THE CRIMINAL DEFENSE ATTORNEY EXCEPTION TO THE FOURTH AMENDMENT

Rachel Simon[*]

I. INTRODUCTION

Edward Snowden[1] made Americans dramatically more aware of government surveillance—its very existence, as well as the danger it presents to civil liberties. The advantages of surveillance for law enforcement are obvious,[2] yet the population remains wary of a government inching ever closer to Big Brother.[3] That said, outrage is muted by the reality that most of us have never felt its adverse effects directly. Storied criminal defense attorney and law professor Mark Denbeaux ("Professor Denbeaux") is an exception. Although his story is rare today, it foreshadows events that attorneys around the world imminently face.

[*] Rachel Simon, J.D., 2014, Seton Hall University School of Law; B.Mus., 2007, The Juilliard School. The author thanks her family, friends, and professors for their advice and support.

[1] Edward Snowden is a former NSA contractor who revealed in June 2013 to *The Washington Post* and *The Guardian* that the NSA has been mass-collecting data on millions of American citizens' phone calls. Both newspapers won Pulitzer Prizes for the revelations; Snowden was charged with three federal offenses, including violation of the 1917 Espionage Act. *See* Ed Pilkington, *Guardian and Washington Post Win Pulitzer Prize for NSA Revelations*, THE GUARDIAN, Apr. 14, 2014, at A1, *available at* http://www.theguardian.com/media/2014/apr/14/guardian-washington-post-pulitzer-nsa-revelations.

[2] *See, e.g.*, Criminal Complaint at ¶¶ 9–15, United States v. Tsarnaev, No. 13-10200 (D. Mass. Apr. 21, 2013), 2013 WL 3231316 (explaining how Boston Marathon bomber Dzhokhar Tsarnaev was caught using private surveillance footage).

[3] *See, e.g.*, *Cloaks Off*, ECONOMIST (Nov. 2, 2013), http://www.economist.com/news/international/21588890-foreign-alarm-about-american-spying-mounting-sound-and-fury-do-not-always-match-0; Steven Erlanger, *Outrage in Europe Grows Over Spying Disclosures*, N.Y. TIMES, July 1, 2013, at A4, *available at* http://www.nytimes.com/2013/07/02/world/europe/france-and-germany-piqued-over-spying-scandal.html?pagewanted=all; David Meyer, *Academics Band Together to Plead for Online Privacy*, GIGAOM (Jan. 3, 2014), http://gigaom.com/ 2014/01/03/academics-band-together-to-plead-for-online-privacy/; Frank Pasquale, *Focusing on Core Surveillance Harms*, CONCURRING OPINIONS (Aug. 16, 2013), http://www.concurringopinions.com/archives/2013/08/focusing-on-core-surveillance-harms.html.

Professor Denbeaux has defended Southern civil rights activists, Black Panthers, and Vietnam War protestors.[4] He has served as a forensics expert before Congress and innumerable federal courts, including at the trial of Oklahoma City bomber Timothy McVeigh.[5] More recently, Professor Denbeaux has assumed representation of several detainees held as "enemy combatants" at the Military Detention Center in Guantanamo Bay, Cuba ("Guantanamo"). Consequently, the United States federal government ("government") monitors Professor Denbeaux's communications—private and public, intimate and mundane, whether with his family or, most significantly, with his clients.[6] Unfortunately, Professor Denbeaux is not alone; the government appears to be monitoring the communications of all the defense attorneys who represent Guantanamo detainees.[7]

This kind of surveillance presents a two-fold problem. First, government eavesdropping on attorney-client communications makes an unequivocal farce of our justice system, and undercuts the constitutional protections embodied in the Fourth, Fifth, and Sixth Amendments. Second, despite the enormity of the invasion of Professor Denbeaux's privacy, only two federal courts have even recognized that an attorney can state a Fourth Amendment claim for government eavesdropping on attorney-client communications.[8] Neither case was successful on the merits. Thus, there is simply no impetus for the government to stop its illegal intrusions anytime soon.

Other scholars note that government monitoring of attorney-client communications immediately erodes the attorney-client privilege,[9] directly violates the Sixth Amendment right to effective assistance of counsel,[10] and likely vitiates the Fifth Amendment right to

---

[4] *Mark P. Denbeaux: Seton Hall Law Faculty*, SETON HALL LAW, http://law.shu.edu/Faculty/fulltime_faculty/Mark-Denbeaux.cfm (last visited January 5, 2015).

[5] *Id.*

[6] Interview with Mark Denbeaux, Professor of Law, Seton Hall University School of Law (November 20, 2013).

[7] *See infra* Part II; *see also* Spencer Ackerman, *Guantánamo Hearings Halted Amid Accusations of FBI Spying On Legal Team*, THE GUARDIAN (April 14, 2014), http://www.theguardian.com/world/2014/apr/14/guantanamo-bay-hearing-halted-fbi-spying.

[8] *See* Gennusa v. Shoar, 879 F. Supp. 2d 1337 (M.D. Fl. 2012) (attorney and client sufficiently stated a Fourth Amendment violation based on unlawful police surveillance at the police station to survive a 12(b)(6) motion); Lonegan v. Hasty, 436 F. Supp. 2d 419 (E.D.N.Y. 2006) (same).

[9] Kristen V. Cunningham & Jessica L. Srader, *The Post 9-11 War on Terrorism . . . What Does It Mean for the Attorney-Client Privilege?*, 4 WYO. L. REV. 311, 312 (2004).

[10] U.S. CONST. amend. VI; Tamar R. Birckhead, *The Conviction of Lynne Stewart and the Uncertain Future of the Right to Defend*, 43 AM. CRIM. L. REV. 1, 43 (2006).

due process.[11] However, these collective rights—privilege, due process, and right to counsel—may only be invoked by the client being prosecuted. Likewise, where prior scholarship discusses the Fourth Amendment implications of government spying on attorney-client communications, it focuses on violations of the client's constitutional rights.[12] This focus is facially sound, considering that violations of the Fourth Amendment are typically remedied by suppressing evidence obtained by its violation;[13] suppression of evidence has no remedial value as to the illegal intrusion on an attorney's privacy. Indeed, constitutional jurisprudence largely ignores or rejects the notion that an attorney has Fourth Amendment rights separate and apart from her client when it comes to monitoring attorney-client communications.[14]

This Comment argues that there is not, and should not be, a "criminal defense attorney" exception to the Fourth Amendment. Specifically, the government should not be permitted to monitor a private citizen's personal communications without a warrant simply because he is representing a criminal defendant—even if that defendant is accused of terrorism. Because the Judiciary's response to such egregious constitutional violations is patently insufficient, this Comment submits that Congress must legislate to keep the Executive in check. Part II provides evidence of government surveillance of attorney-client communications, using Professor Denbeaux's experience at Guantanamo to frame the issue. Part III outlines the legality of such surveillance, insofar as Congress has passed laws allowing government surveillance of attorney-client communications in certain, limited contexts. Part IV sets forth the current Fourth Amendment jurisprudence and assesses what rights attorneys have to

[11] U.S. CONST. amend. V; Cunningham & Srader, *supra* note 9, at 335.

[12] *See, e.g.*, Teri Dobbins, *Protecting the Unpopular from the Unreasonable: Warrantless Monitoring of Attorney Client Communications in Federal Prisons*, 53 CATH. U. L. REV. 295, 298 (2004); Ellen S. Podgor & John Wesley Hall, *Government Surveillance of Attorney-Client Communications: Invoked in the Name of Fighting Terrorism*, 17 GEO. J. LEGAL ETHICS 145, 155 (2003); ACLU, REGARDING EAVESDROPPING ON CONFIDENTIAL ATTORNEY-CLIENT COMMUNICATIONS (66 Fed. Reg. 55062) (2001), *available at* https://www.aclu.org/racial-justice_prisoners-rights_drug-law-reform_immigrants-rights/coalition-comments-regarding-eaves.

[13] Wong Sun v. United States, 371 U.S. 471, 484–85 (1963) (extending exclusionary rule to evidence found as a consequence of the initial constitutional violation, also known as "fruit of the poisonous tree"); Mapp v. Ohio, 367 U.S. 643, 655 (1961) (announcing exclusionary rule whereby unconstitutionally obtained evidence is inadmissible at trial).

[14] *See, e.g.*, Weatherford v. Bursey, 429 U.S. 545, 562–68 (1977) (Marshall, J., dissenting) (noting that eavesdropping on attorney-client communications violates the Fifth and Sixth Amendments, but ignoring potential Fourth Amendment violations).

private communications. Part V explains the ways in which government monitoring of attorney-client communications violates the Fourth Amendment rights of the attorney. Part VI argues that Congress must legislate to provide both a cause of action for aggrieved attorneys and an incentive for the government to stop illegally spying on private citizens. Part VII concludes the Comment.

II. EVIDENCE OF GOVERNMENT SPYING

As of June 2013, it is beyond question that the United States federal government has been spying on its citizens for decades.[15] The government publicly justifies its mass surveillance programs on grounds of national security and counterterrorism.[16] Considering that Guantanamo is where the government houses alleged "high-value detainees" suspected of terrorism,[17] it is less than surprising to learn that various federal agencies have been spying on daily activities at Guantanamo since its inception. As detailed *infra*, what is perhaps more surprising is that such surveillance is occurring after the federal government has been admonished for secretly videotaping suspected terrorists' meetings with their attorneys, on no fewer than four prior occasions.

Before suspected 9/11 terrorists were sent to Guantanamo, they were held at the Metropolitan Detention Center ("MDC") in Brooklyn, New York. In March 2003, the Department of Justice Office of the Inspector General ("DOJ OIG") reported on pervasive breaches of private meetings between attorneys and their clients detained at the MDC:

> In total, we found more than 40 examples of staff videotaping detainees' attorney visits. On many videotapes, we were able to hear significant portions of what the detainees were telling their attorneys and sometimes what the attorneys were saying as well. It appeared that detainees' attorney visits were

[15] *See, e.g.*, Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps In To User Data Of Apple, Google and Others*, THE GUARDIAN, June 6, 2013, at A1, *available at* http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

[16] *See* In re Application of the F.B.I. for an Order Requiring Production of Tangible Things from [Redacted], No. 13-109 (FISA Ct. August 29, 2013), 2013 WL 5741573.

[17] *See, e.g.*, DONALD RUMSFELD, KNOWN AND UNKNOWN (2011) ("I wanted transfers of detainees to Guantanamo to be kept to a minimum—to only individuals of high interest for interrogation who posed a threat to our nation's security."); Memorandum from Donald Rumsfeld to Chairman, Joint Chiefs of Staff and Commander, U.S. Central Command (Apr. 21, 2003) (declassified in part Jul. 9, 2010) ("We need to stop populating Guantanamo Bay with low-level enemy combatants. GTMO needs to serve as an [REDACTED] not a prison for Afghanistan.").

