

1-1-2013

Asocial Media: Cops, Gangs, and the Internet

James R. O'Connor

Follow this and additional works at: <http://scholarlycommons.law.hofstra.edu/hlr>



Part of the [Law Commons](#)

Recommended Citation

O'Connor, James R. (2013) "Asocial Media: Cops, Gangs, and the Internet," *Hofstra Law Review*: Vol. 42: Iss. 2, Article 9.
Available at: <http://scholarlycommons.law.hofstra.edu/hlr/vol42/iss2/9>

This document is brought to you for free and open access by Scholarly Commons at Hofstra Law. It has been accepted for inclusion in Hofstra Law Review by an authorized administrator of Scholarly Commons at Hofstra Law. For more information, please contact lawcls@hofstra.edu.

NOTE

ASOCIAL MEDIA: COPS, GANGS, AND THE INTERNET

I. INTRODUCTION

Criminal street gangs are not a new phenomenon in America,¹ but recent developments in technology and social interactions have changed the game—gangs are increasingly using social media to accomplish gang objectives and commit crimes.² This is no secret to law

1. See G. DAVID CURRY & SCOTT H. DECKER, *CONFRONTING GANGS: CRIME AND COMMUNITY* 13 (1998). While there is some disagreement among scholars as to exactly when gangs first emerged in the United States, it is generally accepted that they have been operating here since at least the nineteenth century. Compare *id.* at 13-14 (asserting that youth gangs have existed in the United States since at least the 1870s), with JOHN T. WHITEHEAD & STEVEN P. LAB, *JUVENILE JUSTICE: AN INTRODUCTION* 96 (7th ed. 2013) (claiming that the first youth gangs emerged as early as 1783. For more information about the emergence of gangs in the United States, see TYLER ANBINDER, *FIVE POINTS: THE NINETEENTH CENTURY NEW YORK CITY NEIGHBORHOOD THAT INVENTED TAP DANCE, STOLE ELECTIONS, AND BECAME THE WORLD'S MOST NOTORIOUS SLUM* 31 (2001) (discussing the earliest known account of American gang activity—as reported in *The Herald* in March 1836—which described a gang assault allegedly perpetrated by the infamous Bowery Boys gang in New York City).

2. See, e.g., NAT'L GANG INTELLIGENCE CTR., *NATIONAL GANG THREAT ASSESSMENT: EMERGING TRENDS* 11, 41 (2011) [hereinafter *THREAT ASSESSMENT*], available at <http://www.fbi.gov/stats-services/publications/2011-national-gang-threat-assessment/2011-national-gang-threat-assessment-emerging-trends> ("Gangs are becoming increasingly savvy and are embracing new and advanced technology to facilitate criminal activity and enhance their criminal operations."). The National Gang Intelligence Center's 2011 report, *National Gang Threat Assessment: Emerging Trends* ("*Threat Assessment*"), attributes a recent surge in gang membership to "the facilitation of communication and recruitment through the Internet and social media." *Id.* at 11. The *Threat Assessment* further asserts that social media has "made gang activity more prevalent and lethal" by providing an especially accessible avenue for gang members to "intimidate rivals and police, conduct gang business, showcase illegal exploits, and facilitate criminal activity"—all of which can lead to violence. See *id.* at 41-42; see also Scott Gutierrez, *Street Gangs Using Internet for Violent Bragging Rights: Masked Hoodlums Making Threats at MySpace, Other Sites*, SEATTLEPI.COM (July 9, 2006, 10:00 PM), <http://www.seattlepi.com/local/article/Street-gangs-using-Internet-for-violent-bragging-1208477.php> (indicating that as many as eight years ago, gang experts and law enforcement officials across the country had become deeply concerned by the growing presence of gang activity online, particularly on MySpace); Thomas Watkins, *Gangs' Use of Twitter, Facebook on the Rise*, HUFFINGTON POST (Feb. 2, 2010, 2:24 PM), http://www.huffingtonpost.com/2010/02/02/gangs-use-of-twitter-facebook_n_445551.html (reporting law enforcement's estimation in 2010 that "gangs are making greater use of Twitter and

enforcement. In fact, police departments and prosecutors regularly use the Internet and social media networks to obtain incriminating evidence against gang members—evidence that is often ruled admissible in court.³ Although the majority of the information seized in these investigations is highly personal and profoundly private, the details of the government's specific data-collection and data-storage practices remain shrouded in secrecy due to a glaring lack of regulation and transparency.⁴ Such

Facebook, where . . . they can make threats, boast about crimes, [and] share intelligence on rivals . . . [but that] the much-older MySpace . . . remains gang members' online venue of choice").

3. See, e.g., *People v. Liceaga*, No. 280726, 2009 WL 186229, at *3-4 (Mich. Ct. App. Jan. 27, 2009) (upholding the admission of a MySpace photo to identify defendant, who was depicted holding the murder weapon and "throwing" a gang sign"); INT'L ASS'N OF CHIEFS OF POLICE, SOCIAL MEDIA SURVEY RESULTS (2013) [hereinafter IACP SURVEY], available at <http://www.iacpsocialmedia.org/Portals/1/documents/2013SurveyResults.pdf> (detailing a survey of five hundred law enforcement agencies, spanning forty-eight states, in which 86.1% of the surveyed agencies reported using social media for criminal investigations, and 80.4% reported that social media has helped them solve crimes); Beth C. Boggs & Misty L. Edwards, *Does What Happens on Facebook Stay on Facebook? Discovery, Admissibility, Ethics, and Social Media*, 98 ILL. B.J. 366, 367-69 (2010) (noting that a court will typically admit online information into evidence without any special consideration or heightened scrutiny, but the determination of whether such information is discoverable is hardly well settled or well defined, as courts have struggled to uniformly decide discoverability disputes); George W. Knox, *Gang Members on Facebook: Should We Look the Other Way?*, NAT'L GANG CRIME RES. CENTER, <http://www.ngcrc.com/gangface.html> (last visited Jan. 2, 2014) (describing the relative ease with which investigators can utilize Facebook to identify and surveil gangs and other groups that present a security threat); John Lynch & Jenny Ellickson, Criminal Div., U.S. Dep't of Justice, Presentation to Computer Crime & Intellectual Prop. Section: Obtaining and Using Evidence from Social Networking Sites (Aug. 2009) [hereinafter Obtaining and Using Evidence], available at https://www.eff.org/files/filenode/social_network/20100303_crim_socialnetworking.pdf (revealing that federal law enforcement agencies regularly obtain personal information online).

4. See, e.g., Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored E-Mail*, 2008 U. CHI. LEGAL F. 121, 138 ("People reveal in their e-mails more about their political opinions, religious beliefs, personal relationships, intellectual interests, and artistic endeavors than they ever revealed over the telephone [and] . . . [s]tored e-mails, in particular, contain a vast archive of people's past activities."); Boggs & Edwards, *supra* note 3, at 367 ("A surprising number of people are shockingly candid when posting to their public profile on a social networking site."); T.C. Sottek, *NSA Used PRISM to Collect More than 200 Million Internet Communications a Year as of 2011*, VERGE (Aug. 21, 2013, 4:24 PM), <http://www.theverge.com/2013/8/21/4645042/nsa-prism-internet-communication-collection-200-million-fisc-order>. Writing for *The Verge*, T.C. Sottek revealed that the National Security Agency ("NSA")—purportedly targeting terrorist activity—secretly "collect[ed] private electronic data of users from services like Gmail, Facebook, Outlook, and others," including "incidental data belonging to innocent Americans with no connection to terrorism." Sottek, *supra* (internal quotation marks omitted); see also *infra* Part III (detailing the clandestine and officious data-collection practices of the NSA and other government agencies). Thus, in the course of a legitimate Internet investigation, the government can collect (and store) law-abiding citizens' private information without their knowledge, even though these citizens have little to no connection to the class of crimes that allegedly triggered the initial investigation. See Sottek, *supra*; see also Roger Yu, *Social Media Role in Police Cases Growing*, USA TODAY, Mar. 19, 2012, at 11B (quoting Lieutenant Lisa Thomas of the Cincinnati Police Department, who stated in 2012 that the department's Real Time Crime Center was "looking [on social media networks] at friends and friends of friends of the suspects" (emphasis added)). According to an

clandestine government policies create a slippery slope—one that could potentially transform the American society into a dystopia.⁵

It appears that law enforcement primarily gathers gang-related online data in two forms: (1) evidence of past, present, or impending gang crime; and (2) evidence of an individual's affiliation, or even mere association, with a particular street gang.⁶ Social network administrators are aware of the growing trend of gangs' increased use of the Internet.⁷ Some social media networks have implemented easy-to-use reporting policies to allow users (and some non-users) to notify network administrators of users' improper or illegal "abuses."⁸ The administrator

article by Roger Yu, Cincinnati's Real Time Crime Center ("RTCC") "monitor[s] the Internet and the cameras installed across the city." Yu, *supra*. In one reported instance, the RTCC was scrutinizing social media accounts to uncover information about the suspects of an ongoing criminal investigation. *Id.* While examining the suspects' Facebook pages, as well as the pages belonging to the suspects' "friends and friends of friends," RTCC analysts uncovered evidence of an unrelated (and undisclosed) crime when they "stumbled upon an online video . . . showing an act of armed robbery, helpfully taped by the perpetrators themselves." *See id.* Yu notes that the aggregate number of online investigations conducted by the Cincinnati Police Department remains unknown, as are the specific details regarding the precise nature and extent of online investigations, the department's storage (and destruction) practices, and the regularity with which police investigate suspects' associations—such as family, friends, and friends of friends. *See id.* Due to the current lack of regulation and transparency surrounding such law enforcement practices, citizens will likely never know whether the government has collected and stored their personal information—or, even, if they were ever surveilled by the government. *See Sottek, supra*; Watkins, *supra* note 2 (relating law enforcement's remarkable reluctance to discuss specific details of online investigations of gang activity).

5. *See infra* Part III.

6. *See Liceaga*, 2009 WL 186229, at *3-5 (admitting a MySpace photo, which prosecutors used to identify defendant and establish his gang involvement, into evidence); Kathryn Kinnison Van Namen, Comment, *Facebook Facts and Twitter Tips—Prosecutors and Social Media: An Analysis of the Implications Associated with the Use of Social Media in the Prosecution Function*, 81 MISS. L.J. 549, 552-53, 563-65 (2012) (indicating that various district attorneys and police departments have their own Facebook accounts, which they use—in part—to encourage citizens to provide "tips" about past, pending, and imminent crimes in their communities, and to evaluate suspects' and witnesses' personal associations and affiliations; investigate criminal activity; and prosecute gang members); *infra* Parts III.C–IV.A; *see also* IACP SURVEY, *supra* note 3 (noting that 80.4% of surveyed police departments reported "that social media has helped [them] solve crimes in their jurisdiction," and that 66.1% reported using social media for "intelligence" purposes).

