was an expert witness for the *Michaud* defense as to the relevance of the NIT source code, whose testimony Judge Bryan found particularly persuasive. *See* Order on Procedural History and Case Status in Advance of May 25, 2016 Hearing at 3–4, United States v. Michaud, No. 3:15-cr-05351 (W. D. Wash. May 18, 2016).

94. *See generally* Matthew M. Aid, *Inside the NSA's Ultra-Secret China Hacking Group*, FOREIGN POLICY (Jun. 10, 2013) https://foreignpolicy.com/2013/06/10/inside-the-nsas-ultra-secret-china-hacking-group/ [https://perma.cc/8H8P-D6YP]; David Gilbert, *Cyber Arms Race*, VICE NEWS (Mar. 26, 2017), https://news.vice.com/story/the-u-s-government-is-stockpiling-lists-of-zero-day-software-bugs-that-let-it-hack-into-iphones [https://perma.cc/D3SQ-XXFD].

95. *Vulnerabilities Equities Process*, ELECTRONIC PRIVACY INFORMATION CENTER, https://epic.org/privacy/cybersecurity/vep/ [https://perma.cc/9EZJ-GX7V].

96. *Id.*

C. CIPA in United States v. Tippens

David Tippens is another Playpen defendant who was caught by Operation Pacifier. *United States v. Tippens* makes for interesting comparison to *Michaud* because Tippens is being tried for the same crimes, which were detected by the same NIT. He is being represented by the same public defender: Colin Fieman. The same judge, Judge Robert Bryan, is hearing the case. The major difference is that between Michaud's winning graymail and Tippens's trial, the FBI retroactively classified the NIT source code.[97] Tippens's trial could use CIPA procedures to avoid graymail rather than facing a disclose or dismiss dilemma.

At first, Tippens's defense pursued the same strategy as in *Michaud*: challenging the warrant on grounds of extraterritoriality and Fourth Amendment particularity. This tactic met with, perhaps predictably, the same degree of success it had previously. Tippens also moved to dismiss because the FBI's conduct of Operation Pacifier, running an international child pornography distribution network, was outrageous and beyond the bounds of common decency.[98] This too failed.

The next step was to graymail the prosecution by moving to compel disclosure of certain information. This information included, among other things, the NIT source code, as the defense team had also requested in *Michaud*, on the theory that the NIT malware implanted on Tippens's computer might have left it vulnerable to hacks by unknown third parties. If so, there might be reasonable doubt that those third parties could have planted incriminating child pornography on Tippens's computer. Tippens also moved to compel discovery answering the question of whether the FBI's NIT had been reviewed by the Vulnerabilities Equities Process, arguing that that information was material as to the outrageousness of the FBI's operation.[99]

From that point forward, CIPA procedures entered the case.[100] Judge Bryan issued a CIPA Section 3 protective order, held an ex parte, in camera hearing to discuss disclosure of the NIT code and whether it had been submitted for VEP review, and conducted a CIPA Section 2 pretrial conference with counsel to discuss the introduction of classified material. Following the ex parte, in camera hearing, Judge Bryan reversed the course he took in *Michaud* and declined to compel discovery of the NIT source code and whether it had been submitted for

97. *See* Government's Response to Defendant's Motion to Compel at 22 n.8, United States v. Darby, No. 2:16-cr-00036 (E.D. Va. Mar. 10, 2016).

98. *See* Order on Defendants' Motion To Dismiss Indictment, Defendants' Motion to Suppress Evidence, Defendants' Motion to Exclude Evidence, and Third Order on Defendants' Motion To Compel Discovery at 6, United States v. Tippens, et al., No. 3:16-cr-05110 (W.D. Wash. Nov. 30, 2016). "Outrageous government conduct occurs when the actions of law enforcement officers or informants are 'so outrageous that due process principles would absolutely bar the government from invoking judicial processes to obtain a conviction.'" United States v. Black, 733 F.3d 294, 302 (9th Cir. 2013) (quoting United States v. Russell, 411 U.S. 423, 431–32, (1973)).

99. Second Order on Defendant's Motion to Compel Discovery at 3, United States v. Tippens, et al., No. 3:16-cr-05110 (W.D. Wash. Oct. 24, 2016).

100. *Id.*

VEP review—whatever happened in the hearing convinced him that those pieces of information did not meet the *Roviaro* "relevant and helpful" standard.[101]

On December 1, 2016, the day after Judge Bryan issued the order denying Tippens's motion to compel discovery, a security blog hinted that a Firefox browser patch had recently been issued by Mozilla, the browser's maker, to remedy a vulnerability that allowed code to be run which would transmit the host system's IP address to a third party—behavior identical to that of the FBI's NIT.[102] No one could prove it, but it appeared that the zero-day exploit used by the NIT, and the NIT source code itself, had been discovered. Tippens again moved to compel discovery, arguing that since the NIT was publicly known, its disclosure could no longer harm the government's interest in keeping it secret. Judge Bryan again declined to compel discovery because public disclosure of the NIT code did not alter its classification status. Tippens could have taken out an ad in the *New York Times* with the NIT source code on it, but until the government declassified it, he couldn't compel the FBI to confirm that the leaked code was indeed their NIT.