> recorded intentionally. . . . In sum, we conclude[] that audio taping attorney visits violated the law and interfered with the detainees' effective access to legal counsel.[18]

Although the DOJ OIG clearly found that this conduct violated federal law[19] and the detainees' constitutional rights, it is unclear whether any remedial action was taken. It appears that the government instead attempted to circumvent statutory and constitutional constraints by having clandestine agencies, rather than municipal policemen, conduct the furtive recording of attorney-detainee meetings.

One notorious incident of a clandestine agency's picking up the baton is the 2002 CIA recording of interrogations of detainee Abu Zubaydah.[20] The recordings comprised ninety-two videotapes.[21] One "initial purpose" of recording the interrogations was to create "a record of Abu Zubaydah's medical condition and treatment should he succumb to his wounds and questions arise about the medical care provided to him by [the] CIA."[22] That said, "[a]nother purpose was to assist in the preparation of the debriefing reports."[23] Indeed, the CIA listened to the audio from the videotapes of the interrogations to prepare debriefing reports.[24] After public revelation of the tapes' existence, the CIA's Director of Clandestine Operations ordered the destruction of all ninety-two tapes in November 2005.[25]

A second incident surfaced in 2010, when the CIA admitted that it had twice misinformed the Department of Justice about whether it possessed recorded interrogations of Ramzi Binalshibh.[26] The CIA had previously claimed that it destroyed all recordings of Binalshibh around the same time it destroyed the ninety-two recordings of Abu Zubaydah in 2005.[27] In 2010, however, the Agency admitted that it still

---

[18] DEPARTMENT OF JUSTICE OFFICE OF THE INSPECTOR GENERAL, SUPPLEMENTAL REPORT ON SEPTEMBER 11 DETAINEES'ALLEGATIONS OF ABUSE AT THE METROPOLITAN DETENTION CENTER IN BROOKLYN, NEW YORK (2003), *available at* http://www.justice.gov/oig/special/0312/chapter3.htm#B.

[19] *Id.* (noting violation of 28 C.F.R. § 543.13(e)).

[20] CIA OFFICE OF THE INSPECTOR GENERAL, SPECIAL REVIEW – COUNTERTERRORISM DETENTION AND INTERROGATION ACTIVITIES (SEPTEMBER 2001–OCTOBER 2003), *available at* http://www.thetorturedatabase.org/files/foia_subsite/pdfs/CIA000349. pdf.

[21] *Id.*

[22] *Id.*

[23] *Id.*

[24] *Id.*

[25] Dan Eggen & Joby Warrick, *CIA Destroyed Videos Showing Interrogations,* WASH. POST (Dec. 7, 2012), http://www.washingtonpost.com/wp-yn/content/article/2007/12/06/AR2007120601828_pf.html.

[26] *US Confirms Interrogation Tapes,* AL-JAZEERA (Aug. 18, 2010), http://www.aljazeera.com/news/americas/2010/08/201081853357268955.html.

[27] *Id.*

possessed two videotapes and one audiotape of Binalshibh's interrogations.

A third notorious incident of the United States' conducting interrogation recordings involved the worldwide, broadcasted recording of Omar Khadr, a Canadian who was held at Guantanamo since the age of sixteen.[28] In February 2003, Canadian Security Intelligence Service officials interrogated Khadr in Guantanamo. In July 2008, Khadr's defense attorneys publicly released recordings of the interrogation made by the recording equipment in the attorney-client meeting room.[29] A Special Agent for the United States Naval Criminal Investigative Service ("NCIS") watched and listened to the Khadr recordings one week after they were made and reported on the intelligence gathered during the sessions.[30] Ultimately, seven hours of interrogations of Khadr conducted over four days at Guantanamo appeared in an edited, feature-length documentary film.[31]

While the MDC recordings were generally of private attorney-client meetings, the Guantanamo recordings were limited to interrogations, where a detainee's attorney may or may not have been present. That all changed in January 2013, when the discovery that an "external body" was surreptitiously monitoring and *censoring* the Military Commission hearings at Guantanamo, superseding the presiding judge's supposed sole authority to do so, emerged.[32] The external body censored Khalid Sheikh Mohammed's Learned Counsel, David Nevin, while he recited the title of a motion that contained mostly unclassified information pertaining to CIA dark site prisons. The Military Commission's presiding judge, Army Colonel James Pohl, taken by surprise, stated:

> [I]f some external body is turning the commission off under their [sic] own view of what things ought to be, with no reasonable explanation because [there] is no classification on it, then we are going to have a little meeting about who turns that light on or off.[33]

---

[28] *Key Events in the Omar Khadr Case,* CBC NEWS (Sep. 30, 2012), http://www.cbc.canews/politics/story/2012/09/30/omar-khadr-timeline.html.

[29] *Id.*

[30] *Report of Investigative Activity*, AIR FORCE OFFICE of SPECIAL INVESTIGATIONS, 60 (Feb. 24, 2003), http://graphics8.nytimes.com/packages/pdf/world/20080711khadr.pdf.

[31] *4 Days inside Guantanamo*, YOU DON'T LIKE THE TRUTH, http://www.youdontlikethetruth.com (last visited January 5, 2015).

[32] Unofficial Transcript of the KSM et al. (2) Hearing Dated Jan. 28, 2013 from 1:31 PM to 2:46 PM at 1445:14–1446:7, *available at* http://www.mc.mil/CASES/MilitaryCommissions.aspx.

[33] *Id.* at 1446:2–7.

Within one week, Judge Pohl seemed to not only accept having an external body eavesdrop on, and censor, the Military Commission hearings, but also even defend the notion on the government's behalf. Specifically, Judge Pohl challenged one defense attorney for Abd al-Rahim al-Nashiri by asking, "[d]oes it surprise you that the United States government has all sorts of ability to monitor conversations throughout the world?"[34]

Soon after the government's display of courtroom eavesdropping capabilities, defense counsel for Guantanamo detainees learned that the meeting rooms assigned to them for private conversations with their clients had been bugged with convincingly disguised microphones for surreptitious audio recording.[35] The microphones, made by Louroe, are hidden in realistic smoke detector shells mounted on the meeting rooms' ceilings.[36] According to Louroe, these microphones are "often used in law enforcement interview rooms," because they are "sensitive enough to capture a suspect's comments even when whispered."[37] That said, a public relations manager of Louroe specifically shunned clandestine usage of its products at Guantanamo: "If I'm monitoring audio covertly or surreptitiously, then it is 100% illegal. Not only have I broken the law, but I can't use any of that audio as evidence in a court case."[38] Public relations spin notwithstanding, however, there is no debate that the microphones in the attorney-client meeting rooms at Guantanamo are specifically designed for monitoring conversations that the speakers wish to keep confidential.

---

[34] Unofficial Transcript of the Al Nashiri (2) Hearing Dated Feb. 5, 2013 from 9:01 AM to 9:56 AM at 1556:3–5, *available at* http://www.mc.mil/CASES/MilitaryCommissions.aspx.

[35] *See generally* MARK DENBEAUX ET AL., SPYING ON ATTORNEYS AT GTMO: GUANTANAMO BAY MILITARY COMMISSIONS AND THE DESTRUCTION OF THE ATTORNEY-CLIENT RELATIONSHIP (2013) [hereinafter DENBEAUX ET AL., SPYING ON ATTORNEYS], *available at* http://law.shu.edu/ProgramsCenters/PublicIntGovServ/policyresearch/upload/spying_on_attorneys_at_GTMO.pdf.

[36] Transcript of the KSM et al. Hearing Dated Feb. 12, 2013 from 1:00 PM to 2:37 PM at 1984:5–1985:11, 2021:4–2022:5, *available at* http://www.mc.mil/CASES/MilitaryCommissions.aspx.

[37] Joseph Goudlock, *Where Are You Using Louroe Electronics?*, LOUROE ELECTRONICS BLOG (Sep. 27, 2012, 12:00 AM), http://www.louroe.com/blog.php.

[38] Cameron Javdani, *Legal Use of Audio,* LOUROE ELECTRONICS BLOG (Sep. 6, 2011, 4:51 PM),
http://louroe.com/blog.php.

Following the public discovery of the listening devices, Army Colonel John Bogdan ordered the audio recording equipment in attorney-client meeting rooms to be disconnected, but not dismantled.[39] In addition to the secret microphones, however, each attorney-client meeting room also hosted at least two video cameras. Colonel Bogdan confirmed that there was one infrared camera mounted on the wall opposite "from where the detainee would be locked in when there was not a meeting," and another encased, point-tilt-zoom camera mounted in a corner.[40] At least one of the video cameras in each of the attorney-client meeting areas is so sensitive that "from the distance they are in the cell, most definitely" they are capable of zooming to read "very tiny writing" on a document used during an attorney-client discussion.[41] It is questionable whether installing, maintaining, and using video cameras with such powerful lenses exceeds the ostensible security needs at Guantanamo.

On March 25, 2013, personnel from the Office of Military Commissions, Office of Chief Defense Counsel ("OCDC") discovered that there had been corruptions to and loss of electronic files containing attorney work-product, attorney-client communications, and other privileged and confidential documents stored on the OCDC's shared "O-drive."[42] The O-drive was the exclusive repository of all defense attorney work at Guantanamo; only those with the defense privilege were supposed to have access, and there was nowhere else for attorneys to save their work. OCDC personnel also discovered that the defense attorneys' internet activity, which itself revealed confidential work-product and client communications, was being monitored and reviewed.[43] Several defense teams reported these intrusions to the OCDC, Military Commission, and Department of Defense staff.[44]

On March 26, 2013, the defense team of detainee Ibrahim al Qosi alleged that the government conducted a search of 540,000 of its emails,[45] in addition to allowing unrestricted access to all defense files

[39] Transcript of the KSM et al. Hearing Dated Feb. 13, 2013 from 10:28 AM to 12:02 PM at 2243:1–4, *available at* http://www.mc.mil/CASES/ MilitaryCommissions.aspx.

[40] *Id.* at 2227:7–2228:19.

[41] *Id.* at 2239:11–2240:8.

[42] Defense Motion to Abate Proceedings at 1, No. CMCR-13-001, AE155A (U.S.M.C. Apr. 13, 2013).

[43] *Id.* at 3.

[44] *Id.* at 6–9.