7. Knox, *supra* note 3 (contrasting the approaches used by MySpace and Facebook in addressing social media gang activity). MySpace allows any person with Internet access, even one without a MySpace account, to report "gang-related language and/or images," which are prohibited by its "explicit guidelines." *Id.* Moreover, MySpace enforces a zero-tolerance policy for violations of its anti-gang "terms of use." *Id.* Facebook, on the other hand, has adopted a "laissez faire" attitude; it provides no mechanism "to report that a violent criminal street gang is gang-banging on Facebook." *Id.* Although hands-off reporting policies—such as those employed by Facebook—allow nefarious gang activity to persist online, they actually benefit law enforcement by increasing the amount of available gang intelligence, since gang members are permitted to remain active on the networks. *Id.* (demonstrating how a laissez-faire reporting policy can serve as a boon to online gang investigations).

8. *See id.*

of the network then examines the reported content, evaluates it, and determines whether to close the user's account and remove the content from the website.⁹ In some instances, information is voluntarily shared with law enforcement.¹⁰ However, these policies are often vague and far from transparent.¹¹

Courts, for the most part, find few problems with admitting evidence recovered under such circumstances, as long as it is relevant,¹² authenticated,¹³ and otherwise admissible.¹⁴ Notably,

9. *See id.*

10. *See* Obtaining and Using Evidence, *supra* note 3; Yu, *supra* note 4 (reporting that Facebook shares information with authorities to prevent fraud and other illegal activities, but refuses to elaborate on its information sharing practices).

11. *See* Knox, *supra* note 3.

12. Boggs & Edwards, *supra* note 3, at 369; *see, e.g.*, People v. Liceaga, No. 280726, 2009 WL 186229, at *3-4 (Mich. Ct. App. Jan. 27, 2009); *see also* FED. R. EVID. 402 (stating that evidence must be relevant in order to be admissible at trial). Evidence is relevant if: "(a) it has any tendency to make a fact more or less probable than it would be without the evidence; and (b) the fact is of consequence in determining the action." FED. R. EVID. 401. Evidence of gang affiliation gathered from social media can be found relevant as, for instance, such evidence may tend to identify a particular defendant in a criminal case. *See, e.g.*, Liceaga, 2009 WL 186229, at *3-4 (holding that MySpace photos of defendant holding a gun and "'throwing' a gang sign" were relevant in identifying defendant as the shooter and in tending to prove his familiarity with the murder weapon, where the defense theory was an accidental discharge of the firearm); *see also* Eric Tucker, *Don't Drink and Drive, Then Post on Facebook*, MSNBC (July 18, 2008, 1:37 PM), <http://www.nbcnews.com/id/25738225/?GT1=43001#UwFCgvdXeU> (describing cases where judges were swayed to impose stiff prison sentences on drunk-driving defendants after prosecutors presented photos from social media websites depicting the defendants—after their arrests—abusing alcohol, disrespecting the court, or showing an overall lack of remorse for their crimes).

13. *See* Heather L. Griffith, Note, *Understanding and Authenticating Evidence from Social Networking Sites*, 7 WASH. J.L. TECH. & ARTS 209, 217-23 (2012). Photographic and video evidence from social networking sites is particularly vulnerable to authenticity attacks. *See id.* at 222-23; *see also* Zachariah B. Parry, Note, *Digital Manipulation and Photographic Evidence: Defrauding the Courts One Thousand Words at a Time*, 2009 U. ILL. J.L. TECH. & POL'Y 175, 182-83 (illustrating the ease with which photographic evidence can be manipulated). Further, the person portrayed online may not be the real person—in fact, the "real person" may not even be real. *See* Manti Te'o Girlfriend Lennay Kekua Was a Man, CHICAGONOW (Jan. 25, 2013, 7:17 AM), <http://www.chicagonow.com/mayor-daily/2013/01/manti-teo-lennay-kekua-696>. Many states have passed laws criminalizing the impersonation of another online due to the serious nature of the potential consequences of such conduct—that is, the embarrassment and humiliation that arises when such impersonation is revealed, or, conceivably, the stress of criminal investigations and prosecutions based upon falsified social media evidence. *See, e.g.*, CAL. PENAL CODE § 528.5(a)–(d) (West Supp. 2013) (providing that "any person who knowingly and without consent credibly impersonates another actual person through or on an Internet Web site or by other electronic means for purposes of harming, intimidating, threatening, or defrauding another person is guilty of a public offense," and subject to fines of one thousand dollars, one year in jail, or both). However, many courts do not seem to be concerned with authentication and impersonation issues as they relate to criminal investigations. *See* Aviva Orenstein, *Friends, Gangbangers, Custody Disputants, Lend Me Your Passwords*, 31 MISS. C. L. REV. 185, 212-15 (2012). For a more thorough discussion of the authentication issues surrounding evidence obtained from social media, *see id.* at 202-21.

14. *See, e.g.*, Van Namen, *supra* note 6, at 565 (assembling that most courts admit relevant evidence regardless of its online form). *But see, e.g.*, Justin P. Murphy & Matthew A.S. Esworth,

however, law enforcement is not necessarily breaking any specific laws through its current investigative and data-mining practices.¹⁵ But, perhaps it should be.

This Note argues that law enforcement is properly using social media to investigate active cases and past crimes, and, when brought to its attention, to prevent imminent crime.¹⁶ However, law enforcement is dangerously toeing the line of constitutionality by collecting the personal data of non-suspects (and their purported affiliations or associations with a gang), and congressional guidance is needed to monitor these Orwellian practices.¹⁷ Since its sweeping, secretive data-collection practices were revealed in 2013, the National Security Agency (“NSA”) has become the center of a maelstrom of controversy and polemic public debate.¹⁸ The Planning Tool for Resource Integration, Synchronization, and Management (“PRISM”) tool—an NSA electronic surveillance program—exemplifies the type of government monitoring activities that urgently need transparency and regulation to give effect to the Fourth Amendment’s protections against unwarranted and unreasonable searches and seizures.¹⁹ Accordingly, this Note focuses on the government’s unregulated digital surveillance of suspected gang members and their associations, and the potential chilling effect that such practices may have on the First Amendment rights to free speech and association.²⁰

Part II of this Note will provide background regarding gang culture and gang members’ migration to social media; a basic understanding of gang norms and common practices is helpful to illustrate the volume of incriminating evidence that social media contains.²¹ Part III describes the

The ESI Tsunami: A Comprehensive Discussion About Electronically Stored Information in Government Investigations and Criminal Cases, CRIM. JUST., Spring 2012, at 31, 31 (surmising that courts have provided “little guidance” regarding electronically stored information).

15. See *infra* Parts III.C–IV.A.

16. See *infra* Parts II–IV.

17. See *infra* Parts III–IV; see generally GEORGE ORWELL, NINETEEN EIGHTY-FOUR (1949) (describing a hypothetical future where all citizens are constantly monitored by a totalitarian government that sees and knows all).

18. See Sottek, *supra* note 4.

19. See *infra* Parts III–IV.

20. See *infra* Parts II–IV.

21. See *infra* Part II. Gang members’ conduct is often driven by the desire to display certain coveted characteristics that are uniquely defined by gang culture; for instance, the highly valued attribute “toughness.” See Walter B. Miller, *Lower Class Culture as a Generating Milieu of Gang Delinquency*, J. SOC. ISSUES, Aug. 1958, at 5, 5-9. The desire to appear tough is inextricably intertwined with the common gang practice of “representing”—displaying one’s gang affiliation, as prompted by a sense of deviant duty and passionate pride, through the use of various “identifiers” such as graffiti, hand signs, symbols, clothes, and dance—and, more recently, through boasts of gang crimes on social media. *Id.* at 7-18; see SANYIKA SHAKUR, MONSTER: THE AUTOBIOGRAPHY

current state of the law with respect to online gang investigations by reviewing statutes permitting law enforcement to obtain electronic data from social media administrators and Internet Service Providers (“ISPs,” singularly “ISP”); court decisions upholding the admission of social media evidence in gang prosecutions; and relevant scholarly commentary on these issues.²² This Part also discusses the absence of statutory authority permitting the data-mining practices and online surveillance of suspected gang members and their families and friends, setting the stage for Part IV.²³ Part III further illuminates how the lack of legislative guidance and the related lack of transparency from law enforcement create a dangerously cavalier scenario that is rife with potential constitutional violations.²⁴ In this vein, Part III analyzes relevant constitutional protections as they relate to the collection of data on gang members not formally accused of crimes—with particular attention to the freedom of association²⁵—as well as the collection of data with respect to suspects’ friends and families.²⁶ Part III also addresses current investigative techniques, whether by law enforcement agencies or prosecutors, as well as the widely disparate reporting policies of various social media networks.²⁷

Part IV.A asserts that the current shadowy state of the law regarding law enforcement’s investigations and data-collection procedures leads to unbridled surveillance practices that lurk precariously close to the point of violating the Constitution.²⁸ To resolve this, Part IV.B proposes a federal statute that requires uniform reporting procedures for social media that would allow evidence of gang-related

OF AN L.A. GANG MEMBER 169 (1993); David Décary-Héту & Carlo Morselli, *Gang Presence in Social Network Sites*, 5 INT’L J. CYBER CRIMINOLOGY 876, 879-80 (2011); Gutierrez, *supra* note 2 (reporting the widespread use of social media as an avenue for gang members to brag about crimes); see also HOMEFRONT PROTECTIVE GROUP, TODAY’S GANGS: HOW TO RECOGNIZE THE SIGNS (2006), available at http://www.shannonscorner.com/downloads/Gang_Awareness.pdf.

22. See *infra* Part III; see also Brian Hyer, Note, *Protecting John Doe: A New Standard for John Doe Subpoenas that Respects the Right to Speak Anonymously Online*, 9 GEO. J.L. & PUB. POL’Y 495, 496, 498-99 (2011) (referring to ISPs as “the purveyors of online speech” and “tools of First Amendment expression”).

23. See *infra* Part III. Similarly problematic is the lack of scholarly commentary on the issue. See *infra* Parts II–III.

24. See *infra* Part III.

25. See *NAACP v. Alabama*, 357 U.S. 449, 460 (1958) (“It is beyond debate that freedom to engage in association for the advancement of beliefs and ideas is an inseparable aspect of the ‘liberty’ assured by the Due Process Clause of the Fourteenth Amendment, which embraces freedom of speech.”).

26. See *infra* Part III.

27. See *infra* Part III.C.

28. See *infra* Part IV.A.

crime to be communicated to the administrator.²⁹ The administrator would then be directed to follow internal procedures and potentially notify law enforcement if the evidence of a *crime* is credible.³⁰ But social media networks' policies must be clear, which the proposed legislation will ensure.³¹ The proposed statute further grants law enforcement the positive authority to collect data from social media administrators and the individual users' ISPs,³² if there is probable cause³³ to believe that a crime has occurred, or there is a reasonable probability of "imminent lawless action."³⁴ The statute explicitly prohibits data-collection based on a user's mere affiliation or association with a gang or gang member.³⁵ This comports with the freedom of association, and, thus, the statute should be upheld if challenged on such grounds.³⁶

As discussed in Part IV, state legislatures could use the federal statutes as models to draft their own state-specific regulations, and, perhaps, provide their citizens with additional privacy safeguards, as states may grant their respective citizens rights that extend beyond those provided by the federal government.³⁷ Similarly, state officials could issue executive orders directing state law enforcement authorities to act within the confines of the proposed federal statute.³⁸ The state executive orders could instruct the relevant agencies to promulgate additional safeguards by creating unambiguous policies and procedures within and among the various departments.³⁹ Likewise, a state executive, such as the attorney general, could issue a report urging the legislature to enact statewide laws to comply with the federal statute proposed herein.⁴⁰

29. See *infra* Part IV.B.

30. See *infra* Part IV.B.

31. See *infra* Part IV.B.

32. See *infra* Part IV.B.

33. The statute requires a higher standard of proof for evidence of criminality that is gathered from social media websites and other online sources due to the inherently unreliable nature of Internet evidence, and the significant authentication issues surrounding electronic evidence in general. See *infra* Part IV.