Since they possessed what was, in all likelihood, the NIT source code, but could not prove it, Tippens's defense counsel negotiated an agreed stipulation, pursuant to CIPA Section 6(c)(1)(A), with the government admitting the facts that the classified NIT source code would tend to prove, that the NIT used

> an existing vulnerability that would allow the NIT to execute on a target computer without the knowledge of the computer's user. . . . It is possible that an exploit could make temporary or permanent changes to the security settings of a user's computer that could allow someone to subsequently run commands on that computer without the user's knowledge.[103]

By admitting that the NIT had allowed the FBI to execute commands on Tippens's computer—transmitting his true IP address to the FBI—the prosecution had admitted the possibility that a third party might also have done so.

At trial, the government introduced computer forensic evidence and testimony to counter Tippens's assertion that his computer had been tampered with by an unknown third party. In a surprise move, Tippens's defense counsel asked for a closed hearing to discuss the disclosure of classified information the defense had just acquired: portions of the March 7, 2017 Wikileaks release of documents on

---

101. Order on Defendants' Motion To Dismiss Indictment, Defendants' Motion to Suppress Evidence, Defendants' Motion to Exclude Evidence, and Third Order on Defendants' Motion To Compel Discovery at 27–28, United States v. Tippens, et al., No. 3:16-cr-05110 (W.D. Wash. Nov. 30, 2016) (citing Roviaro v. United States, 353 U.S. 53, 60–61 (1957)).

102. *See* Eduard Kovacs, *Mozilla Patches Firefox Zero-Day Exploited to Unmask Tor Users*, SECURITYWEEK (Dec. 1, 2016) [https://perma.cc/Z4VE-66C3].

103. Stipulation of the Parties Regarding the NIT and Related Matters at 2, United States v. Tippens, et al., No. 3:16-cr-05110 (W.D. Wash. Mar. 1, 2017).

CIA hacking tools, which revealed that the government possessed the capability to:

> hack into a computer without leaving any trace that it had been hacked or that an exploit had been placed on it. . . . [A] thorough forensic examination . . . would not be able to determine whether child pornography had been planted. . . . The proposed exhibits, in other words, would directly confront the Government's repeated assertion that the computer and devices showed no signs of a third party hack, which proved there was no hack.[104]

In response, the prosecution asked that Judge Bryan disallow the defense to disclose these classified documents at trial, despite the fact that they had just been publicly leaked. Judge Bryan, for the same reasons that he had declined to compel discovery of the leaked but classified NIT source code, obliged. He then immediately dismissed two of the three counts against Tippens as directed by CIPA Section 6(2):

> (2) Whenever a defendant is prevented by an order under paragraph (1) from disclosing or causing the disclosure of classified information, the court shall dismiss the indictment or information; except that, when the court determines that the interest of justice would not be served by dismissal of the indictment or information, the court shall order such other action, in lieu of dismissing the indictment or information, as the court determines is appropriate. Such action may include, but need not be limited to—
>
> (A) dismissing specified counts of the indictment or information;
>
> (B) finding against the United States on any issue as to which the excluded classified information relates; or
>
> (C) striking or precluding all or part of the testimony of a witness.[105]

Although Tippens's graymail was at least partially successful, as of the time of this writing, he is still being prosecuted for one count of possession of child pornography.

CONCLUSION

The law enforcement privilege seen in the Playpen graymail cases is analogous to the state secrets privilege at work in earlier graymail cases such as *North* and *Libby*. Both privileges protect sensitive sources and methods. Both privileges display a tension between defendants' evidentiary rights and the government's compelling interest in protecting sensitive sources and methods, resulting in a

104. Order on Government's Motion Seeking Clarification of This Court's Order Dismissing Counts 1 and 3 of the Superseding Indictment at 3–4, United States v. Tippens, No. 3:16-cr-05110 (W.D. Wash. Mar. 16, 2017).

105. 18 U.S.C. App. 3 § 6(e)(2) (2012).

disclose or dismiss dilemma for prosecutors. Although the state secrets privilege perhaps may claim an older pedigree, both the state secrets privilege and the law enforcement privilege came of age in the post-World War II expansion of the intelligence community: respectively, the CIA as foreign intelligence and the FBI as domestic counterintelligence and law enforcement.

However, there are key differences between the state secrets privilege and the law enforcement privilege. The defendants in cases where the state secrets privilege is invoked are generally either agents of foreign powers or members of the national security community acting in their official capacities. One expects graymail defenses in trials involving terrorist plots, espionage rings, or intelligence community personnel misconduct: very serious crimes that, by nature, occur only infrequently. On the other hand, the defendants in law enforcement privilege cases are ordinary domestic criminals: "common criminals" like Daniel Rigmaiden whose crimes may be commonplace, neither infrequent nor particularly severe.