[45] Petitioner's Emergency Motion for Appropriate Relief to Stop the Unauthorized Disclosure of Privileged Defense Counsel Communications and Other

in response to court orders, Freedom of Information Act requests, congressional inquiries, and search requests from other governmental agencies.[46] The government responded in April 2013 that no one in the Office of the Chief Prosecutor or on the Privilege Review Team reviewed the content of any privileged or otherwise confidential defense communication.[47] Nonetheless, in May 2013, Colonel Karen Mayberry, OCDC Chief Defense Counsel for Military Commissions, certified that she had investigated these allegations with the government offices and agencies involved and found them to be true.[48]

Colonel Mayberry uncovered further that: (1) IT and other staff were neither "trained in, [n]or in any way concerned with, attorney-client confidences or privilege[s]"; (2) staff regularly turned defense files "over to the requester without any scrutiny as to whether the results contain[ed] privileged or confidential files";[49] (3) results turned over "without limitations on the personnel authorized to view the information";[50] (4) past assurances over the sufficiency of securing privileged and confidential documents using encryption and password protection "were wrong";[51] and, amazingly, (5) staff from the various agencies involved had been discussing the security and confidentiality problems since at least 2008—i.e., had been aware of the problems and simply failed to agree on the appropriate solution.[52] As a result, Colonel Mayberry ordered all defense counsel, both military and civilian, to stop communicating client information via the provided email accounts, as well as to stop storing files on any provided drives.[53]

In April 2014, the author personally witnessed the most egregious incident of government interference in the attorney-client relationship at Guantanamo to date. On April 13, 2014, defense counsel for the five co-defendants in *United States v. Khalid Sheikh Mohammed, et al.*, who are accused of planning and executing the 9/11 terrorist attacks, jointly filed an emergency motion notifying the Military Commission that two FBI agents had interviewed the defense security officer ("DSO") working for defendant Ramzi bin al Shibh's team on Sunday, April 6, 2014 and compelled him to sign a "preventative cooperation

Electronic Defense Records at 2, No. CMCR-13-001 (U.S.M.C. 2013).

[46] *Id.* at 3.

[47] Declaration of Col. Karen Mayberry, No. CMCR-13-001 (U.S.M.C. May 2, 2013).

[48] *Id.*

[49] *Id.* ¶7.

[50] *Id.*

[51] *Id.* ¶5.

[52] *Id.* ¶5–14.

[53] In April 2014, Col. Mayberry advised the author personally that her directive remains in effect.

agreement" that included a non-disclosure provision.[54] A DSO is a legal team's advisor and liaison to government agencies on security issues. In plain English, bin al Shibh's DSO agreed to act as an ongoing FBI informant and not tell anyone about it, including the rest of his legal team. The DSO had a change of heart and informed his supervisors of the FBI agreement on April 9, 2014.[55]

The scope of the FBI investigation remains unknown, and the government's substantive responses remain redacted.[56] Media observers of the April hearings reported that the FBI questioned the DSO about alleged 9/11 mastermind Khalid Sheik Mohammed's ("KSM") defense counsel, specifically inquiring about how an unclassified manifesto[57] penned by KSM was released to the media in January.[58] In other words, the FBI was purportedly *investigating KSM's defense attorney* in lieu of investigating KSM himself. Although not providing affirmative information on the scope of the FBI investigation, the government has shot down the media reports as mistaken, stating that the FBI investigation does not pertain to that disclosure.[59]

Even to a law student, it was painfully obvious that no one—prosecution, defense, or judge—knew how to proceed when faced with the FBI derailment. Indeed, Judge Pohl frequently asked both parties how they thought the hearings should proceed in order to devise a workable plan moving forward.[60] Defense counsel argued that, as the subjects of an ongoing FBI investigation, they were conflicted insofar as their interests in defending against that investigation might conflict with their interests in defending their clients.[61] Further, they could not

[54] Emergency Joint Defense Motion to Abate Proceedings and Inquire into Existence of Conflict of Interest
Burdening Counsel's Representation of Accused, No. AE292 (U.S.M.C. Apr. 13, 2014).

[55] *Id.*

[56] *See, e.g.*, Amended Order Re Emergency Joint Defense Motion to Abate Proceedings and Inquire into Existence of Conflict of Interest Burdening Counsel's Representation of Accused, No. AE292QQ (U.S.M.C. Dec. 16, 2014).

[57] Ryan J. Reilly, *Mastermind of the Sept. 11 Attacks Wants to Convert His Captors*, HUFFINGTON POST (Jan. 14, 2014, 2:00 PM), http://www.huffingtonpost.com/2014/01/14/khalid-sheikh-mohammed-manifesto_n_4591298.html.

[58] Spencer Ackerman, *9/11 Military Court Adjourns Trial until June amid FBI Spying Probe*, THE GUARDIAN (April 17, 2014, 3:10 PM), http://www.theguardian.com/world/2014/apr/17/911-court-guantanamo-bay-adjourn-trial-june-fbi-spying.

[59] *See* Public Government Response to Defense Emergency Motion, No. AE292H (U.S.M.C. Apr. 14, 2014).

[60] *See generally* Transcript of the KSM et al. Motions Hearing Dated April 15, 2014 from 9:15 AM to 11:13 AM, *available at* http://www.mc.mil/CASES/Military Commissions.aspx.

[61] *Id.*; *see* Emergency Joint Defense Motion, *supra* note 54.

know whether members of their defense teams had signed non-disclosure agreements with other agencies after being likewise approached, and such a lack of knowledge prevented them from advising their clients on waiver of the conflict.[62] As such, Judge Pohl issued an order on April 15, 2014 requiring all current and former defense team members to disclose only to their lead counsel any disclosures/agreements with any federal agencies.[63] Lead counsel was instructed to then make the ethical call on what needs to be disclosed to the MC to resolve a conflict of interest. Defense counsel was further instructed to submit proposed orders stating what evidence and witnesses they want the Military Commission to subpoena to inquire into the FBI issue by close of business on Wednesday, April 16, 2014.[64]

The government denies any knowledge of the FBI investigation.[65] That said, a former prosecution team member, Joanna Baltes, now serves as Chief of Staff to the Deputy Director of the FBI.[66] At a minimum, this relationship raises questions about the prosecution team's knowledge of the FBI investigation. In an abundance of caution, therefore, Judge Pohl issued an order on Wednesday, April 16, 2014, appointing a Special Review Team to review all matters pertaining to the investigation and Special Trial Counsel to represent the United States in order to keep the prosecution team led by General Martins insulated.[67] The Special Review Team's conclusions were later found insufficient to address all issues raised by the defense, and were not considered in the Military Commission's December 2014 order (1) compelling the FBI to maintain a log of those who access the files of the (still sealed) investigation at issue, (2) requiring disclosure of that log to the Military Commission upon request, and (3) ensuring that the FBI investigative file remains sequestered from the government prosecution team moving forward.[68]

In close, the Military Commission has twice been forced to set aside its docketed schedule and deal with unexpected intrusions by clandestine agencies' spying on attorney-client communications. As of

---

[62] Emergency Joint Defense Motion, *supra* note 54.

[63] Interim Order Re Emergency Defense Motion to Abate Proceedings and Inquire into Existence of Conflict of Interest Burdening Counsel's Representation of Accused, No. AE292C (U.S.M.C. Apr. 15, 2014).

[64] *Id.*

[65] Transcript of the KSM et al. Motions Hearing Dated April 14, 2014 from 9:15AM to 9:51 AM at 7766, *available at* http://www.mc.mil/CASES/MilitaryCommissions.Aspx.; *see* Public Government Response, *supra* note 59.

[66] *See* Transcript of the KSM et al. Motions, *supra* note 60, at 7789–90.

[67] *See* Interim Order, *supra* note 63.

[68] *See* Amended Order, *supra* note 56.

December 2014, it is undisputed that the government recorded attorney-client communications at Guantanamo via audio and video recording,[69] that the government deleted only defense attorney files on local computers,[70] and—most significantly—that the government surveillors gave the illegally obtained evidence to the government prosecutors.[71]

III. LEGALITY OF GOVERNMENT SPYING

Congress has passed legislation allowing government spying on attorney-client communications in certain, limited circumstances. These laws purport to place strict limits on when law enforcement is permitted to spy on attorney-client communications, in recognition of the sacrosanct place attorney-client communications hold in American law. This section outlines the ways in which the government has statutory authority to legally and constitutionally intrude on attorney-client communications, as well as the ways in which the judiciary has attempted to hold the executive branch to the legislature's directives. As discussed in Part V, *infra*, the judiciary has been largely unsuccessful at reigning in the Executive.

A. The Federal Wiretap Act

Before 1967, the police did not need to get a warrant to listen-in on conversations occurring over phone company lines. But in that year, the Supreme Court decided two cases which made clear that unrestricted electronic surveillance could violate the Fourth

[69] Even the prison's lawyer and head warden admitted to audio surveillance. *See* Chris McGreal, *Guantanamo Commander Admits Listening Devices Eavesdropped on Lawyer Meetings with Clients,* THE GUARDIAN (Feb. 18, 2013), *available at* http://www.rawstory.com/rs/2013/02/18/guantanamo-commander-admits-listening-devices-eavesdropped-on-lawyer-meetings-with-clients/ ("The prison's lawyer, Captain Thomas Welsh, told the court he discovered the room was fitted with hidden microphones early last year and reported it to the then warden, Colonel Donnie Thomas, to seek assurances that meetings between the accused and their lawyers were not being spied on. Bogdan said he was not informed when he took over. He told the court that the FBI was in control of the room until 2008 and that he has since discovered that the bugs were accidentally disconnected in October during renovations but then secretly reconnected by an unnamed intelligence service two months later, suggesting they were still in use.").

[70] *See* Daphne Eviatar, *Lawyers Say Gitmo Computer Problems Make Defending 9/11 Accused Impossible,* HUFFINGTON POST (Aug. 23, 2013, 5:30 PM), https://www.huffingtonpost.com/daphne-eviatar/lawyers-say-gitmo-compute_b_3806590.html (noting deletion of defense attorney files).

[71] *See* Peter Finn, *Guantanamo Dogged by New Controversy after Mishandling of E-Mails,* WASH. POST (Apr. 11, 2013), *available at* http://articles.washingtonpost.com/ 2013-04-11/national/38458944_1_defense-attorneys-defense-lawyers-defense-counsel (noting that "hundreds of thousands" of defense emails were turned over to the prosecution).

Amendment. In *Katz v. United States* ("*Katz*"), the Court held that eavesdropping counted as a Fourth Amendment search requiring a warrant.[72] In *Berger v. New York*, the Court held that New York's wiretap statute violated the Fourth Amendment because the statute: (1) was authorized for too long a time; (2) failed to require a specific description of the crime being committed or the persons or things to be searched; and (3) neither required notice to the target nor a showing of special circumstances to abrogate the notice requirement.[73] Congress enacted the Wiretap Act in 1968 to ensure that any electronic surveillance by federal agents complies with the requirements of the Fourth Amendment post-*Katz* and *Berger*.[74] Generally, the Wiretap Act "criminalizes and creates civil liability for intentionally intercepting electronic communications without a judicial warrant."[75]

Section 2516 of the Wiretap Act provides for the interception of wire, oral, and electronic communications by federal agencies upon an application to a federal judge showing that the interception may provide evidence of federal crimes.[76] At a minimum, the application must state all facts justifying the applicant's belief that an order should be issued[77] and the time period of the requested interception;[78] the judge may require additional evidence.[79] The judge may authorize the interception if there is probable cause to believe that: (1) an individual

[72] Katz v. United States, 389 U.S. 347, 351 (1967).