34. See *Brandenburg v. Ohio*, 395 U.S. 444, 447 (1969) (*per curiam*); *infra* Parts III.A, IV.B.

35. See *infra* Part IV.B.

36. See *infra* Parts III.B, IV.B.

37. See *infra* Part IV.B. This is the case because the federal government sets the *minimum* amount of citizens' rights, and therefore states may extend to their citizens additional rights and privileges, so long as they comply with the federal *minimum*. See U.S. CONST. art. VI, cl. 2; see also YALE KAMISAR ET AL., *BASIC CRIMINAL PROCEDURE* 25 (13th ed. 2012).

38. See *infra* Part IV.B (citing U.S. CONST. art. VI, cl. 2).

39. See *infra* Part IV.B.

40. See *infra* Part IV.B. This may be proper if the state legislature does not immediately pass legislation mirroring the proposed federal statute. Again, these state executive orders could even urge state legislators to stretch beyond the limits provided by the federal statute, in order to provide that state's citizens with *additional* privacy rights. See *supra* note 37 and accompanying text.

Part V encourages more scholarly commentary on the issue of gang investigations conducted through social media channels.⁴¹ The lack of specific legislation addressing this issue is one of the main problems in this arena, as this absence cultivates a headstrong atmosphere among the law enforcement authorities that investigate gang members (and law-abiding citizens) online.⁴² This cavalier atmosphere is cluttered with the clouds of brewing constitutional violations,⁴³ and the need to rein in police and prosecutors through statutory regulation is great.⁴⁴

II. GANGS IN AMERICA AND THE RISE OF SOCIAL MEDIA: FROM THE STREET CORNER TO THE FACEBOOK WALL

Anything from wallbangin' (writing your gang name on a wall, advertising) to spitting on someone to fighting—it's all work. And I was a hard worker.

— Sanyika Shakur, *Monster: The Autobiography of an L.A. Gang Member*⁴⁵

Gangs and gang crime pose serious threats to the safety and security of our nation.⁴⁶ As the fabric of our society evolves, social interactions among teens and youth have migrated from the playground to the computer screen; and, accordingly, so have gangs and gang members.⁴⁷ Gangs' online activities have, naturally, expanded the scope of law enforcement's Internet investigations.⁴⁸ But, the unknown nature and extent of the personal data collected—and how that data is both gathered and stored—potentially violate paramount protections of privacy guaranteed by the Constitution.⁴⁹ An understanding of the anti-

41. See *infra* Part V.

42. See *infra* Parts III–V.

43. See *infra* Parts III–V.

44. See *infra* Parts III–V.

45. SHAKUR, *supra* note 18, at 52.

46. THREAT ASSESSMENT, *supra* note 2, at 9 (“Gangs are expanding, evolving and posing an increasing threat to [U.S.] communities nationwide . . . [and] are responsible for an average of 48 percent of violent crime in most jurisdictions and up to 90 percent in several others . . .”). This assessment estimates that there are currently 33,000 gangs with over 1.4 million gang members nationwide. *Id.*

47. See *id.* at 27, 41–42 (contending that “advanced technology, such as wireless Internet . . . has made the recruitment, collaboration, and coordination of criminal activity more efficient and lucrative, and allows direct contact between the gangs and [drug trafficking organizations]”).

48. See *id.* at 27, 41–42.

49. See *infra* Parts III–IV. This is particularly true where the government collects the personal data of gang members without proper suspicion of criminal activity, or when the scope of an investigation extends to law-abiding citizens who happen to be (even tangentially) affiliated with a suspect. See *infra* Part III. The unwarranted invasion of privacy, and the government's intrusion into

social traits and values that permeate gangs and plague their members will help demonstrate why gangs have migrated to the virtual world, which has ultimately led to the problem at hand.⁵⁰

Part II.A will provide general background regarding gangs and gang culture.⁵¹ Part II.A will also articulate several of the main objectives and values that gangs typically harbor.⁵² Part II.B will focus on the advent of the Internet and the rapid migration of gangs from street corners to Internet cafés,⁵³ and will demonstrate how gang culture on the Internet and social media has become prevalent, which has forced law enforcement to expand the scope of its online investigations of gangs and suspected gang members.⁵⁴

A. Gangs and Gang Culture

While there is some debate as to when gangs first emerged in the United States,⁵⁵ the general consensus is that Irish immigrants in the Five Points neighborhood of New York City formed the earliest gangs in the 1800s; these immigrants banded together for protection and as a means of survival.⁵⁶ As time went on, the primary ethnic identity of

citizens' online personas, infringe upon the bedrock of our free and autonomous society. *See infra* Parts III–IV.

50. *See infra* Parts II–III.

51. *See infra* Part II.A.

52. *See infra* Part II.A.

53. *See infra* Part II.B.

54. *See infra* Part II.B; *see also infra* Part III.C (discussing in detail the government's online investigation tactics).

55. *See infra* Part II.B; *see also supra* note 1 and accompanying text. There are many definitions of the term “gang.” Compare BLACK’S LAW DICTIONARY 331 (4th Pocket ed. 2011) (defining a gang as “[a] group of persons who go about together or act in concert, [especially] for antisocial or criminal purposes,” and explaining that “[m]any gangs have common identifying signs and symbols, such as hand signals and distinctive colors”), with FREDERICK M. THRASHER, THE GANG: A STUDY OF 1313 GANGS IN CHICAGO 46 (abridged ed. 1963) (defining a gang as “an interstitial group originally formed spontaneously and then integrated through conflict,” which, essentially, can be any group of youth that form together and engage in mischief). For the purposes of this discussion, the term “gang” refers to large, organized groups—such as the Bloods and Crips—that utilize explicit by-laws, gang rituals, and/or identifying colors and symbols, rather than loosely-organized groups of youth who socialize and commit crimes. For simplicity, this Note defers to the government’s definition of the term “gang” in the U.S. Code, which defines a criminal street gang as “an ongoing group, club, organization, or association of five or more persons . . . that ha[s] as [one] of their primary purposes the commission of . . . criminal offenses.” 18 U.S.C. § 521(a)(A) (2006). In this context, the U.S. Code defines “criminal offenses” as: “(1) a Federal felony involving a controlled substance”; “(2) a Federal felony crime of violence that has as an element the use or attempted use of physical force against the person of another”; and “(3) a conspiracy to commit an offense described in paragraph (1) or (2).” *Id.* § 521(c).

56. *See* HERBERT ASBURY, THE GANGS OF NEW YORK: AN INFORMAL HISTORY OF THE UNDERWORLD 1-2, 26-27 (Thunder’s Mouth Press 2001) (1928) (providing a concise historical overview of the evolution of the American street gang, beginning with the era of the Five Points

gangs evolved from Irish to Italian, then to Jewish, and, finally, to African-American.⁵⁷ Like the gangs of yesteryear, most modern gangs are predominantly composed of youth, and are generally located in densely populated urban areas.⁵⁸

Gangs exhibit attributes of a culture separate and distinct from mainstream society.⁵⁹ Within this gang subculture, there are several norms and values that are, as one scholar posits, absent from mainstream society, but, instead, are “absorbed from the culture of the lower class.”⁶⁰ These include: (1) toughness; (2) trouble; (3) autonomy; (4) excitement; (5) smartness; and (6) fate.⁶¹ These seemingly simple terms warrant further explanation, as they represent meanings in this context that are quite different from their colloquial counterparts.

The term “toughness” does not merely refer to physical strength or athletic ability.⁶² Rather, the term refers to the *need* to “stand up to adversity”—what Walter Miller describes as “whatever the street brings (for example, run-ins with other gangs and the police).”⁶³ Gang culture, Miller explains, is “preoccup[ied] with getting into, or staying out of, trouble”; and “trouble” itself “refer[s] to violent situations or interactions with the police.”⁶⁴ In today’s world, these interactions can, and often do, occur within the realm of social media—for instance, when members of one gang threaten rivals with violence.⁶⁵ “Autonomy,” in this context, means “[t]he intolerance of challenges to one’s personal sphere—the need to stand up to anything or anyone.”⁶⁶ The concern for “autonomy” accounts for gang members’ reluctance to resort to legitimate authorities

neighborhood in New York City); *see also supra* note 1.

57. See James C. Howell & John P. Moore, *History of Street Gangs in the United States*, NAT’L GANG CENTER BULL., May 2010, at 1, 1-4, available at <http://www.nationalgangcenter.gov/Content/Documents/History-of-Street-Gangs.pdf> (describing the emergence, evolution, and ethnic character of street gangs in the northeast and New York City).

58. See, e.g., *id.* at 9, 15 (providing examples of gangs primarily composed of youth, discussing urban areas that are riddled with serious gang problems, and considering various causes of gang activities, such as youth unemployment).

59. See Miller, *supra* note 18, at 6-14 (discussing the focal concerns of the lower class life of which gangs are a part).

60. GENNARO F. VITO & JEFFREY R. MAAHS, *CRIMINOLOGY: THEORY, RESEARCH, AND POLICY* 159 (3d ed. 2012) (discussing the views of a renowned gang researcher, Walter Miller, and applying them to modern street gangs); *see* Miller, *supra* note 18, at 15 (“Focal concerns of the male adolescent corner group are those of the general cultural milieu in which it functions.”).

61. Miller, *supra* note 18, at 7-13.

62. VITO & MAAHS, *supra* note 60, at 159; Miller, *supra* note 18, at 9.

63. VITO & MAAHS, *supra* note 60, at 159; *see* Miller, *supra* note 18, at 9.

64. VITO & MAAHS, *supra* note 60, at 159; *see* Miller, *supra* note 18, at 8.

65. *See infra* Part II.B.