Despite its imperfections, CIPA relieves some of the graymail problem previously associated with the *Reynolds* state secrets privilege, at least in criminal trials involving outsider defendants. By establishing workable procedures for disclosure of classified information by both the prosecution and the defense, CIPA limits the latter's ability to graymail the government by leveraging a disclose or dismiss dilemma. In cases involving the law enforcement privilege, however, CIPA does not apply unless the investigative techniques at issue are actually classified. This limitation has created an absurd situation in which it is easier for defense counsel to gain access to classified information than it is for them to gain access to information protected by the law enforcement evidentiary privilege.

There are at least three possible solutions to the graymail problem in cases where the law enforcement evidentiary privilege is in play. One is the approach used by the FBI in *Tippens*: classify the investigative techniques involved so that CIPA can control discovery and disclosure. Since the purpose of the classification system is to protect information which, if disclosed, could result in harm to national security, one could argue that any investigative technique or surveillance technology that is so sensitive its disclosure could harm national security *should* be classified.[106] However, this solution is normatively undesirable. Except insofar as the FBI is a part of the intelligence community due to its counterintelligence role, police are not spies, at least in a democratic society based on the rule of law. As Judge Learned Hand wrote in the spy trial *United States v. Coplon*:

> All governments, democracies as well as autocracies, believe that those they seek to punish are guilty; the impediment of constitutional barriers are galling to all governments when they prevent the consummation of that just purpose. But those barriers were devised and are precious because they prevent that

106. *See* Exec. Order No. 13,526, 75 Fed. Reg. 707, 707 (Jan. 5, 2010).

> purpose and its pursuit from passing unchallenged by the accused, and unpurged by the alembic of public scrutiny and public criticism. A society which has come to wince at such exposure of the methods by which it seeks to impose its will upon its members, has already lost the feel of freedom and is on the path towards absolutism.[107]

The second possible solution is to limit the use of surveillance technology by domestic law enforcement. Surveillance technology adapted from the military and intelligence community is a powerful tool for investigating crime. However, such power comes with risk. As surveillance technology becomes more common and trickles down to state and local law enforcement, the risk increases that information about that technology's use, capabilities, or technical specifications will be disclosed. This risk is even more pronounced with regard to sophisticated criminals and foreign adversaries, who are more likely to "go dark," adopting technical counter-surveillance methods to protect themselves. It is also more pronounced with regard to zero-day vulnerabilities, whose usefulness expires once they are widely known. The countervailing government interest in prosecuting crime must outweigh the risk of harm to national security by disclosure. This may be the case when the domestic crimes are especially heinous, such as the child pornography at issue in the Playpen cases. Put another way, law enforcement cannot have its cake and eat it too. Use surveillance technology to catch ordinary domestic criminals, and it may be too compromised when the federal government needs to use it to stop rarer, more serious, existential threats to national security. Reserve the use of surveillance technology for national security purposes only, and foreclose legitimate, effective means to stop child pornography and other serious domestic crimes.

The third, and best, solution is the one Congress embraced to solve the graymail problem inherent in the *Reynolds* state secrets privilege: a new statutory mechanism for controlled disclosure. This statutory mechanism could establish CIPA-like procedures for the use of information gathered by sensitive law enforcement surveillance technologies such as cell site simulators as well as hacking techniques such as the Playpen NIT. A statutory solution could also provide an opportunity to balance the competing government interests in prosecuting crimes and protecting sensitive national security information using democratic process and values, instead of leaving it entirely to prosecutorial discretion, or worse, police discretion. Congress could, for instance, define which crimes or categories of crimes are serious enough to warrant controlled disclosure of law enforcement surveillance techniques under CIPA-like procedures. It could also define which crimes are not serious enough to warrant the use of surveillance technologies whose disclosure might harm national security. A surveillance technology statute could also pre-empt the Vulnerabilities Equities Process to ensure that it is not co-opted on the one hand by intelligence agencies who aggressively

107. United States v. Coplon, 185 F.2d 629, 638 (2d Cir. 1950).

hoard zero-day vulnerabilities, or on the other by law enforcement agencies who favor their use in criminal investigations. Finally, a statutory solution could set clear parameters under which state and local police could use surveillance technologies whose disclosure could harm national security.

History repeats itself. The graymail problems that once attended criminal cases involving the *Reynolds* state secrets privilege now present themselves in cases involving the law enforcement privilege. The policy reasons that moved Congress to pass CIPA are still sound, and should now move Congress to pass legislation to defeat law enforcement privilege graymail by allowing for controlled disclosure of sensitive, but unclassified, law enforcement investigative techniques and surveillance technologies.