[73] 388 U.S. 41, 59–60 (1967).

[74] *See* United States v. United States Dist. Court, 407 U.S. 297, 302 (1972) ("Much of Title III was drawn to meet the constitutional requirements for electronic surveillance enunciated by this Court.").

[75] Adams v. City of Battle Creek, 250 F.3d 980, 982 (6th Cir. 2001).

[76] 18 U.S.C. § 2516(1) (2012). The judge may also grant orders authorizing interception of communications that may provide evidence of other enumerated offenses under Title 18, including: (1) Presidential and Presidential staff assassination, kidnapping, and assault (§ 1751); (2) hostage taking (§ 1203); (3) destruction of aircraft or aircraft facilities (§ 32); (4) threatening or retaliating against a federal official (§ 115); (5) Congressional, Cabinet, or Supreme Court assassination, kidnapping, and assault (§ 351); (6) wrecking trains (§ 1992); (7) production of false identification documents (§ 1028); (8) fraud and misuse of visas, permits, and other documents (§§ 1546, 2516(1)(c), 2516(1)(p)); and (9) crimes related to alien smuggling (§ 2516(1)(p)).

[77] 18 U.S.C. § 2518(1)(b) (1998). The statement should include (1) details about the offense that is being or is about to be committed, (2) a description of the nature and location of the place where the communication is to be intercepted, (3) a description of the type of communications to be intercepted, and (4) "the identity of the person, if known, committing the offense and whose communications are to be intercepted." *Id.* It must also state whether "other investigative procedures have been tried and failed, or why [such procedures] reasonably appear to be unlikely to succeed if tried or [why such procedures would] be too dangerous." *Id.* § 2518(1)(c).

[78] *Id.* § 2518(1)(d).

[79] *Id.* § 2518(2).

is committing, has committed, or is about to commit one of the enumerated offenses; (2) communications concerning that offense will be obtained through the interception; (3) the place of interception is "leased to, listed in the name of, or commonly used" by the surveillance target; and (4) "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous."[80] The Wiretap Act restricts applicants for eavesdropping warrants to "publicly responsible officials subject to the political process" so that "should abuses occur, the lines of responsibility [would] lead to an *identifiable person*."[81] Finally, the Act provides that its enumerated remedies and sanctions are "the only judicial remedies and sanctions for *nonconstitutional violations*"[82] involving interception of wire and electronic communications. As discussed in Part V, *infra*, *constitutional* violations of the Wiretap Act by federal actors are remedied in a *Bivens* action.

The Wiretap Act provides a number of exceptions to its application, including when a party consents, when the target is foreign rather than domestic, and when a service provider rather than an agency is conducting the monitoring.[83] The Act also allows for warrantless surveillance in the event of an emergency, which involves the "(i) immediate danger of death or serious physical injury to any person, (ii) conspiratorial activities threatening the national security interest, or (iii) conspiratorial activities characteristic of organized crime."[84] Significantly, the Wiretap Act provides specific protections for privileged communications, which maintain their privileged character regardless of interception.[85] In recognition of the long-established evidentiary rules of privilege, *United States v. Turner* made clear that telephone conversations are "privileged" under the Wiretap Act only if they are "privileged other than by virtue of their character as private telephone conversations."[86]

---

[80] *Id.* § 2518(3)(a)–(d).

[81] Omnibus Crime Control and Safe Streets Act of 1968, 2 Stat. 2112 United States Code Congressional and Administrative New, 90th Congress, 2nd Session, 1968, Volume 2, p. 2112, Senate Report No. 1097. *See also* United States v. Cihal, 336 F. Supp. 261, 265 (W.D. Pa. 1972).

[82] 18 U.S.C. § 2518(10)(c) (1998) (emphasis added).

[83] *See* 18 U.S.C. § 2511 (2008).

[84] 18 U.S.C. § 2518(7) (1998).

[85] 18 U.S.C. § 2517(4) (1968).

[86] 528 F.2d 143, 155 (9th Cir. 1975).

While privileged communications are inadmissible at trial, law enforcement officers are not entirely prohibited from intercepting telephone conversations between attorney and client under the Wiretap Act. Section 2518(5) requires that electronic eavesdropping be conducted "in such a way as to minimize the interception of communications not otherwise subject to interception,"[87] including privileged and, presumably, constitutionally-protected communications.[88] Nevertheless, law enforcement officers who have lawfully established a wiretap can monitor attorney-client communications to the extent necessary to determine that the attorney is not participating in criminal activity along with the subject of their investigation.[89] This is known as the "crime fraud exception."[90]

Under the crime fraud exception, law enforcement officers may legally monitor attorney-client communications under the Wiretap Act.[91] For example, in *United States v. Johnston*, federal Drug Enforcement Agents tapped the phone of defendant Johnston, an attorney, in investigating a marijuana distribution ring involving Johnston's client.[92] The Agents heard Johnston help the drug-dealing client create a false alibi, and Johnston was subsequently indicted and convicted of conspiracy to distribute marijuana.[93] Johnston argued that the wiretaps violated the Wiretap Act's minimization requirement because the inculpatory conversations were privileged attorney-client communications. The Tenth Circuit disagreed, upholding the District Court's ruling that because the content of the conversations was unlawful criminal advice and not lawful legal advice, the conversations were not privileged and thus not subject to the minimization requirement.[94]

---

[87] 18 U.S.C. § 2518(5) (1998).

[88] *See, e.g.*, United States v. Harrelson, 754 F.2d 1153, 1169 (5th Cir. 1985) ("Section 2518(5) requires the government to minimize the interception of privileged communications."); United States v. DePalma, 461 F. Supp. 800, 821 (S.D.N.Y. 1978) ("[o]nce the parties have been identified and the conversation between them is determined to be nonpertinent or privileged, monitoring of the conversation must cease immediately.").

[89] *See* United States v. Hyde, 574 F.2d 856, 869–70 (5th Cir. 1978).

[90] *See, e.g.*, United States v. Zolin, 491 U.S. 554, 575 (1989), *vacated in part on other grounds*, 905 F.2d 1344 (9th Cir. 1990).

[91] *See, e.g.*, United States v. Knoll, 16 F.3d 1313, 1319 (2d Cir. 1994) (dismissing attorney's Fourth Amendment grievance regarding government-sanctioned burglaries of his firm to obtain incriminating documents implicating him and a client in bankruptcy fraud).

[92] 146 F.3d 785, 794 (10th Cir. 1998).

[93] *Id.*

[94] *Id.*

Although Johnston was in fact guilty of the conspiracy offense, the *Johnston* case illuminates the danger that the government's violation of the Wiretap Act may be excused so long as it guesses correctly about an attorney's participation in a crime. That is, the government was monitoring Johnston's private and privileged conversations and only learned that such conduct did not constitute a violation of the Wiretap Act when a court retrospectively determined the legal status of the conversations as non-privileged. Had Johnston been innocent and given only legal advice, the government's monitoring without any minimization procedures would have remained a Wiretap Act violation.[95]

Of course, the Wiretap Act was enacted before cellphones and smartphones. The Wiretap Act thus provides less assistance today, in that its drafters did not anticipate the growing popularity of wireless communications. As will be seen, statutory amendments, as well as advancements in communications technology, resolved this issue by establishing recognizable privacy interests for parties to wireless conversations.[96]

B. 18 U.S.C. § 2702 (Stored Communications Act)

The Stored Communications Act ("SCA"), codified at 18 U.S.C. § 2702 et seq., seeks to protect records held by communications service providers, such as phone companies, internet service providers ("ISP"), webmail providers, instant message or text providers, or bulletin board sites. In relevant part, the provision states:

> (a) Prohibitions.—(1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and (2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service . . . ; and (3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service . . . to any governmental entity.[97]

In order to get a communications provider to turn over records beyond basic subscriber information, the government either has to get

[95] 18 U.S.C. § 2518(5) (1998).

[96] *See generally* Dobbins, *supra* note 12, at 295.

[97] 18 U.S.C. § 2702 (2008).

a search warrant or a special court order.[98] Section 2703 allows disclosure of an electronic communication (1) pursuant to a warrant, without notice to the subscriber, or (2) pursuant to an administrative warrant or court order, if the communication is over 180 days old, and with notice to the subscriber. Section 2703(d) states that a court order may issue "only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."

Section 2707 provides a civil action for any person aggrieved by the knowing or intentional violation of 18 U.S.C. § 2702.[99] Section 2707(b) states that relief may be granted in the form of preliminary, declaratory, or equitable form, that both compensatory and punitive damages are available, and that attorney's fees and costs may also be granted. While Section 2707(e) provides three "complete" defenses to violations of the SCA,[100] Section 2708 provides that "the remedies and sanctions described in this chapter are the only judicial remedies and sanctions for *nonconstitutional* violations of this chapter."[101] As with constitutional violations of the Wiretap Act, constitutional violations of the SCA by federal agents are remedied in a *Bivens* action, discussed in Part V, *infra*.

Under the SCA, then, attorney-client communications may be monitored by the government if they are turned over by the content provider (e.g., Google, Yahoo, Hotmail) pursuant to a warrant or court order issued upon an epistemic, reasonable belief that the communications pertain to an ongoing criminal investigation. Thus, theoretically, if the government believes a criminal has communicated with her attorney about the crime being investigated, then the government could potentially receive all attorney-client communications under the SCA. Indeed, the attorney may never know that the government has obtained her attorney-client communications pursuant to the SCA,[102] and certainly cannot take steps to redress the attendant privacy violation.

---

[98] 18 U.S.C. § 2703 (2009).

[99] 18 U.S.C. § 2707 (2002).

[100] The three complete defenses are: (1) good faith reliance on a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization; (2) good faith reliance on a request of an investigative or law enforcement officer . . . ; or (3) good faith determination that . . . this title permitted the conduct complained of. *Id.* § 2707(e).

[101] 18 U.S.C. § 2708 (1986) (emphasis added).

[102] 18 U.S.C. § 2703 (2009).