66. VITO & MAAHS, *supra* note 60, at 159; *see* Miller, *supra* note 18, at 12-13. Today, this personal sphere extends to one’s online persona—no longer are threats and intimidations made solely on the streets; they are now issued across social media networks as well. *See infra* Part II.B.

to deal with crimes—specifically violent crimes—that were committed against them or directed at their respective gang.⁶⁷ Instead, gangs and gang members prefer to settle such disputes autonomously, on their own.⁶⁸

“Excitement” can be viewed in terms of the ordinary definition of the word, in that gang members perceive life as “all about the thrill”; however, their thrill-seeking activities tend to focus on “flirting with danger” and “engaging in conflict,” a far departure from the forms of excitement entertained by law-abiding citizens.⁶⁹ Likewise, the term “smartness” does not refer to traditional measures of intelligence, such as IQ; rather, “smartness” denotes “street smarts”—an asset to which gang culture assigns a “high value.”⁷⁰ In other words, a gang member must be able to “handle oneself on the street.”⁷¹ In today’s world, the “street” has extended beyond the pavement into the blogosphere.⁷² It follows that gang members must be capable of adequately responding to intimidation and threats from rival gang members across social media outlets, otherwise they will suffer the repercussions of being viewed as weak—that is, unable or unwilling to properly represent and defend their gang and its values.⁷³ Finally, Miller uses the term “fate” to convey the notion, common among gang members, that “whatever happens is meant

67. See VITO & MAAHS, *supra* note 60, at 159; Miller, *supra* note 18, at 12-13.

68. See VITO & MAAHS, *supra* note 60, at 159; Miller, *supra* note 18, at 12-13.

69. VITO & MAAHS, *supra* note 60, at 159; see Miller, *supra* note 18, at 10-11.

70. VITO & MAAHS, *supra* note 60, at 159; Miller, *supra* note 18, at 9-10. One collateral consequence of the social media revolution is that the “street” is no longer confined to the pavement and playground. See *supra* note 2 and accompanying text; see also Van Namen, *supra* note 6, at 555 (analogizing social networks to “the new public square”). Thus, today’s gang members likely strive to possess and portray the “smartness” to act (and react) accordingly—they must be able to “handle [themselves]” not only on the street, but also online. See THREAT ASSESSMENT, *supra* note 2, at 11, 41-42 (confirming that gang members have extended their enterprises to cyberspace, and that they successfully use the Internet and social media to further their devious endeavors); VITO & MAAHS, *supra* note 60, at 159 (defining “smartness” as the ability to “handle oneself on the street”); Miller, *supra* note 18, at 7-13 (demonstrating that gang members exert great effort to evince the attributes of gang culture, which preponderate all other values and goals). Today’s gang members assert these aberrant attributes by creating online personas that allow them to represent their particular gang’s values and norms, attack rival gang members’ reputations and “toughness,” respond to similar affronts to their own reputations or “toughness,” and, as law enforcement has observed, plan, execute, and brag about crimes. See THREAT ASSESSMENT, *supra* note 2, at 41-42; Miller, *supra* note 18, at 7-13.

71. VITO & MAAHS, *supra* note 60, at 159; see also Miller, *supra* note 18, at 9-10 (contending that smartness is “highly valued” among gang members, and that “[t]hose who demonstrate competence in this skill are accorded considerable prestige”). The ideal gang leader will combine both smartness and toughness, but smartness is considered to be more valuable in gang culture, “reflecting a general . . . respect for ‘brains’ in the ‘smartness’ sense.” Miller, *supra* note 18, at 10.

72. See Gutierrez, *supra* note 2; Watkins, *supra* note 2; see also text accompanying note 2.

73. See VITO & MAAHS, *supra* note 60, at 160; Miller, *supra* note 18, at 15 (discussing that adherence to these values is important to maintaining status); *infra* Part III.A.

to be”⁷⁴—a belief that contributes to the impetuous, reactive nature of gang members, and the contagious, retaliatory violence that plagues gangs in American neighborhoods.⁷⁵

B. The Advent of the Internet and the Migration of Gangs Online

With the advent of the Internet, gangs quickly transformed their activities and objectives from the street corner to the computer lab.⁷⁶ Today, gangs are so prevalent on the Internet—engaging in activities such as recruiting, bragging about recent crimes, and even planning criminal activities—that law enforcement has dedicated significant resources toward the online investigation of gangs and gang members.⁷⁷ These tactics are being used by both state and federal law enforcement

74. VITO & MAAHS, *supra* note 60, at 159; Miller, *supra* note 18, at 11-12; *see supra* note 18. Professors Erick Barnes and Robert Homant elaborate on Miller’s “fate” concern through the so-called “Valhalla Effect.” Telephone Interview with Erick Barnes, Professor of Sociology & Criminal Justice, Univ. of Detroit Mercy (Nov. 21, 2012) (on file with *Hofstra Law Review*). The Valhalla Effect, a theory introduced by Professors Barnes and Homant, frames Miller’s concept of fate through the ancient Norse myth of Valhalla—the “hall of the fallen.” *Id.*; *see Valhalla*, 12 THE NEW ENCYCLOPEDIA BRITANNICA 245 (15th ed. 2010). Professors Barnes and Homant note that, like the mythical Norse heroes who died valiantly in battle and were rewarded with a place in Valhalla, gang members’ notions of fate drive their decisions to “go down fighting”—as in the context of “suicide by cop”—with the belief that they, too, will be forever remembered as heroes. *See* Telephone Interview with Erick Barnes, *supra*. For an example of how the fate focal concern can be expressed through social media, *see* Crimesider Staff, *Eric Ramsey, Mich. Rape Suspect, Reportedly Posted He Was “About to Get Shot” Before Being Killed by Police*, CBS NEWS (Jan. 21, 2013, 10:37 AM), http://www.cbsnews.com/8301-504083_162-57564965-504083/eric-ramsey-mich-rape-suspect-reportedly-posted-he-was-about-to-get-shot-before-being-killed-by-police (reporting that a rape suspect utilized his social media account to exhibit his intent to go down fighting by engaging police in a suicidal gun battle—the purest example of the Valhalla Effect).

75. *See* Miller, *supra* note 18, at 11 (discussing how fate is related to excitement, which involves high risk activity including fighting).

76. *See* THREAT ASSESSMENT, *supra* note 2, at 11, 41-42; Gutierrez, *supra* note 2.

77. *See, e.g.,* Van Namen, *supra* note 6, at 565; Emily Gogolak, *Inside the Weird World of Tracking Gang Members Social Media*, ATLANTIC (July 27, 2012), <http://www.theatlanticcities.com/neighborhoods/2012/07/inside-weird-world-tracking-gangs-social-media/2734>; *see also, e.g.,* THREAT ASSESSMENT, *supra* note 2, at 41-42 (attributing recruitment efforts via social media, in part, to a recent increase in gang membership across the United States); Tom Hays, *NYPD Is Watching Facebook to Fight Gang Bloodshed*, NBC NEWS (Oct. 2, 2012, 6:24 PM), <http://www.nbcnews.com/technology/technolog/nypd-watching-facebook-fight-gang-bloodshed-6239746> (“‘Rockstarz up 3-0,’ one suspect boasted – a reference to the body count from a bloody turf war between [two] Brooklyn gangs . . .”).

agencies.⁷⁸ Authorities have even created specific training manuals to instruct agents on how to lawfully obtain information from social media accounts.⁷⁹

Though information and scholarly commentary on this issue is scarce, a recent study compiled specific data on the presence of street gangs on both Facebook and Twitter.⁸⁰ The results, displayed in the tables below, are startling.⁸¹ Each of these accounts may exhibit majorly detrimental gang activities, such as intimidating rival gangs and gang members, planning future gang-crimes, and, of course, recruitment of new members, which ensures the perpetuity of the gang.⁸²

Table 1⁸³

Gang Name	No. of Twitter Profiles	No. of Followers
Bloods	9	47,171
Hells Angels	24	13,411
Latin Kings	22	6823
Mara Salvatrucha (MS-13)	21	3303
Crips	12	3657
Almighty Vice Lord Nation	6	402
Shower Posse	3	155
Indian Posse	2	997
18th Street	1	205
Wah Ching	1	32

78. See, e.g., Hays, *supra* note 77 (noting the increased use of Facebook by the New York Police Department and New York prosecutors to investigate, prosecute, and convict gang members, and the countervailing privacy interests related to such surveillance efforts).

79. See, e.g., Obtaining and Using Evidence, *supra* note 3.

80. See Décary-Héту & Morselli, *supra* note 18, at 878, 880, 882-86.

81. See *id.* at 882-86; *infra* tables 1-2.

82. See Décary-Héту & Morselli, *supra* note 18, at 884-87 & tbls.1-2.

83. *Id.* at 885 & tbl.2.

Table 2⁸⁴

Gang Name	No. of Facebook Pages/Groups	No. of Facebook Fans/Members (2010)	No. of Facebook Fans/Members (2011)
Hells Angels	36	14,775	42,811
Crips	38	4598	5457
Bloods	39	1993	3497
Mara	45	5923	1454
Salvatrucha (MS-13)			
Latin Kings	31	1255	1003
18th Street	5	93	727
Almighty	2	555	527
Vice Lord Nation			
Indian Posse	4	N/A	426
Wah Ching	3	6	100
Shower Posse	3	297	53

As anyone can clearly see from the data, gang prevalence on the Internet and social media is substantial.⁸⁵ What is scarier is the speed with which online gang activities are rising.⁸⁶ This migration of gang presence to the Internet is not without explanation.⁸⁷ Indeed, it makes perfect sense that gangs would want to expand their activities to the Internet.⁸⁸ Gangs are constantly trying to grow their illegal operations, spread their criminality, and, perhaps most importantly, increase their memberships.⁸⁹ Social media networks and the Internet can facilitate these processes more efficiently than traditional methods.⁹⁰

Today, Facebook alone boasts more than one billion users.⁹¹ It has become commonplace for citizens and businesses to create online

84. *Id.* at 883 & tbl.1.

85. *See id.*; *supra* tables 1–2.

86. *See* Décarry-Héty & Morselli, *supra* note 18, at 883. For example, the Hells Angels nearly tripled its Facebook membership in just one year. *Id.*

87. *See infra* text accompanying notes 88–95.

88. *See* Miller, *supra* note 18, at 17 (explaining that gang activity is driven by core gang values); *supra* Part II.A (discussing how the protection of core gang values now requires Internet activity).

89. *See* Miller, *supra* note 18, at 17 (elucidating that the intention of gangs is to commit crimes and that they tend to “recruit from the most ‘able’ members of the community”).

90. *See* THREAT ASSESSMENT, *supra* note 2, at 41–42.

91. Barbara Ortutay, *Facebook Tops 1 Billion Users*, USA TODAY (Oct. 4, 2012, 4:44 PM), <http://www.usatoday.com/story/tech/2012/10/04/facebook-tops-1-billion-users/1612613>.

personas in an effort to express themselves, advertise, or conduct business.⁹² Indeed, nearly every facet of American society is “harnessing the power of social [media] to their advantage,” including normative social groups and commercial enterprises.⁹³ If one views a gang as a business, it is not hard to imagine why gangs and their members (employees) have migrated to social media.⁹⁴ This is particularly so when viewed in light of Miller’s focal concerns.⁹⁵

III. UNREGULATED SOCIAL MEDIA INVESTIGATIONS OF SUSPECTED GANG MEMBERS AND ACQUAINTANCES RISK VIOLATING THE CONSTITUTION’S PARAMOUNT PROTECTIONS OF PRIVACY

*I am a generally law abiding citizen with nothing I can think of that would require monitoring . . . but I wanted to know if I was having data collected about me and if so, what.*⁹⁶

Gang-related speech on social media networks generally falls into one or more of the following types of speech: (1) pure speech, protected by the First Amendment; (2) incitement speech; (3) fighting words; and (4) true threats, the latter three not being entitled to freedom of speech protection.⁹⁷ However, it is not clear whether law enforcement is, perhaps unintentionally, ignoring First Amendment safeguards with respect to pure speech through its data-mining practices, which create “digital dossiers” on suspected gang members based solely on speech that should be free from censorship, prohibition, and punishment.⁹⁸ Here, the data-mining *itself* is punishment.⁹⁹ And the government may not

92. See Van Namen, *supra* note 6, at 551, 555 & n.10.

93. *Id.* at 551-52.