C. Bureau of Prisons Regulation, 28 C.F.R. 501.3

On October 30, 2001, then United States Attorney General John Ashcroft authorized a new Bureau of Prisons rule ("BOP Regulation") that allows warrantless monitoring of all communications between specified federal inmates and their attorneys when the Attorney General himself has a reasonable suspicion that the particular inmate "may use communications with attorneys or their agents to further or facilitate acts of terrorism."[103] The BOP Regulation expressly applies to communications that fall within the attorney-client privilege.[104]

On April 11, 2002, Lynne Stewart ("Stewart"), a criminal defense attorney, was arrested for providing material support and resources to a terrorist organization as a result of communicating with her terrorist client. Stewart represented Sheik Omar Abdel Rahman, leader of terrorist organization the Islamic Group, who was convicted for the 1993 World Trade Center bombings.[105] The government's case against Stewart developed from monitoring her jailhouse communications with Rahman pursuant to the BOP Regulation. Trial testimony showed that during prison visits to Rahman in May 2000 and July 2001, Stewart: (1) violated the BOP Regulation by distracting guards and acting as a decoy so that Rahman and his interpreter, Mohammed Yousry, could covertly discuss issues related to Islamic Group governance, strategy, and policy;[106] (2) provided "cover" for Yousry to read letters and other messages from third parties to Rahman and for Rahman to dictate outgoing letters to Yousry;[107] and (3) conveyed to a Reuters reporter Rahman's politically charged statement that he was "withdrawing his

---

[103] 28 C.F.R. § 501.3(d) (2003). The Attorney General may rely on information from the head of a federal law enforcement or intelligence agency. *Id.*

[104] *Id.*

[105] Indictment, United States v. Ahmed Abdel Sattar, Yassir Al-Sirri, Lynne Stewart & Mohammed Yousry, No. 02-395 (S.D.N.Y. Apr. 9, 2002), *available at* http://news.findlaw.com/cnn/docs/terrorism/ussattar040902ind.pdf.

[106] *See* Transcript of Stewart and Yousry at 17, Prison Visit with Rahman (May 20, 2000), *available at* http://www.lynnestewart.org/5201.pdf ("Stewart: 'I am making allowances for them looking in at us and seeing me never speaking and writing away here while you talk Arabic.'").

[107] *See* Transcript of Stewart and Yousry at 49–51, Prison Visit with Rahman (May 19, 2000), *available at* http://www.lynnestewart.org/5191.pdf (Stewart stating that she can "get an Academy Award" for her performance covering Yousry's private conversations with Rahman). *See also* Trial Testimony of Lynne Stewart at 7764–66 (Oct. 27, 2004), *available at* http:// www.lynnestewart.org/transcripts/102704.txt (testifying to comments made to Yousry during May 19, 2000 prison visit).

support" for the cease-fire in Egypt that had been upheld by factions of the Islamic Group since 1997.[108] Her conviction garnered widespread attention, highlighting the tension between a defendant's right to unfettered communication with his lawyer and the ever-increasing reach of the federal government post-9/11.[109] To date, Stewart is the only terrorist's lawyer who has faced criminal charges.[110]

The BOP Regulation presents many of the same problems as the Wiretap Act and SCA. Specifically, it lacks procedural safeguards beyond the Executive's own discretion and, further, lacks either *ante* or *post hoc* judicial oversight. Thus, while Stewart was guilty of aiding a terrorist,[111] there may be other attorneys whose communications are being monitored who are wholly innocent. All in all, the BOP Regulation does not appear to be a necessary tool in the government's war on terror, given that these communications could be monitored pursuant to a court order under the Wiretap Act,[112] FISA,[113] or the Patriot Act.[114] It does, however, make the unfettered monitoring of attorney-inmate communications by the government that much easier to accomplish.

---

[108] *See* Trial Testimony of Esmat Salaheddin at 5573–75 (Sept. 13, 2004), *available at* http://www.lynnestewart.org/transcripts/091304.txt (testifying that Stewart conveyed Rahman's statement regarding the cease-fire to a reporter); Trial Testimony of Lynne Stewart, *supra* note 107, at 7810, 1816 (stating that Salaheddin's testimony was accurate).

[109] *See, e.g.*, Michael Powell & Michelle Garcia, *Sheik's U.S. Lawyer Convicted of Aiding Terrorist Activity*, WASH. POST, Feb. 11, 2005, at A01 ("Stewart's case became a litmus test for how far a defense attorney could go in aggressively representing a terrorist client without crossing the line into criminal behavior."); Victoria Ward, *U.S. Civil Rights Lawyer Guilty of Aiding Terrorism*, PRESS ASSOC., Feb. 11, 2005 (reporting Stewart's conviction); *Civil Rights Lawyer Lynne Stewart Convicted of Aiding Terrorists*, NAT'L PUB. RADIO, Feb. 11, 2005 (discussing Stewart's conviction).

[110] *See* Laurel E. Fletcher et al., *Defending the Rule of Law: Reconceptualizing Guantanamo Habeas Attorneys,* 44 CONN. L. REV. 617, 673 n.150 (2012).

[111] While Rahman was certainly a dangerous terrorist seeking to commit additional violence, further context reveals that Stewart's prosecution was at least as much for her political support of dissidents like Rahman as it was for her criminal acts. *See generally* Deborah L. Rhode, Editorial, *Terrorists and Their Lawyers*, N.Y. TIMES, Apr. 16, 2002, at A27; Birckhead, *supra* note 10, at 21; Laurel E. Fletcher et al., *supra* note 110, at 673 n.150.

[112] The Wiretap Act is available because the communications pertain to a national security interest. 18 U.S.C. § 2518(7) (1998).

[113] Indeed, Rahman and Stewart's communications were monitored pre-2001 pursuant to a FISC order. *See* Birckhead, *supra* note 10, at 21.

[114] The Patriot Act is available because the communications pertain to terrorism. 50 U.S.C. § 1861(a)(1) (2014).

D. The USA PATRIOT Act

The USA PATRIOT Act ("Patriot Act") plays a special role in this Comment, given its enactment as a counterterrorism-based surveillance statute.[115] Generally, Section 215 of the Patriot Act ("Section 215") allows government surveillance of communications if they are connected to terrorism. Specifically, Section 215 allows the Federal Bureau of Investigation ("FBI") to order any person or entity to turn over "any tangible things" if the FBI "specif[ies]" that the order is "for an authorized investigation . . . to protect against international terrorism or clandestine intelligence activities."[116] It requires the FBI to provide a statement of facts showing that there are reasonable grounds to believe the tangible things are relevant to the authorized investigation and to implement minimization procedures "applicable to the retention and dissemination."[117]

Nonetheless, Section 215 expands the FBI's domestic spying power, insofar as the FBI (1) need not show probable cause, nor even reasonable suspicion, that the person whose records it seeks is engaged in criminal activity, (2) need not have any suspicion that the subject of the investigation is a foreign power or agent of a foreign power, and (3) can investigate United States citizens based, in part, on their exercise of First Amendment rights.[118] The FBI can investigate non-citizens based solely on their exercise of First Amendment rights.[119] Significantly, those served with Section 215 orders are prohibited from disclosing that fact to anyone else.[120]

50 U.S.C. § 1861(e) provides that "[a] person who, in good faith, produces tangible things under an order pursuant to this section shall *not be liable to any other person* for such production. Such production shall *not be deemed to constitute a waiver of any privilege* in any other proceeding or context."[121] While this provision protects the confidentiality of privileged material, there is no practical redress for a person whose privacy is intruded upon by another's compliance with Section 215. If, for example, one's doctor were handed a Section 215

[115] Indeed, its very name, USA PATRIOT Act, is an acronym for the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001." Pub. L. No. 107–56, 115 Stat. 272 (2001).

[116] 50 U.S.C. § 1861(a)(1) (2006).

[117] *Id.* § 1861(b)(1)–(2).

[118] Section 215 authorizes investigations of U.S. persons that are "not conducted *solely* upon the basis of activities protected by the first amendment to the Constitution." *Id.* § 1861(a)(1) (emphasis added).

[119] *Id.*

[120] *Id.* §§ 1861(c)(2)(E), 1861(d)(1).

[121] *Id.* § 1861(e) (emphasis added).

request for one's medical records, the doctor could turn them over without fear of any liability despite the fact that the materials ostensibly retain their privileged status. There would be no liability for the doctor and no redress for the patient, however, since the patient could not be informed that either the Section 215 request, or the doctor's compliance with it, even existed.[122]

A person violates Section 215 by either intentionally engaging in electronic surveillance that is not authorized by the Patriot Act or by knowingly or even negligently disclosing such surveillance.[123] A violation of Section 215 is punishable by a "fine of not more than $10,000 or imprisonment for not more than five years, or both."[124] It is a complete defense if the defendant was an investigative officer whose surveillance was conducted pursuant to a search warrant or court order.[125]

As discussed further in Part V, *infra*, the complete secrecy of Section 215 monitoring and the complete defense of acting pursuant to a court order raise serious concerns for attorneys. First, the judicial check on the Executive's use of Section 215—the Foreign Intelligence Surveillance Courts ("FISC")[126]—has been wholly ineffective insofar as the FISCs appear to merely rubber-stamp all Section 215 requests in the name of national security. On these grounds, the FISC held that Section 215 authorizes ubiquitous surveillance of American citizens' telephone and email metadata to sniff out suspected terrorists, which in turn does *not* violate the Fourth Amendment.[127] If the FISC will authorize widespread and non-targeted surveillance in the name of counterterrorism, it appears that the FISC would readily authorize targeted surveillance of an attorney representing a person suspected of terrorism. Second, that attorney would never know that her

---

[122] *See* 50 U.S.C. §§ 1861(c)(2)(E), 1861(d)(1) (2006).

[123] 50 U.S.C. § 1809(a)(1)–(2) (2010).

[124] *Id.* § 1809(c).

[125] *Id.* § 1809(b).

[126] FISA is the acronym for the Foreign Intelligence Surveillance Act (50 U.S.C. ch. 36), a domestic statute that prescribes procedures for the physical and electronic surveillance and collection of "foreign intelligence information" between "foreign powers" and "agents of foreign powers" (which may include American citizens and permanent residents suspected of espionage or terrorism). *See* 50 U.S.C. §1801(b) (2010). FISA establishes Foreign Intelligence Surveillance Courts to provide judicial review of surveillance conducted under FISA's authority to ensure constitutional compliance; any surveillance conducted pursuant to FISA must first be approved by a FISC. *Id.* § 1809. FISC proceedings are secret, *ex parte*, and non-adversarial; only the government submits evidence, after which the FISC judge approves or denies the surveillance.

[127] *See* In re Application, *supra* note 16.

communications are being monitored pursuant to a Section 215 order.[128] Professor Denbeaux only asserts to know that his private, non-Guantanamo-related communications are being monitored because government prosecutors have made statements and taken actions that would be impossible or inexplicable in the absence of surreptitious monitoring. With the current FISC's rubber-stamp approval, Section 215 represents a sweeping authorization for the government to monitor the content of any person's private communications, without his or her knowledge or consent, so long as the government can show some connection to terrorism.[129] Without knowing the surveillance is occurring, the target cannot seek redress for the Fourth Amendment violation such monitoring represents.

IV. THE FOURTH AMENDMENT: AN ATTORNEY'S RIGHT TO PRIVACY

The Fourth Amendment grants the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[130] Security in one's papers includes the right to privacy in all personal correspondence;[131] security in one's person includes the right to privacy as to one's bodily integrity and freedom of movement.[132]A search is unreasonable, and the Fourth Amendment violated, when a government actor either (1) physically intrudes on a protected area or item to obtain information or evidence,[133] or (2) violates a person's reasonable expectation of privacy with regard to a protected area or item.[134]

---

[128] 50 U.S.C. §§ 1861(c)(2)(E), 1861(d)(1) (2006).

[129] In a public address, President Obama recently promised that federal agencies will *now begin to limit* their mass surveillance under Section 215 to "only" those persons "two steps removed" from known terrorists. By this formula, because Professor Denbeaux communicates with his clients in Guantanamo (who are suspected of terrorism), and this author communicates with Professor Denbeaux, the government is likely monitoring the content of this author's personal communications as part of its counterterrorism efforts. President Barack Obama, Remarks on Signals [NSA] Intelligence Programs at The White House (Jan. 17, 2014).

[130] U.S. CONST. amend. IV.

[131] *See* Nixon v. Adm'r of Gen. Servs., 433 U.S. 425, 529 (1977) (Burger, C.J., dissenting) ("[T]ruly private papers or communications, such as a personal diary or correspondence . . . lie at the core of First and Fourth Amendment interests.").

[132] Richard A. Posner, *Rethinking the Fourth Amendment*, 1981 SUP. CT. REV. 49, 51 (1981).

[133] United States v. Jones, 132 S. Ct. 945, 950 (2012) (re-establishing physical trespass as a Fourth Amendment search).

[134] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (establishing that a Fourth Amendment violation occurs when a state violates a person's subjective expectation of privacy, where that expectation is one that society deems objectively reasonable).

Historically, Fourth Amendment jurisprudence relied on property law, finding violations only where the government committed a physical trespass on a protected area or item.[135] A paradigm shift occurred in Fourth Amendment analysis with the 1967 case of *Katz*.[136] In *Katz*, the police placed a listening device on the outside of a phone booth. Reasoning that the Fourth Amendment "protects people not places,"[137] the *Katz* Court held that the device violated the Fourth Amendment rights of the caller—notwithstanding the lack of a physical trespass into the phone booth—because it infringed on the caller's reasonable expectation of privacy.

In his concurrence, Justice Harlan argued for a two-pronged test to find a Fourth Amendment violation, wherein a defendant must (1) manifest a subjective expectation of privacy, which is (2) one that society deems objectively reasonable.[138] In *Katz*, the Court found that the caller manifested a subjective expectation of privacy by closing the phone booth door.[139] Justice Harlan acknowledged that a phone booth "is a temporary private place whose momentary occupants' expectations of freedom from intrusion are recognized [by society] as reasonable."[140] Because Katz's conduct satisfied both the subjective and objective prongs of what later became known as the *Katz* test, the Court found that the government's conduct violated Katz's Fourth Amendment rights.[141] The Court expressly adopted the *Katz* test in the 1979 case of *Smith v. Maryland* ("*Smith*").[142]

For decades following *Katz*, Fourth Amendment cases turned on the right to privacy. Then, in the 2012 case of *United States v. Jones* ("*Jones*"),[143] the Court ruled that *Katz* had supplemented, rather than replaced, the earlier trespass standard. In *Jones*, law enforcement officers attached a GPS device to the exterior of Jones' car without Jones' knowledge or consent and tracked his movements for twenty-

---

[135] Olmstead v. United States, 277 U.S. 438 (1928) (finding no trespass, and thus no Fourth Amendment violation, where wiretapping occurred on the outside of a building); *see also* Goldman v. United States, 316 U.S. 129 (1942) ("Detectaphone" on outside of building not a Fourth Amendment violation); On Lee v. United States, 343 U.S. 747 (1952) (speaker's consent to presence of informant precluded trespass, required to find Fourth Amendment violation).

[136] 389 U.S. at 347.

[137] *Id.* at 351.

[138] *Id.* at 361 (Harlan, J., concurring).

[139] *Id.* at 352.

[140] *Id.*

[141] *Id.* at 359.

[142] 442 U.S. 735, 739–40 (1979).

[143] 132 S. Ct. 945 (2012).

eight straight days.[144] Since the intrusion on the vehicle—a common law trespass—was for the purpose of obtaining information, the Court ruled that it was a Fourth Amendment search and unreasonable absent a warrant.[145] The Court relied on *Jones*' "trespass" reasoning in *Florida v. Jardines*[146] to rule that police cannot bring a drug-detection dog to sniff at the front door of a home without probable cause and a warrant.

In the aftermath of *Jones*, if a government action is designed to obtain information, then either a trespass or a "*Katz* invasion of privacy" will render that action a search in violation of the Fourth Amendment. Thus, an attorney may rely on either physical trespass or a *Katz* invasion of privacy in asserting a violation of her Fourth Amendment rights.

A. Limits of the Fourth Amendment—Public vs. Private Papers

This Comment addresses government surveillance of an attorney's person, as well as his papers, via surreptitious electronic recording. As to papers, the Fourth Amendment does not protect that which is voluntarily exposed to the public.[147] Instead, it is primarily concerned with protecting that which comprises a person's intimate life. For the purposes of constitutional protection, therefore, it is paramount to distinguish between public and private papers.

In the 1976 case of *United States v. Miller* ("*Miller*"), the Supreme Court held that citizens have no privacy expectation in their bank records, insofar as the information kept in these papers is *voluntarily conveyed* to the banks in the usual course of business.[148] Applying similar reasoning, the Court held in the 1979 case of *Smith*[149] that Americans have no expectation of privacy in the telephone numbers they dial; as a result, a subpoena on telephone companies to turn over pen registers does not violate the Fourth Amendment.[150] Bank and telephone records, therefore, are public papers for constitutional purposes.

Smith and *Miller* are distinguishable from the instant situation on a number of grounds. First, the validly gathered information in those cases did not comprise private communications that have recognized constitutional and evidentiary protections. Here, both attorney-client conversations, as well as notes and emails drafted by the attorney in the

---

144 *Id.* at 948.
145 *Id.* at 954.
146 Florida v. Jardines, 133 S. Ct. 1409, 1417 (2013).
147 United States v. Miller, 425 U.S. 435, 443 (1976).
148 *Id.*
149 442 U.S. 735 (1979).
150 *Id.* at 745–46.

course of his legal representation, are afforded attorney-client and work-product privilege in addition to protection under the Sixth Amendment's right to effective assistance of counsel that bars interception of attorney-client communications.[151] Second, the information in *Smith* and *Miller* was voluntarily turned over to third-parties, who in turn gave it to the government; here, the government is illegally taking the information without the parties' knowledge or consent.[152] Thus, neither *Smith* nor *Miller* provides a barrier to recovery by an attorney whose private communications are monitored without his knowledge or consent. If anything, these cases serve to underscore that, where information is not voluntarily turned over to a third party—indeed, where measures have been taken to guard against the possibility that third parties will obtain that information—the information retains its Fourth Amendment privacy protections.

B. Limits of the Fourth Amendment—Personal Rights

United States v. Payner ("*Payner*") is often cited for the proposition that attorneys do not have a reasonable expectation of privacy distinct from their client's. This reliance on *Payner* is misplaced. *Payner* held that constitutional rights are personal and may not be vicariously asserted.[153] In *Payner*, the IRS broke into a banker's briefcase to steal documents about defendant Payner's fraudulent transactions. The Supreme Court held that the defendant had no recourse for the knowingly illegal intrusion into the banker's briefcase because the defendant had no reasonable expectation of privacy in either (1) another person's effects/papers or (2) the information he had voluntarily turned over to the banker.

The *Payner* Court did *not*, however, hold that the *banker* had no recourse for the violation of his personal constitutional rights, which is the precise issue this Comment addresses. Said another way, *Payner* precludes Professor Denbeaux's *client* from seeking to suppress emails stolen from Professor Denbeaux's account, but does *not* preclude Professor Denbeaux himself from asserting a violation of his own Fourth Amendment rights. Thus, *Payner* cannot be used to deny that an attorney has Fourth Amendment rights distinct from his client's.

---

[151] *See, e.g.*, Geders v. United States, 425 U.S. 80, 91 (1976) (preventing defendant from consulting with counsel during overnight recess violates Sixth Amendment); Weatherford v. Bursey, 429 U.S. 545, 563 (1977) (Marshall, J., dissenting) ("[G]overnmental incursions into confidential lawyer-client communications threaten criminal defendants' right to the effective assistance of counsel.").

[152] *See infra* Part II; *see also supra* note 7.

[153] United States v. Payner, 447 U.S. 727 (1980).

C. Limits of the Fourth Amendment—Privacy Expectations in Jail

An incarcerated person has a lesser expectation of privacy than a free man.[154] It does not necessarily follow, however, that attorney communications with an incarcerated client receive lesser Fourth Amendment protection than with an un-incarcerated client. Indeed, the Supreme Court expressly stated in *Lanza v. New York* ("*Lanza*") that "[e]ven in jail, or perhaps especially there, the relationship which the law has endowed with particularized confidentiality must continue to receive unceasing protection."[155]

More recently, the United States District Court for the Eastern District of New York in *Lonegan v. Hasty* ("*Lonegan*") held that "in the prison setting, attorney-client communications generally are distinguished from other kinds of communications and exempted from routine monitoring."[156] *Lonegan* involved the taping of suspected 9/11 terrorists' attorney-client meetings at the Brooklyn, New York MDC.[157] The government argued that the presence of video cameras in the meeting area and the fact that the detainees were terrorism suspects rendered the defense attorneys' subjective expectation of privacy objectively unreasonable.[158] The *Lonegan* court disagreed, holding that "the existence of robust protections for attorney-client communications makes [the attorneys'] expectation of privacy in their conversations with Detainees reasonable."[159] Indeed, the *Lonegan* court expressly noted that attorney-client communications are protected by the Fourth Amendment,[160] and found that the attorneys had stated a sufficient claim of a Fourth Amendment violation to survive a motion to dismiss.

---

[154] Hudson v. Palmer, 468 U.S. 517, 526 (1984) ("[T]he Fourth Amendment proscription against unreasonable searches does not apply within the confines of the prison cell. The recognition of privacy rights for prisoners in their individual cells simply cannot be reconciled with the concept of incarceration and the needs and objectives of penal institutions."); Florence v. Bd. of Chosen Freeholders of Cnty. of Burlington, 132 S. Ct. 1510, 1517 (2012) (holding that even detained arrestees have a lesser expectation of privacy in arriving at jail).

[155] Lanza v. New York, 370 U.S. 139, 143–44 (1962); *see also* In re State Police Litig., 888 F. Supp. 1235, 1256 (D. Conn. 1995) ("[W]here conversations (in jail) consist of privileged communications between clients and their attorneys, an expectation of privacy is reasonable.").

[156] Lonegan v. Hasty, 436 F. Supp. 2d 419, 432 (E.D.N.Y. 2006). This statement may be contrasted with the BOP Regulation, which involves targeted rather than routine monitoring.

[157] *See* discussion *supra* Part II.

[158] *Lonegan*, 436 F. Supp. 2d at 432.

[159] *Id.*

[160] *Id.* at 435.