94. Compare *id.* at 551 n.10 (indicating that businesses utilize social media to market and promote themselves in pursuit of commercial success), with THREAT ASSESSMENT, *supra* note 2, at 41-42 (indicating that gangs utilize social media to advertise criminal activity, spread propaganda, and attract new recruits).

95. See VITO & MAAHS, *supra* note 60, at 159; Miller, *supra* note 18 at 7-13; *supra* Part II.A.

96. David Harris-Gershon, *NSA Rejecting Every FOIA Request Made by U.S. Citizens*, DAILY KOS (July 6, 2013, 4:48 PM), <http://www.dailykos.com/story/2013/07/06/1221694/-NSA-Rejecting-Every-FOIA-Request-Made-by-U-S-Citizens#> (internal quotation marks omitted) (quoting a thirty-six-year-old U.S. citizen, Clayton Seymour, pondering what personal information the government was collecting about him).

97. See *infra* Part III.A.

98. See Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1083-88, 1095 (2002) [hereinafter Solove, *Digital Dossiers*] (defining a “digital dossier” as a detailed collection of one’s personal information, which is aggregated, typically unbeknownst to the individual, by private corporations—and often shared with law enforcement—essentially amounting to a “digital biograph[y]”); *infra* Part III.A-C.

99. See Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1934-37 (2003) [hereinafter Richards, *Dangers of Surveillance*] (urging Americans to “recognize that

punish such speech.¹⁰⁰ Even though there is no statute specifically addressing the issue, there is a pressing need for such a statute in order to give guidance to the executive branch and create transparency.¹⁰¹ This will ensure that the First Amendment is not slowly (and secretly) eroding away.¹⁰²

Articulated well over a decade ago, Daniel J. Solove raised concerns over the fact that private companies and other third parties that compile digital dossiers can share citizens' so-called digital biographies with law enforcement; however, we know today that the government compiles digital dossiers of its own accord.¹⁰³ But, we know neither how far such practices reach, nor the details of how such practices are carried out.¹⁰⁴ Notwithstanding the distinct problem of secret government surveillance, the government's independent creation of digital dossiers exacerbates Solove's concerns for many reasons: namely, law enforcement's resources are surely superior to those of third parties, potentially increasing the level of intrusion into law-abiding citizens' private lives, and the government's practice of collecting personal data directly from the source obviates the need to comply with laws designed to regulate government access to information held by third parties.¹⁰⁵

Part III.A will articulate the protections of the freedom of speech that are embedded in the U.S. Constitution, and the various exceptions to those protections.¹⁰⁶ An understanding of these basic concepts is necessary to recognize how and when gang-related speech on the Internet can be punished, and when it should not be.¹⁰⁷ Part III.B will transition from the freedom of speech to the related freedom of association, which is integral to understanding how law enforcement's

surveillance is harmful" for many reasons—namely, its palpable potential to dilute constitutional rights and “chill the exercise of our civil liberties”); *infra* Part IV.A. It is well settled that privacy is one of the most basic and fundamental foundational doctrines of the Constitution and of U.S. citizens' expectations and privileges. See generally DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW (4th ed. 2011) (providing eight chapters of expert commentary on privacy laws, and recognizing that emerging technologies present serious challenges to the significant rights such laws were designed to protect).

100. See U.S. CONST. amend. I; *infra* Part III.A–B.

101. See *infra* Parts III–IV.

102. See *infra* Part IV.

103. See Solove, *Digital Dossiers*, *supra* note 98, at 1088–89 (asserting that “the type of information collection that raises concern involves data gathered from dossiers maintained in private sector entities”); see, e.g., Sottek, *supra* note 4.

104. See, e.g., Watkins, *supra* note 2 (conveying law enforcement's reluctance to discuss gang activity on social media for fear of revealing its investigative techniques).

105. See Solove, *Digital Dossiers*, *supra* note 98, at 1088–89; see also Richards, *Dangers of Surveillance*, *supra* note 99, at 1934–36.

106. See *infra* Part III.A.

107. See *infra* Part III.A.

investigations, data-mining procedures, and subsequent prosecutions too close to the line of violating fundamental rights.¹⁰⁸ It will also discuss why the lack of congressional guidance and oversight is dangerous.¹⁰⁹ Part III.C discusses in detail the investigations of gang members via social media, e-mail, and online avenues.¹¹⁰ While the scholarly literature and law enforcement's disclosures on the topic are scarce,¹¹¹ sufficient data suggests that a large number of gang investigations are conducted using evidence collected from the Internet.¹¹² It is not far-fetched to infer that the scope of the information gathered is often overly broad, or, what is even more troubling, wholly unrelated to a legitimate criminal investigation.¹¹³ This Part clarifies the

108. See *infra* Part III.B.

109. See *infra* Part III.B.

110. See *infra* Part III.C.

111. See Décary-Héту & Morselli, *supra* note 18, at 878, 880; Watkins, *supra* note 2 (noting that “[m]any police agencies are reluctant to discuss the phenomenon” of gangs’ expansion to social media).

112. See Orenstein, *supra* note 13, at 196, 205-06, 212 (observing that social media holds “obvious benefits for police investigations,” and that courts often admit social media evidence to establish gang affiliation); Van Namen, *supra* note 6, at 563-65 (citing several examples of prosecutorial use of social media evidence to reveal associations and affiliations, and to convict gang members); Yu, *supra* note 4 (asserting that “social media has become a mainstay in police work”); see also IACP SURVEY, *supra* note 3, at 1, 3, 11 (reporting that 86.1% of surveyed agencies used social media for criminal investigations, and 66.1% used social media for intelligence purposes).

113. See, e.g., Yu, *supra* note 4 (revealing law enforcement’s monitoring of suspect’s “friends” and “friends of friends,” all of whom had no involvement in the underlying matter); see also Ellen Nakashima, *NSA Gathered Thousands of Americans’ E-mails Before Court Ordered It to Revise Its Tactics*, WASH. POST, Aug. 21, 2013, at A1 (“For several years, the [NSA] unlawfully gathered tens of thousands of e-mails and other electronic communications between Americans as part of a now-revised collection method . . .”); Sottek, *supra* note 4. Sottek criticizes the NSA’s PRISM, which had secretly collected over 200 million Internet communications per year from ISPs, without the ISPs’ informed consent. PRISM, a massive, once-clandestine surveillance and data-mining program, “[c]ollect[ed] [personal information and private content such as photos, e-mails, audio and video messages, and connection logs] directly from the servers of [ISPs]: Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple.” Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST, June 7, 2013, at A1; see also Ben Dreyfuss & Emily Dreyfuss, *What Is the NSA’s PRISM Program? (FAQ)*, CNET (June 7, 2013, 11:44 AM), http://news.cnet.com/8301-1009_3-57588253-83/what-is-the-nsas-prism-program-faq. Despite a recent decision declaring that certain domestic NSA practices of “bulk collection of metadata” violate Fourth Amendment privacy rights, it is disconcerting that the government was permitted to engage in such broad, secretive activities in the first place, intruding on the privacy of thousands of unsuspecting, ordinary Americans without the knowledge of Congress. *Klayman v. Obama*, No. 13-0881, 2013 WL 6598728, at *1-7 (D.D.C. Dec. 16, 2013); Bill Mears & Evan Perez, *Judge: NSA Domestic Phone Data-Mining Unconstitutional*, CNN JUSTICE (Dec. 16, 2013, 8:52 PM), <http://www.cnn.com/2013/12/16/justice/nsa-surveillance-court-ruling>; see also Nakashima, *supra*. The nature of such practices—conducted without the knowledge of Congress, and authorized by a secret court—insulates the government’s behavior from public challenge “because [the] details [are] shrouded in secrecy, denials, and unassessable invocations of national security interests.” Richards, *Dangers of*

problem at hand and demonstrates why the proposed statute resolves the issue, quelling any lingering concerns about constitutional violations.¹¹⁴

A. Freedom of Speech

The First Amendment to the Constitution prohibits Congress from passing any law “abridging the freedom of speech.”¹¹⁵ But there are exceptions.¹¹⁶ Generally, most scholars agree that the courts have carved out six distinct categories of speech that exist outside the ambit of First Amendment protection—therefore, speech that constitutes any of these exceptions can be constitutionally punished or censored by the government.¹¹⁷

First, freedom of speech does not apply to advocacy that “is directed at inciting or producing imminent lawless action and is likely to incite or produce such action.”¹¹⁸ *Brandenburg v. Ohio*¹¹⁹ was a landmark Supreme Court decision concerning a Ku Klux Klan (“KKK” or “Klan”) rally that was filmed by a Cincinnati television reporter at the request of the KKK’s leader, Clarence Brandenburg.¹²⁰ The televised rally depicted Brandenburg in white, hooded Klan garb, using racial epithets and threatening violence if the federal government did not cease “suppress[ing] the white, Caucasian race.”¹²¹ Based on these

Surveillance, *supra* note 99, at 1160-61; see Eric Lane et. al., *Too Big a Canon in the President's Arsenal: Another Look at United States v. Nixon*, 17 GEO. MASON L. REV. 737, 771 (2010); Richards, *Dangers of Surveillance*, *supra* note 99, at 1934, 1948 (“[S]ecret government programs cannot be challenged until they are discovered.”). In sum, the NSA circumvented the doctrine of separation of powers. See U.S. CONST. art. I (vesting “[a]ll legislative Powers . . . in a Congress”); *id.* art. II (vesting “[t]he executive Power . . . in a President”); *id.* art. III (placing “[t]he judicial Power of the United States . . . in one supreme Court, and in such inferior Courts as the Congress may . . . establish”); *Sottek*, *supra* note 4. The same secretive practices, and the same overbroad results, may be underway with respect to federal or state law enforcement’s online gang investigations. See *infra* Part III.C. Likewise, such unregulated collection and storage of personal data from gang investigations could violate the Constitution, as some of the NSA’s conduct has. See *Klayman*, 2013 WL 6598728, at *1; *infra* Part III.C.

114. See *infra* Part III.B–C; *infra* Part IV (presenting the proposed statute).

115. U.S. CONST. amend. I.

116. See, e.g., *Chaplinsky v. New Hampshire*, 315 U.S. 568, 571-72 (1942) (“There are certain well defined and narrowly limited classes of speech, the prevention and punishment of which has never been thought to raise any Constitutional problem.”).

117. See *Virginia v. Black*, 538 U.S. 343, 359 (2003) (holding that true threats are not protected); *Brandenburg v. Ohio*, 395 U.S. 444, 447 (1969) (per curiam) (explaining that speech that is likely to incite “imminent lawless action” is not protected); *Chaplinsky*, 315 U.S. at 572 (finding that prohibited speech includes “the lewd and obscene, the profane, the libelous, and the insulting or ‘fighting words’”).

118. See *Brandenburg*, 395 U.S. at 447.

119. 395 U.S. 444 (1969) (per curiam).

120. *Id.* at 445.