While some intrusive measures unique to prison life may lower an attorney's expectation of privacy while there—such as turning over a cell phone or being subject to a pat-down—these measures should not affect the attorney's expectations with regard to his client conversations. First, the sacrosanct position of attorney-client communications in the legal sphere militates in favor of the notion that privacy and confidentiality will govern all such communications.[161] As stated in *Lanza*, the attorney-client relationship is guarded with the utmost protection, even or perhaps especially in jail. Second, the intrusive measures taken in prisons are justified on the grounds of physical safety and security, not obtainment of information for law enforcement purposes. There is no increase in physical safety by the surreptitious monitoring of privileged communications. As such, an attorney retains the same expectation of privacy in a jail with regard to her attorney-client communications as she does elsewhere.

In the case of Guantanamo habeas corpus attorneys, an attorney has an even higher expectation of privacy when escorted to a private interview room to meet her client, while receiving express assurances that no surveillance is occurring within.[162] Those assurances speak to the reasonableness of the attorney's subjective expectation of privacy, and would certainly influence the reasonable person's expectations under the circumstances.

V. GOVERNMENT INTRUSION INTO ATTORNEY-CLIENT COMMUNICATIONS VIOLATES THE FOURTH AMENDMENT PRIVACY RIGHTS OF THE ATTORNEY

Because traditional "standing" doctrine has been abrogated in favor of the *Katz* reasonable expectation of privacy test,[163] an attorney's right to assert a constitutional violation is not dependent on, or derivative of, his client's right to assert the same. Instead, so long as the government actor has either violated an attorney's reasonable expectation of privacy or physically trespassed on an attorney's protected area or item, the attorney's Fourth Amendment rights have been violated. Said another way, government intrusion into attorney-

[161] *See* Gennusa v. Shoar, 879 F. Supp. 2d 1337, 1349 (M.D. Fl. 2012) ("No reasonable attorney in Gennusa's position would have expected that her conversations with her client were being actively monitored and recorded when no officers were present in the room.").

[162] *See supra* Part II.

[163] Rakas v. Illinois, 439 U.S. 128, 139 (1978) ("[W]e think the better analysis forthrightly focuses on the extent of a particular defendant's rights under the Fourth Amendment, rather than on any theoretically separate, but invariably intertwined, concept of standing.").

client communications violates the Fourth Amendment privacy rights of the attorney under either the *Katz* invasion of privacy test or the *Jones* trespass test.

A. The Katz Test—Subjective Expectation of Privacy

To reiterate, the *Katz* test requires that a government actor violate a person's subjective expectation of privacy, which is one that society objectively recognizes as reasonable.[164] Generally, a person manifests her subjective expectation of privacy by taking actions that signal the exclusion of others. Building a fence around one's home,[165] putting up "No Trespassing" signs,[166] and drawing the blinds[167] have all been held as sufficient manifestations of a subjective expectation of privacy. As to papers specifically, a person may put private documents in a locked briefcase[168] or deposit box.[169] For intangible papers like emails, most people have the ability to password-protect their email accounts.[170] Taking additional steps like encryption[171] or, in the special case of attorneys, having a "confidentiality notice,"[172] would likewise suffice. As to verbal communications, actions like whispering, closing the door, or asking others not to interrupt signal to the outside world that the conversation about to take place is private.[173] Indeed, closing the phone booth door was all the proof the Supreme Court required to demonstrate a subjective expectation of privacy in the *Katz* case

[164] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

[165] *See, e.g.*, Florida v. Riley, 109 S. Ct. 693 (1989).

[166] *See, e.g.*, United States v. Dunn, 480 U.S. 294, 302 (1987).

[167] *See, e.g.*, United States v. Fields, 113 F.3d 313, 321 (2d Cir. 1997) (noting that no reasonable expectation of privacy, and therefore no Fourth Amendment violation, existed where defendant failed to draw the blinds and contraband was visible); United States v. Wisniewski, 21 M.J. 370, 372 (C.M.A. 1986) (same); United States v. $61,433.04 U.S. Currency, 894 F. Supp. 906, 917 (E.D.N.C. 1995), *aff'd sub nom.*, United States v. Taylor, 90 F.3d 903 (4th Cir. 1996) (same).

[168] *See, e.g.*, United States v. Payner, 447 U.S. 727, 732 (1980).

[169] *See, e.g.*, United States v. Thomas, No. 88-6341, 1989 U.S. App. LEXIS 9628, at *6 (6th Cir. July 5, 1989).

[170] *See, e.g.*, United States v. Andrus, 483 F.3d 711, 718 (10th Cir. 2007) (comparing password-protected files with a "locked footlocker" or other locked, personal containers for Fourth Amendment purposes).

[171] *See, e.g.*, Trulock v. Freeh, 275 F.3d 391, 412 (4th Cir. 2001) (likening encryption to locked, personal containers and citing a Department of Justice manual indicating that there can be no apparent authority to search encrypted or password-protected emails).

[172] *See, e.g.*, Convertino v. U.S. Dep't of Justice, 674 F. Supp. 2d 97, 110 (D.D.C. 2009) (finding confidentiality notice sufficient to manifest reasonable expectation of privacy in attorney-client emails even though sent through employer email account).

[173] In re Sealed Case, 737 F.2d 94, 102 (D.C. Cir. 1984).

itself.[174]

In the case of the Guantanamo attorneys, each of the lawyers manifested a subjective expectation of privacy as to communications with their clients in several ways. First, the attorneys were only allowed to meet their clients in one closed, secure interrogation room in Camp Echo.[175] Second, the attorneys questioned multiple government representatives regarding the security and privacy of the meeting room, and were assured on multiple occasions that the meetings were not being monitored.[176] Third, the habeas attorneys were all directed to use one allegedly secure server for sending and storing emails and documents related to their representation. Many of the defense's emails and work-product documents disappeared from that secure server.[177] The government assured the attorneys that their documents and emails were erroneously erased during a technical malfunction in backing up the secure drive; coincidentally enough, however, none of the government's own emails or documents were deleted during this process. Only defense documents disappeared. In sum, the Guantanamo attorneys manifested a subjective expectation that their client conversations—both in-person and remote—would remain private.

B. The Katz Test—Objectively Reasonable Expectation of Privacy

There is simply no question that an objectively reasonable expectation exists that attorney-client communications are not being surreptitiously monitored by the government. Society at large must expect attorney-client communications to be confidential, or else attorneys would never be able to elicit sufficient facts from their clients to adequately prepare a defense. The Supreme Court has noted the damaging "chilling effect" on attorney-client communications that would result if society did not have faith that attorneys keep mum about clients' business.[178]

The law is rife with language extolling the necessity of keeping attorney-client communications confidential. As the Supreme Court puts it, "[b]ecause of the significance of encourag[ing] the client to

---

[174] Katz v. United States, 389 U.S. 347, 351 (1967).

[175] DENBEAUX ET AL., SPYING ON ATTORNEYS, *supra* note 35, at 1.

[176] *Id.* at 6.

[177] Defense Motion to Abate, *supra* note 42.

[178] Fisher v. United States, 425 U.S. 391, 402–05 (1976) (attorney-client privilege protects only those disclosures which might not have been made absent the privilege, because the purpose of the privilege is to encourage confidential disclosures by a client to an attorney).

communicate fully and frankly with counsel, attorney-client communications have been universally recognized as confidential—even after the client's death."[179] As one scholar writes, "the expectation of privacy associated with [attorney-client communications] is more than reasonable—it is necessary."[180] In addition to being the oldest of all evidentiary privileges,[181] the Model Rules of Professional Conduct likewise recognize the confidentiality of attorney-client communications.[182] Even the far-reaching BOP Regulation requires that the attorney be notified if monitoring is to take place.[183] In fact, violating attorney-client confidentiality is so egregious an offense to our legal system that it *per se* represents a violation of the client's Fifth Amendment right to due process of law,[184] as well as his Sixth Amendment right to the effective assistance of counsel.[185] There is thus no doubt that society is prepared to recognize an attorney's expectation that her client conversations are private.

In sum, the Guantanamo attorneys manifested a subjective expectation that their client communications were private, which is an expectation that society deems reasonable. As such, surreptitious government monitoring of these conversations—after express assurances that no monitoring was taking place, no less—constitutes a Fourth Amendment search under the *Katz* test.

C. The Jones Trespass Test

Again, the Supreme Court held in *Jones* that whenever the government physically intrudes on a constitutionally protected area or item to obtain information for law enforcement or investigative reasons, a Fourth Amendment search has occurred and a warrant is required.[186] *Jones* also clarified that a "seizure" of property occurs when there is "some meaningful interference with an individual's possessory interest" in that property.[187] Under *Jones*, government surveillance of attorney-client communications is a Fourth Amendment trespass on two grounds. First, the notes attorneys take during client

[179] Swidler v. United States, 524 U.S. 399, 410–11 (1998) (emphasis added).

[180] Cunningham & Srader, *supra* note 9, at 339.

[181] FED. R. EVID. 501.

[182] MODEL RULES OF PROF'L CONDUCT R. 1.6 (2015).

[183] 28 C.F.R. § 501.3(d)(2) (2014).

[184] Dobbins, *supra* note 12.

[185] *See* Weatherford v. Bursey, 429 U.S. 545 (1977); Massiah v. United States, 377 U.S. 201 (1964). *See also* Lonegan v. Hasty, 436 F. Supp. 2d 419, 432 (E.D.N.Y. 2006).

[186] United States v. Jones, 132 S. Ct. 945, 950 (2012).

[187] *Id.* at 958 (Alito, J., concurring) (quoting United States v. Jacobsen, 466 U.S. 109, 113 (1984)).

conversations, as well as their emails or other correspondence relating to the legal representation, are constitutionally protected "papers" under the Fourth Amendment.[188] The viewing and copying of attorney notes via furtive digital video recording constitute a trespass search under *Jones*. Likewise, the government's surreptitious deletion of attorney emails and work-product documents from the allegedly secure server constitutes a "seizure."[189] Second, the designated room in which attorneys meet their clients to have confidential and privileged conversations is a constitutionally protected area.[190] Much like the "spike mikes" of generations past, the clandestine placement of video cameras and microphones in the designated room where attorneys meet their clients is a physical trespass into the intimate papers, effects, and person of the attorney.

It is clear that the government interfered with Guantanamo attorney-client communications for the illicit reason of "obtaining information."[191] First, one of the stated purposes of recording attorney-client conversations at Guantanamo Bay "was to assist in the preparation of debriefing reports."[192] Second, multiple government agencies have drafted reports based on the same attorney-client recordings.[193] Assuming, *arguendo*, that the eavesdropping was not for law enforcement purposes, there is little value to listening-in on attorney-client communications at Guantanamo beyond getting the defense's trial strategy. Such a purpose, of course, is no less illicit under the Fourth Amendment because it is still a trespass on a constitutionally protected area for the purpose of obtaining information. Thus, whether the government's actions at Guantanamo vis-a-vis attorney-client communications are analyzed under the *Katz* expectation of privacy test or the *Jones* trespass test, the result is the same: the government is violating the Fourth Amendment.