121. *Id.* at 446 & n.1.

documented acts, Brandenburg was convicted of advocating violence under Ohio's Criminal Syndicalism Act,¹²² and the Ohio appellate courts upheld his conviction.¹²³ But the U.S. Supreme Court reversed and overturned Brandenburg's conviction, holding that a state may not punish abstract advocacy of force or law violation "except where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action."¹²⁴ This "incitement test," articulated by the Supreme Court in *Brandenburg*, remains in use to this day, and speech that satisfies it is generally categorized as incitement speech—one of the six major categories of speech that is not protected by the First Amendment.¹²⁵ Indeed, speech that satisfies the *Brandenburg* test may be prohibited without running afoul of the First Amendment.¹²⁶

Second, the Supreme Court has repeatedly held that the U.S. Constitution permits Congress to pass laws that prohibit another type of speech, one that is separate and distinct, yet closely related to

122. OHIO REV. CODE § 2923.13 (1958). The statute made it a crime to "advocate . . . the duty, necessity, or propriety of crime, sabotage, violence, or unlawful methods of terrorism as a means of accomplishing industrial or political reform," or to "voluntarily assemble with any society, group, or assemblage of persons formed to teach or advocate the doctrines of criminal syndicalism." *Id.*

123. *Brandenburg*, 395 U.S. at 444-45.

124. *Id.* at 447-49 & n.4 (reversing Brandenburg's conviction and explaining that all state "[s]tatutes affecting the right of assembly, like those touching on freedom of speech, must observe the established distinctions between mere advocacy and incitement to imminent lawless action," and explaining that punishable speech must be directed at, and likely to result in, imminent lawless action).

125. See KATHLEEN M. SULLIVAN & GERALD GUNTHER, CONSTITUTIONAL LAW 806-10 (17th ed. 2010) (discussing cases that have applied the incitement test following *Brandenburg*); *supra* note 118 and accompanying text. While the modern incitement test owes its conception to the holding in *Brandenburg*, the Supreme Court had articulated essentially the same test nearly half a century earlier, in Justice Oliver Wendell Holmes's progressive dissent in *Abrams v. United States*, 250 U.S. 616 (1919). Justice Holmes opined:

[W]hen words are used exactly, a deed is not done with intent to produce a consequence unless that consequence is the aim of the deed. It may be obvious, and obvious to the actor, that the consequence will follow, and he may be liable for it even if he regrets it, but he does not do the act with intent to produce it unless the aim to produce it is the proximate motive of the specific act, although there may be some deeper motive behind.

Abrams, 250 U.S. at 627 (Holmes, J., dissenting). Holmes further remarked: "It is only the present danger of immediate evil or an intent to bring it about that warrants Congress in setting a limit to the expression of opinion where private rights are not concerned." *Id.* at 628. The "immediate evil" discussed in Holmes's dissent is considered by many to be the source of the "imminence" element of the modern test, elucidated in *Brandenburg*. See *Brandenburg*, 395 U.S. at 444-45; *Abrams*, 250 U.S. at 627; see also, e.g., Steven G. Gey, *A Few Questions About Cross Burning, Intimidation, and Free Speech*, 80 NOTRE DAME L. REV. 1287, 1329-30 (2005).

126. See *Brandenburg*, 395 U.S. at 447.

“incitement speech”—that is, “true threats.”¹²⁷ According to Justice O’Connor, a true threat encompasses:

[T]hose statements where the speaker means to communicate a serious expression of an intent to commit an act of unlawful violence to a particular individual or group of individuals. The speaker need not actually intend to carry out the threat. Rather, a prohibition on true threats “protect[s] individuals from the fear of violence” and “from the disruption that fear engenders,” in addition to protecting people “from the possibility that the threatened violence will occur.” Intimidation in the constitutionally proscribable sense of the word is a type of true threat, where a speaker directs a threat to a person or group of persons with the intent of placing the victim in fear of bodily harm or death.¹²⁸

Thus, a true threat is not necessarily one that the speaker actually intends to carry out, and it may not even be feasible to carry out, but, because it is nevertheless made in a serious manner, and because it is deeply disturbing to society, it may be punished, notwithstanding the First Amendment.¹²⁹ Currently, there is a federal statute in place prohibiting the transmission of communication indicating a threat to injure someone.¹³⁰ Due to the reluctance of law enforcement to fully disclose the nature of its online investigations,¹³¹ it is not clear whether gang members are investigated for violating this or similar statutes.¹³²

127. *Virginia v. Black*, 538 U.S. 343, 359 (2003); *Watts v. United States*, 394 U.S. 705, 707-08 (1969).

128. *Black*, 538 U.S. at 359-60 (second alteration in original) (citations omitted) (quoting *R.A.V. v. St. Paul*, 505 U.S. 377, 388 (1992)).

129. *See id.*

130. 18 U.S.C. § 875(c) (2006) (“Whoever transmits in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another, shall be fined under this title or imprisoned not more than five years, or both.”).

131. *See infra* Part III.C (explaining that the extent of law enforcement’s use of online investigation tools is unknown); *see also* David Harris-Gershon, *NSA Rejecting Every FOIA Request Made by U.S. Citizens*, TIKKUN DAILY (July 6, 2013), <http://www.tikkun.org/tikkundaily/2013/07/06/nsa-rejecting-every-foia-request-made-by-u-s-citizens>.

132. *See, e.g.,* Hays, *supra* note 77 (noting the use of social media to investigate past acts of violence, rather than threats of future violence). However, perhaps law enforcement could (and should) be investigating potential online violations of true-threat statutes in order to prevent actual violence. *See Black*, 538 U.S. at 359; Décarý-Hétu & Morselli, *supra* note 18, at 885-86; Gogolak, *supra* note 77; Gutierrez, *supra* note 2. Online gang speech often includes intimidation and provocation of rival gangs through ridicule and direct insults, which generally fall under the unprotected category of “fighting words,” and, at times, contain “true threats”—specific threats to a specific rival gang member—which society is disturbed to “hear” online. *See* Décarý-Hétu & Morselli, *supra* note 18, at 885-86; Gutierrez, *supra* note 2; Knox, *supra* note 3; *supra* text accompanying notes 118-29. In such instances, the government may be basing investigations solely on violations of these statutes when there is no credible evidence or “probable cause” to believe that other criminality is afoot, as opposed to discovering possible gang affiliation and subsequently gathering information on an unidentified subject and his family, friends, and acquaintances. *See* Yu,

Another type of speech that the government can prohibit and punish is speech that courts refer to as “fighting words.”¹³³ The Supreme Court has defined fighting words as “those personally abusive epithets which, when addressed directly and in person to the ordinary citizen, are, as a matter of common knowledge, inherently likely to provoke violent reaction.”¹³⁴ According to the Supreme Court, such speech can be prohibited and punished by the government because fighting words “by their very utterance inflict injury or tend to incite an immediate breach of the peace.”¹³⁵ In order for speech to be characterized as “fighting words,” and therefore outside the ambit of freedom of speech protection, the speech must be “directed to the person of the hearer.”¹³⁶ Furthermore, statutes prohibiting such speech must be “narrowly drawn to define and punish *specific* conduct as constituting a clear and present danger to a *substantial* interest of the State.”¹³⁷

Violations of these types of statutes must “raise such clear and present menace to public peace and order” as to constitutionally permit punishment.¹³⁸ And, like other freedom of speech exceptions, these prohibitory statutes “may not unduly suppress free communication of views, religious or other, under the guise of conserving desirable conditions.”¹³⁹ It is therefore clear that the freedom of speech is a fundamental right that mandates strict safeguards against legislation that censors or punishes speech.¹⁴⁰ The fighting words exception is yet another example of the limited (and somewhat extreme) circumstances in which speech can be prohibited, notwithstanding constitutional protections.¹⁴¹

In order for a state to punish citizens for fighting words, the applicable statute must be narrow and specific, and can prohibit only the most egregious violations—those that are likely to elicit drastic and disturbing consequences, such as a violent response from the hearer.¹⁴² But, unlike other types of freedom of speech exceptions, the hearer must

supra note 4; Knox, *supra* note 3; *infra* Part III.C.

133. Cohen v. California, 403 U.S. 15, 20 (1971) (internal quotation marks omitted).

134. *Id.*

135. See Chaplinsky v. New Hampshire, 315 U.S. 568, 572 (1942).

136. Cantwell v. Connecticut, 310 U.S. 296, 309 (1940).

137. *Id.* at 311 (emphasis added).

138. *Id.*

139. *Id.* at 308. Perhaps “other” views could include notions of gang sympathy or indications of gang affiliation, association, or even full-fledged membership. See, e.g., Knox, *supra* note 3 (explaining that users of Facebook join groups online that espouse the views of gangs).

140. See Knox, *supra* note 3.

141. See Cohen v. California, 403 U.S. 15, 20 (1971); Chaplinsky v. New Hampshire, 315 U.S. 568, 572 (1942); Cantwell, 310 U.S. at 309-10.

142. See Cantwell, 310 U.S. at 311.

also be the subject of the “abusive” speech.¹⁴³ For example, if a member of the Crips street gang posted a Facebook message generally insulting the Bloods street gang, it would likely fall outside the scope of the fighting words exception and could not be punished.¹⁴⁴ This insult would not be directed towards a specific hearer, and so arguably would not be “in person” due to its online nature.¹⁴⁵

There might, however, be specific circumstances where a gang insult made on a social media network could be considered fighting words. For example, a Crip member (“C”) could privately send a message directly to a Blood member (“B”), disrespecting B and the Bloods, and communicating in such an abusive nature that an ordinary citizen would reasonably consider it inherently likely to elicit a violent reaction.¹⁴⁶ While the speech in this hypothetical is written, not oral, the “instant” nature of the message, and the evolution of social speech since the advent of the Internet, might satisfy the in-person element of the fighting words exception, as outlined by *Chaplinsky v. New Hampshire*.¹⁴⁷

Thus, such gang-related fighting words might be likely to incite “an immediate breach of the peace,”¹⁴⁸ as B in the hypothetical would receive that message immediately after C sent it, and it was intended to insult B, the hearer. Due to the focal concerns of toughness, autonomy, and trouble,¹⁴⁹ B might immediately respond to C with a similarly violent, threatening message, and might possibly begin to plan an in-

143. *Id.* at 309-10.

144. See *Cohen*, 403 U.S. at 16, 20 (finding that the phrase “Fuck the Draft” on defendant’s jacket, worn inside of a courthouse, was not a personal insult directed to any particular person “*actually or likely to be present*,” and thus did not constitute fighting words (emphasis added) (internal quotation marks omitted)); *Cantwell*, 310 U.S. at 302-03, 311 (overturning defendants’ convictions for breaching the peace for playing a phonograph record insulting the Catholic religion in front of two Catholic men).

145. See, e.g., *Cohen*, 403 U.S. at 16, 20.

146. See Gutierrez, *supra* note 2. It is not immediately clear how a court would interpret “ordinary citizen” in such a situation. It might be prudent for a court to apply an “ordinary gang member” standard when analyzing the nature of the speech and its likelihood of inciting an immediate violent response, due to the inherently different nature of gang members’ “focal concerns,” particularly “toughness,” “trouble,” and “autonomy.” See VITO & MAAHS, *supra* note 60, at 159; Miller, *supra* note 18, at 7-13; *supra* Part II.A. But, perhaps the courts could apply the traditional “ordinary citizen” standard and reach the same result; the gang-related insult might not lead an ordinary citizen (that is, a non gang-member) to react violently, but the insulting Facebook message might also contain traditional insults or abusive epithets that would alone be inherently likely to elicit a violent reaction from an ordinary citizen. See *Cohen*, 403 U.S. at 20.

147. 315 U.S. 568, 571-74 (1942); see *supra* Part II.A.