---

[188] *See, e.g.*, United States v. DeFonte, 441 F.3d 92, 94 (2d Cir. 2006) (holding that attorney-notes and other work product stored in a prison cell have a diminished expectation of privacy, but that those stored elsewhere retain their constitutional protections).

[189] *Jacobsen*, 466 U.S. at 113 (holding that a Fourth Amendment "seizure" occurs whenever there is "meaningful interference with," including taking possession of, one's property).

[190] *See* Lanza v. New York, 370 U.S. 139, 143 (1962).

[191] *Jones*, 132 S. Ct. at 950.

[192] DENBEAUX ET AL., SPYING ON ATTORNEYS, *supra* note 35, at 14 (quoting CIA OFFICE, *supra* note 20, at 36).

[193] DENBEAUX ET AL., SPYING ON ATTORNEYS, *supra* note 35, at 14 (*comparing* CIA OFFICE, supra note 20, at 36, *with* AIR FORCE OFFICE, *supra* note 30, at 60).

VI. CONGRESS SHOULD PASS LEGISLATION MAKING INVASION OF PRIVACY A FEDERAL CAUSE OF ACTION

This Comment has thus far identified a two-fold problem. First, the federal government is spying on attorney-client communications at Guantanamo and is very likely spying on Guantanamo attorneys' private communications outside Guantanamo as well.[194] Second, currently available remedies are insufficient to either correct the intrusions or incentivize the government to stay within constitutional bounds. This Part details the insufficiency of current remedies and proposes that the solution is Congressional action.

While Congress has permitted government surveillance of attorney-client communications in some contexts, it nearly always requires procedural safeguards like minimization procedures and *ante* and *post hoc* judicial review.[195] Yet, both the government surveillance and the judicial review may be conducted permissibly in secret.[196] Those who are able to discover the surveillance and seek redress for the unconstitutional invasion of their privacy must file a *Bivens* action.

A *Bivens* action is an eponymous nod to the case that first recognized a cause of action for constitutional violations by federal actors, *Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics*.[197] By contrast, where constitutional violations are carried out by state or municipal actors, aggrieved parties file suit under 42 U.S.C. § 1983. Historically, it made sense for Congress to provide a statutory cause of action for state and municipal constitutional violations but not for federal violations, as the general police power (and therefore the majority of criminal process) was effected by state and municipal actors. As the federal government becomes increasingly involved in general police work, however—particularly in the booming arenas of immigration, drug enforcement, cybercrimes, and terrorism—the federal government's accountability should increase proportionally.

Unlike a Section 1983 claim, liability under *Bivens* attaches only to individual actors and not government agencies.[198] This rule only decreases an aggrieved attorney's possibility of recovery. First, it may be impossible to identify individual actors given the clandestine nature of spying; indeed, it may even be impossible to name which agency the agents work for, as plaintiff Bivens did.[199] Second, there is no implied

194 *See supra* Part II.
195 *See supra* Part III.
196 *See supra* Part III.D.
197 403 U.S. 388 (1971).
198 *Id.* at 396–97.
199 *Id.*

private right of action under *Bivens* against private entities that engage in alleged constitutional deprivations while acting under color of federal law.[200] As such, an aggrieved attorney could not sue, for example, Hotmail, for turning over all of his emails to the government, even if Hotmail violated the attorney's Fourth Amendment rights in doing so.

The biggest hurdle represented by *Bivens* actions, however, is the judiciary itself. Jurists determining *Bivens* actions have unilaterally denied Fourth Amendment claims based on government surveillance; no person—attorney or otherwise—has succeeded on the merits in a Fourth Amendment suit based on government surveillance.[201] Federal courts have only recognized that such a cause of action even exists four times.[202] At least empirically speaking, then, leaving our constitutional right of privacy to the discretion of the judiciary in a *Bivens* action seems imprudent.

Similarly, attorneys have not succeeded in actions asserting violations of the federal statutes alleged to protect citizens' privacy, discussed in Part III, *supra*.[203] Typically, courts dismiss actions by attorneys on grounds of standing, asserting that any constitutional violations that occur due to monitoring attorney-client communications inure to the client.[204] Courts have also dismissed attorneys' suits for failure to state a claim under Federal Rule of Civil

---

[200] *See, e.g.*, Walden v. Ctrs. for Disease Control and Prevention, 669 F.3d 1277 (11th Cir. 2012) (holding that employee could not sue government contractor employer under *Bivens* for Fourth Amendment violations); Flores v. United States, 689 F.3d 894 (8th Cir. 2012) (holding that alien who died in federal custody while awaiting deportation could not sue government contracted doctor or facility under *Bivens*).

[201] At least, the author can find none in the federal courts.

[202] *See* Klayman v. Obama, No. 13-0851 (RJL), 2013 WL 6571596 (D.D.C. Dec. 16, 2013) (holding that content providers like Google and Yahoo have standing to challenge NSA surveillance programs on Fourth Amendment grounds); Fazaga v. F.B.I., 885 F. Supp. 2d 978, 985 (C.D. Cal. 2012) (holding that Muslims sufficiently stated a Fourth Amendment violation based on unlawful police surveillance at their mosque to survive a 12(b)(6) motion); Gennusa v. Shoar, 879 F. Supp. 2d 1337 (M.D. Fl. 2012) (holding that attorney and client sufficiently stated a Fourth Amendment violation based on unlawful police surveillance at the police department to survive a 12(b)(6) motion); Lonegan v. Hasty, 436 F. Supp. 2d 419, 432 (E.D.N.Y. 2006) (same).

[203] *See, e.g.*, Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1143 (2013) (holding that attorneys had no standing to sue for Patriot Act violations stemming from NSA warrantless wiretapping of calls with their international clients); ACLU Found. of S. California v. Barr, 952 F.2d 457, 472 (D.C. Cir. 1991) (holding that attorneys failed to state a claim for Patriot Act violations where police intercepted attorney-client communications pursuant to a FISC order regarding clients); Al-Owhali v. Ashcroft, 279 F. Supp. 2d 13, 26–27 (D.D.C. 2003) (holding that only client, not attorney, could assert constitutional violations based on BOP Regulation monitoring).

[204] *See, e.g.*, Al-Owhali, 279 F. Supp. 2d at 26–27.

Procedure 12(b)(6), asserting either that attorneys do not have independent Fourth Amendment rights or that the surveillance was pursuant to a valid (if secret) court order.[205]

Moreover, the courts charged with keeping the government's surveillance within constitutional bounds—the FISCs—have officially held that secret, widespread, and non-targeted surveillance of American citizens does not violate the Fourth Amendment.[206] In August 2013, however, FISC Chief Judge Reggie B. Walton contradicted this official declaration. In a written statement to the Washington Post, Chief Judge Walton asserted that the FISC lacks the ability to independently verify how often government surveillance violates court rules that protect citizens' privacy and that the FISC cannot check the veracity of the government's assertions that the violations its staff members report are unintentional mistakes.[207] Instead, the "FISC is forced to rely upon the accuracy of the information that is provided to the Court," and "does not have the capacity to investigate issues of noncompliance."[208] Indeed, a May 2012 internal audit revealed thousands of violations of FISC court orders and rules per year.[209] In sum, then, it appears that the judiciary has neither the resources nor the willingness to provide an appropriate level of protection for citizens' constitutional rights in the face of sweeping executive power to conduct secret surveillance.

Even if the judiciary were diligently guarding citizens from unconstitutional government surveillance on a case-by-case basis, the courts' incremental, *ad hoc* response would remain an insufficient check against the current, sweeping executive intrusions. Given the judiciary's paltry response, the legislature is the last resort upon which we must call to keep the Executive in check. Congressional action is the appropriate response because neither the Executive's discretion pre-surveillance nor the judiciary's review post-surveillance has been sufficient to protect citizens' Fourth Amendment rights. Indeed, Congress is aware of the illegality of many federal surveillance

---

[205] *See, e.g.*, ACLU Found. of S. Cal., 952 F.2d at 472.

[206] In re Application, *supra* note 16.

[207] Carol D. Leonnig, *Court: Ability to Police U.S Spying Program Limited*, WASH. POST BLOG (August 15, 2013), http://www.washingtonpost.com/politics/court-ability-to-police-us-spying-program-limited/2013/08/15/4a8c8c44-05cd-11e3-a07f-49ddc7417125_print.html.

[208] *Id.*

[209] Barton Gellman, *NSA Broke Privacy Rules Thousands of Times Per Year, Audit Finds*, WASH. POST (Aug. 15, 2013), http://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html.

programs.[210] And while state law usually controls common law torts such as invasion of privacy,[211] federal law should proportionally expand as the federal government increasingly intrudes on the privacy of everyday citizens for general law enforcement purposes. Moreover, Congress has the resources and expertise to hold hearings and make findings in order to adopt the most effective procedural safeguards, and still retains the surveillance capabilities necessary for the Executive to secure our nation's safety. Given their comparable structures, Congress can even rely on state privacy statutes in drafting new legislation.

VII. CONCLUSION

Government surveillance of average citizens is at best objectionable, and more likely illegal and unconstitutional. Government eavesdropping on attorney-client communications, however, is a particularly egregious violation. Our legal system, as embodied in the United States Constitution, was founded by men diametrically opposed to government interference in everyday life. The Fourth Amendment in particular was meant to stand as a bastion against the government's ability to rummage through our personal effects, including our private correspondence. This Comment argues that there is not, and should not be, a "criminal defense attorney" exception to the Fourth Amendment. Specifically, the government should not be permitted to monitor a private citizen's personal communications simply because she has assumed legal representation of a criminal defendant. Yet, protected by a deferential and submissive judiciary, our federal agencies have been doing precisely that.

While this Comment provides evidence of government surveillance of Guantanamo attorney-client communications, it is easy to extrapolate the experience of Professor Denbeaux and his Guantanamo colleagues to the average, stateside defense attorney. Indeed, recent news headlines suggest that there is far more surveillance being conducted than anyone without security clearance can know. As attorneys, we know better than most the compelling privacy interests at stake when government surveillance goes unchecked. Lest the Fourth Amendment become a distant memory,

[210] *See* Publius, *After FISA Court Decision, Congress Can't Say They Didn't Know What NSA Is Up To*, THE FEDERALIST SOCIETY BLOG (Sept. 18, 2013, 9:54 AM), http://www.fedsocblog.com/blog/after_fisa_court_decision_congress_cant_say_they_didnt_know_what_nsa_is_up/.

[211] RESTATEMENT (SECOND) OF TORTS § 652A (Invasion of Privacy - General Principles) (1977).

it is time we call upon Congress to make unconstitutional, surreptitious government surveillance a federal cause of action for invasion of privacy.