148. *Chaplinsky*, 315 U.S. at 572.

149. See VITO & MAAHS, *supra* note 60, at 159; Miller, *supra* note 18, at 7-13; *supra* Part II.A.

person attack on C, C's friends and family, or other members of the Crips.¹⁵⁰

However, there is a lack of regulation for the use of this type of speech.¹⁵¹ The type of gang-member-to-gang-member interaction described in this hypothetical is likely outside the scope of this Note. The example merely illustrates the possibility of constitutionally permissible statutory prohibitions (and related punishments) regarding gang speech online. For the purposes of this Note, however, such speech is just one of many types that social media users and non-users can report to the network's administrator, who then evaluates it and may discretionarily bring it to the attention of law enforcement.¹⁵²

Law enforcement may, upon inspection of such speech, whether obtained through investigating a public post (with no warrant or subpoena required) or a private message (obtained under statutory authority, usually requiring a warrant or subpoena), begin a file on the suspected gang members based on the gang-related speech.¹⁵³ And, as outlined below, law enforcement will also begin investigating the lives of that suspected gang member's family and friends, and friends of *those* friends, resulting in large numbers of digital dossiers on unwitting and innocent social media users.¹⁵⁴ It is conceivable that law enforcement's investigations and digital dossiers will lead to offline investigations to gather personal data, such as subscriber information, addresses, and billing information—and, potentially, in-person surveillance operations, as well.¹⁵⁵ These investigations are themselves unwarranted punishments,¹⁵⁶ therefore, they should be carefully and narrowly tailored, rather than arbitrary and overbroad.¹⁵⁷

B. Freedom of Association

In addition to the freedom of speech, the First Amendment implicitly provides for the so-called freedom of association, which grants citizens the right to freely come together with other individuals and collectively express, promote, pursue, and defend common

150. See *supra* Part II.A; *supra* notes 2, 43-44 and accompanying text.

151. See, e.g., Knox, *supra* note 3 (discussing how Facebook does not prohibit gang threat activity).

152. See *supra* notes 7-11 and accompanying text.

153. See Stored Communications Act, 18 U.S.C. §§ 2701-2711 (2006); *infra* Part III.C.

154. See Yu, *supra* note 4 (quoting a Cincinnati police lieutenant who stated that the police department was "looking [on social media networks] at friends and friends of friends of the suspects"); see also *infra* Part III.C.

155. See 18 U.S.C. § 2709 (2006); see also Obtaining and Using Evidence, *supra* note 3.

156. See *infra* Part IV.

157. See *Cohen v. California*, 403 U.S. 15, 20 (1971); *supra* Part III.A.

interests.¹⁵⁸ It is well settled that a person's First Amendment right to freedom of speech generally extends to speech conducted on the Internet.¹⁵⁹ Therefore, since the freedom of association is an unenumerated First Amendment right, it, too, deserves protection in the social media setting.¹⁶⁰

But, there are also exceptions to the freedom of association. Certain laws prohibit membership in certain groups, but these narrow situations generally apply only to groups advocating for the toppling of the U.S. government.¹⁶¹ Still, even for statutes relating to something as extreme as an attempted coup,¹⁶² the government, according to the Supreme Court, must prove an individual's specific intent to further an organization's subversive goals in order to punish them for simply being a member.¹⁶³ Generally, the case law on this topic focuses on situations in which the entire nation's security is at risk, and typically involves statutes relating to treason, attempts to overthrow the government, and terrorism.¹⁶⁴

For example, 18 U.S.C. § 2339B—Providing Material Support or Resources to Designated Foreign Terrorist Organizations (“Material Support Statute”)¹⁶⁵—only applies to officially designated Foreign Terrorist Organizations (“FTOs,” singularly “FTO”)—a designation that excludes traditional street gangs.¹⁶⁶ However, the doctrine underlying the Material Support Statute exhibits an important principle; that is, when the government attempts to punish individuals for merely being a member of a group, such punishment is highly regulated, strictly scrutinized, and often requires proof of additional intent or acts that

158. See U.S. CONST. amend. I; *NAACP v. Alabama*, 357 U.S. 449, 461 (1958) (“In the domain of these indispensable liberties, whether of speech, press, or association, the decisions of this Court recognize that abridgement of such rights, even though unintended, may inevitably follow . . .”); see also JEREMY MCBRIDE, *FREEDOM OF ASSOCIATION: THE ESSENTIALS OF HUMAN RIGHTS* 18 (2005).

159. See, e.g., *Reno v. ACLU*, 521 U.S. 844, 870 (1997).

160. See *id.*; *NAACP*, 357 U.S. at 461.

161. See, e.g., 18 U.S.C. § 2385 (1952 & Supp. V 1958) (prohibiting organization of a group that advocates the overthrow of the government).

162. See, e.g., *id.*

163. *Scales v. United States*, 367 U.S. 203, 229-30 (1961).

164. See, e.g., 18 U.S.C. § 2339B (2006) (prohibiting the provision of material support to a foreign terrorist organization); 18 U.S.C. § 2385.

165. 18 U.S.C. § 2339B.

166. See *id.*; BUREAU OF COUNTERTERRORISM, U.S. DEP'T OF STATE, *FOREIGN TERRORIST ORGANIZATIONS* (2012) [hereinafter *FOREIGN TERRORIST ORGANIZATIONS*], available at <http://www.state.gov/j/ct/rls/other/des/123085.htm> (explaining that the term FTO includes sophisticated and politically-oriented terrorist organizations, such as al-Qaida and Hezbollah, and excludes typical domestic street gangs, such as the Crips and the Bloods).

amount to more than merely displaying one's sympathies or affiliations for a group.¹⁶⁷

The Material Support Statute illustrates that, even where national security is at risk on a much larger scale than that posed by street gangs and gang members, an individual is technically not punished for being merely a member of the group, affiliating with the group, or having sympathies for the group.¹⁶⁸ Rather, they can only be punished if they provide "material support" to the group¹⁶⁹—a group that, it bears repeating, is a highly sophisticated and dedicated FTO aimed at total destruction of the U.S. government and the effective annihilation of the American people.¹⁷⁰ At the same time, recent case law has held that an individual may still be held liable, even if such support is intended to be used for non-violent humanitarian causes.¹⁷¹

Still, this First Amendment right does not apply when there are countervailing interests that strongly outweigh the individual's right to freely associate—such as the state's interest in protecting the community or maintaining order.¹⁷² Individual states have passed laws prohibiting the loitering and comingling of gang members on public streets, despite freedom of association implications.¹⁷³ However, judges and lawmakers have been careful to note the rare and extreme circumstances that allow state courts and legislatures to deprive even gang members of the fundamental rights to speak and associate freely when the countervailing interest extremely outweighs the gang members' interest in exercising

167. See, e.g., *Scales*, 367 U.S. at 229-30.

168. See 18 U.S.C. § 2339B.

169. *Id.*

170. See, e.g., FOREIGN TERRORIST ORGANIZATIONS, *supra* note 166.

171. See, e.g., *Humanitarian Law Project v. Reno*, 205 F.3d 1130, 1135-36 (9th Cir. 2000) (upholding the Material Support Statute in lieu of a freedom of association challenge, holding that the contributor is punished for furnishing goods and services that can be used to support a FTO's terrorist activities, not for expressing of the ideas of the supported group).

172. See, e.g., *People ex rel. Gallo v. Acuna*, 929 P.2d 596, 601-02 (Cal. 1997) (upholding an injunction against a state statute that prohibited gang members from being in view of one another on the street or engaging in otherwise legal activities); Ed Bond, *Freedom of Association—For Gangs?*, L.A. TIMES, Feb. 11, 1997, at B1.

173. See, e.g., *Chicago v. Morales*, 527 U.S. 41, 45-46, 51-53 (1999) (holding city ordinance that prohibited criminal street gang members from loitering with one another in a public place invalid because it was impermissibly vague, but recognizing the state's interest in combatting gang activity and noting that the statute did not violate the First Amendment, but rather abridged the liberty guaranteed by the Due Process Clause); Bond, *supra* note 172 (discussing the California Supreme Court's validation of the police and prosecutor practice of serving orders on gang members prohibiting them from standing on rooftops, carrying pagers, or being in view of one another on the street because of the communities' interest in security).

those rights.¹⁷⁴ And, even under such dire circumstances, not all judges agree that the deprivation of such fundamental rights is warranted.¹⁷⁵

Thus, the freedom of association, though not specifically enumerated in the Constitution, carries serious weight when balancing the interests of the individual with those of the government.¹⁷⁶ The association right may prevail, even when the government's countervailing interest involves ensuring its continued existence.¹⁷⁷ But, while simply being a member is not technically punishable, individuals are prohibited from providing certain types of material support that are often interpreted quite broadly to encompass even non-violent activities; still, mere association with, or sympathy for, an FTO is not prohibited by the state action.¹⁷⁸

It is unsettling, then, that local and state law enforcement may infringe on these very same rights when cavalierly investigating suspected gang members, and—more significantly—their families and friends.¹⁷⁹ Infringement of these rights occurs when a citizen's privacy is invaded by the government's data-mining and compiling of digital dossiers without probable cause.¹⁸⁰ Some may argue that much of the information law enforcement gathers is “public” in nature—and available to any normal citizen—thereby failing to trigger constitutional protections.¹⁸¹ However, this Note asserts that: (1) the government often

174. See, e.g., *Acuna*, 929 P.2d at 620 (Kennard, J., concurring in part, dissenting in part). Justice Joyce L. Kennard noted the following declaration of the California legislature in restricting gang activity:

“California is in a state of *crisis* which has been caused by violent street gangs whose members threaten, terrorize, and commit a multitude of crimes against the peaceful citizens of their neighborhoods.” These activities, both individually and collectively, present a *clear and present danger to public order and safety and are not constitutionally protected.*

Id. (emphases added) (quoting CAL. PENAL CODE § 186.21 (1999)).

175. See, e.g., *id.* at 623 (Mosk, J., dissenting). Justice Stanley Mosk stated that:

No doubt Montesquieu, Locke, and Madison will turn over in their graves when they learn they are cited in an opinion that does not enhance liberty but deprives a number of simple rights to a group of Latino youths who have not been convicted of a crime [under California's Street Terrorism Enforcement and Protection Act].

Id.

176. See *NAACP v. Alabama*, 357 U.S. 449, 461-62 (1958).

177. See *Humanitarian Law Project v. Reno*, 205 F.3d 1130, 1137 (9th Cir. 2000). It bears repeating that a citizen is permitted to associate with, and even be a member of, an FTO in light of the freedom of association, but that punishment is reserved solely for providing material support to the FTO. See 18 U.S.C. § 2339B (2006); *supra* notes 165-71 and accompanying text.

178. See *supra* notes 168-71 and accompanying text.

179. See *Knox*, *supra* note 3; *Yu*, *supra* note 4.

180. See *infra* Parts III.C–IV.

181. See *infra* Part IV. When a person's reasonable privacy expectations are not infringed, constitutional protections, such as those extending from the Fourth Amendment, are not triggered. See, e.g., *Katz v. United States*, 389 U.S. 347, 351 (1967) (“What a person knowingly exposes to

obtains non-public information—for example, through national security demand letters (“NSLs”), and Electronic Communications Privacy Act (“ECPA”)¹⁸² and Stored Communications Act (“SCA”)¹⁸³ requests—without establishing probable cause;¹⁸⁴ and (2) a normal citizen who compiles another citizen’s public information (such as posts and pictures) is wholly different from governmental collection of the same information—which will be stored in digital dossiers and law enforcement databases, may potentially resurface at any time, and can be used against the citizen in a prosecution.¹⁸⁵

C. Law Enforcement Investigations

Nothing was your own except the few cubic centimeters inside your skull.

– George Orwell, *Nineteen Eighty-Four*¹⁸⁶

This Subpart will first discuss the procedures and policies of federal and state investigations of online gang activity.¹⁸⁷ Next, it will discuss a bill that, if enacted, will permit private entities to share personal information collected from the Internet with government intelligence agencies.¹⁸⁸ Finally, this Subpart will summarize the methods of data-collection that law enforcement utilize when investigating gang activity online, then discuss the risks to individuals’ rights that surround such practices.¹⁸⁹

the public, even in his own home or office, is not a subject of Fourth Amendment protection.”); see also *Guest v. Leis*, 255 F.3d 325, 333 (6th Cir. 2001) (“Users would logically lack a legitimate expectation of privacy in materials intended for publication or public posting.”); *Van Namen*, *supra* note 6, at 558-59 (“If the user chooses not to alter his or her default security settings on social media, the profile remains open to the public, available for all to view; and a prosecutor could access the information without infringing on a person’s privacy expectations.”). Public information is freely discoverable, and certain social media posts, such as tweets, “may be . . . easily used by prosecutors” where courts interpret them as “part of the public record.” See *Van Namen*, *supra* note 6, at 562-63. But see *Katz*, 389 U.S. at 351 (“[W]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.” (emphasis added)).

182. Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C. (2006)).

183. 18 U.S.C. §§ 2701–2712 (2006 & Supp. II 2002).

184. See David Kravets, *Google Tells Cops to Get Warrants for User E-Mail, Cloud Data*, WIRED (Jan. 23, 2013, 5:29 PM), <http://www.wired.com/threatlevel/2013/01/google-says-get-a-warrant/?cid=5468824>; *infra* Part IV.

185. See *infra* Part IV.

186. ORWELL, *supra* note 17, at 28.

187. See *infra* Part III.C.1–2.

188. See *infra* Part III.C.3.

189. See *infra* Part III.C.4.

1. Federal Investigations

There are no federal regulations currently in place to ensure uniform reporting policies among the various social media outlets.¹⁹⁰ It appears that, despite the view that gangs ought to be eradicated from social media for fear of inciting violence and recruiting new members, the lack of reporting policies on certain websites allows gang activity to remain online unfettered, leaving the accompanying evidence just waiting to be gathered, analyzed, and stored by law enforcement.¹⁹¹ Thus, it may be in law enforcement's interest to allow online gang activity, to facilitate the gathering of intelligence on gang members—and, potentially, their families, friends, and friends of friends.¹⁹²

According to a U.S. Department of Justice (“DoJ”) training manual,¹⁹³ which was released pursuant to a Freedom of Information Act¹⁹⁴ request,¹⁹⁵ law enforcement is statutorily granted the authority to obtain incriminating evidence of gang crimes and individuals' gang affiliations through undercover operations or traditional search warrants.¹⁹⁶ Specifically, the ECPA provides the framework for government seizure of electronic data.¹⁹⁷ Federal agencies, such as the Federal Bureau of Investigation (“FBI”), may request from ISPs, through NSLs, users' subscriber information, including the “name, address, and length of service,” as well as “local and long distance toll billing records.”¹⁹⁸

Additionally, the government can obtain the Internet records of American citizens without evidence of gang affiliation, or any criminal activity, for that matter.¹⁹⁹ Former NSA contractor, Edward Snowden, revealed that the NSA, for years, has been collecting Americans' online data to be subsequently mined, analyzed, and stored.²⁰⁰ While this Note does not suggest that every law enforcement agency is operating on a level of this magnitude, a parallel can be drawn between the NSA's

190. See Knox, *supra* note 3; *supra* notes 8-11 and accompanying text.

191. See Knox, *supra* note 3.

192. See *id.*; Yu, *supra* note 4.

193. Obtaining and Using Evidence, *supra* note 3.

194. 5 U.S.C. § 552 (2006).

195. See Obtaining and Using Evidence, *supra* note 3.

196. See *id.* (noting that MySpace requires a search warrant for private messages or bulletins less than 181 days old).

197. See 18 U.S.C. §§ 2701–2711.

198. *Id.* § 2709.

199. See Sottek, *supra* note 4 (noting that NSA collection practices may gather incidental data that belong to American citizens with no connection to terrorism); see also Obtaining and Using Evidence, *supra* note 3.

200. See, e.g., Nakashima, *supra* note 113; Sottek, *supra* note 4.

recently revealed data-mining practices and law enforcement's everyday online gang investigations.²⁰¹

A presentation by the DoJ outlined several investigative methods for collecting information from social media outlets.²⁰² These methods include: (1) undercover operations; (2) subpoenas; and (3) search warrants, when they are required.²⁰³ A fourth method identified by this DoJ presentation is obtaining special court orders pursuant to § 2703(d) of the SCA.²⁰⁴ Section 2703(d) "does not require agents to obtain a warrant if they are seeking communications that are not in 'electronic storage' with the provider of an 'electronic communication service' or if they are seeking communications that remain in storage for more than 180 days."²⁰⁵ Instead, the SCA requires only that government agents present "specific and articulable facts" demonstrating "reasonable grounds to believe" that the information they seek is merely "relevant and material to an ongoing criminal investigation."²⁰⁶ Additionally, subpoenas—which are sufficient to demand electronic records stored for more than 180 days—are issued beyond the bounds of meaningful judicial review, and generally require a showing of mere relevancy—a lesser hurdle than the stringent probable cause standard.²⁰⁷ Typically, a neutral judge does not approve—or even review—the government's showing that Internet evidence is relevant when granting a subpoena.²⁰⁸ Indeed, "[t]rial subpoenas are typically issued by a clerk of court (or in some cases, an attorney); grand jury subpoenas are typically issued by the clerk of court on behalf of the grand jury; and administrative subpoenas are issued by administrative agencies with appropriate statutory authority."²⁰⁹ None of these methods involve judicial review.²¹⁰

201. See *infra* Part IV.

202. See Obtaining and Using Evidence, *supra* note 3.

203. See *id.* (indicating that search warrants are required when the information sought from a social media outlet, such as MySpace, constitutes "private messages/bulletins less than 181 days old").

204. 18 U.S.C. §§ 2701–2712 (2006 & Supp. II 2002); Obtaining and Using Evidence, *supra* note 3.

205. Bellia & Freiwald, *supra* note 4, at 127.

206. See 18 U.S.C. § 2703(d); Bellia & Freiwald, *supra* note 4, at 127–28 (explaining that the standard for obtaining such court orders is lower than the Fourth Amendment's probable cause standard, which law enforcement traditionally must meet—to the satisfaction of a neutral and detached magistrate—before it can constitutionally seize a citizen's information for later use in court).

207. Bellia & Freiwald, *supra* note 4, at 127–28.

208. *Id.* at 128 (citing William J. Stuntz, *O.J. Simpson, Bill Clinton, and the Transsubstantive Fourth Amendment*, 114 HARV. L. REV. 842, 864 (2001) (equating subpoenas to a "blank check")).

209. *Id.* at 128 n.28.

210. See *id.*

For years, the NSA's actions were carried out in secret, absent any congressional authorization or judicial oversight, save, perhaps, by the secretive court created by the Foreign Intelligence Surveillance Act of 1978 ("FISA").²¹¹ Today, the breadth and depth of law enforcement's gang investigations are similarly surreptitious.²¹² As such, it is impossible to determine whether or not they are uncovering too much irrelevant (yet, private) information.²¹³ A citizen might innocently post a photograph wearing gang-suggestive clothing, or otherwise express sympathy for a particular gang or group.²¹⁴ Although this thought-expression might be entirely benign, perhaps even made in jest, the current lack of government oversight and internal agency regulations permits in-depth, intrusive investigation of that citizen's entire online activity.²¹⁵ This surveillance could even lead to an investigation of that citizen's family, friends, and friends of friends.²¹⁶ This unwarranted invasion of privacy amounts to the punishment of speech—that is, punishment for what may be characterized as thoughtcrime—which may have detrimental, chilling effects on the freedom of expression.²¹⁷

Disclosures from one free e-mail provider suggest that there are large numbers of law enforcement investigations and data-mining activities in general (that is, not specifically related to gang crime), with the majority of the information requested leading to a search warrant that is neither based on probable cause, nor information that is legally relevant to an ongoing investigation.²¹⁸ David Kravets stated:

The data Google is coughing up to the authorities includes e-mail and text-messaging communications, cloud-stored documents and, among other things, browsing activity, and even [Internet Protocol] addresses used to create an account.

In all, agencies across the United States demanded 8,438 times that Google fork over data on some 14,791 accounts for the six-month period ending December 2012. Probable-cause search warrants were

211. 50 U.S.C. §§ 1801–1885 (2006); *see, e.g.*, Nakashima, *supra* note 113; Sottek, *supra* note 4.

212. *See* Décary-Héту & Morselli, *supra* note 18, at 880 (noting that there have been reports of police monitoring social media, but law enforcement denies extensive use); Watkins, *supra* note 2 (explaining that police are reluctant to talk about gang activity on social media because they do not wish to reveal their investigative techniques); *infra* Part IV.

213. *See infra* Part IV.

214. *See, e.g.*, *People v. Liceaga*, No. 280726, 2009 WL 186229, at *3 (Mich. Ct. App. Jan. 27, 2009); Gutierrez, *supra* note 2.

215. *See, e.g.*, Yu, *supra* note 4; *infra* Part IV.

216. *See, e.g.*, Yu, *supra* note 4.

217. *See* ORWELL, *supra* note 17, at 29 (“Thoughtcrime does not entail death: thoughtcrime IS death.”).

218. Kravets, *supra* note 184.

issued in 1,896 of the cases. Subpoenas, which require the government to assert that the data is relevant to an investigation, were issued 5,784 times. Google could not quantify the remaining 758.²¹⁹

What is further troubling is that this data might only represent the tip of the iceberg. The NSA, for example, has collected over 250 million Internet communications per year, as of 2011.²²⁰ Further, many of law enforcement's data-collection practices are kept secret from the public—and from the other branches of government, as well.²²¹ In fact, at least one e-mail providers' top executives were allegedly threatened with incarceration if they revealed the U.S. government's data-collection practices.²²² Kravets reported that:

Google's transparency data is *limited* as it does not include requests under the Patriot Act, which can include National Security Letters with gag orders attached. Nor do the data include anti-terrorism eavesdropping court orders known as FISA orders or any dragnet surveillance programs legalized in 2008, as those are secret, too. In all those instances, probable-cause warrants generally are not required, even for customer content stored in Google's server.²²³

Thus, there is clear potential for constitutional violations when the federal government investigates gangs online.²²⁴ Investigations by state law agencies fare no better with respect to well settled privacy protections.²²⁵

2. State Investigations

State investigations must comply with state law, as well as federal law, as a state may only provide its citizens with protections that are greater than or equal to those provided by federal law.²²⁶ Therefore, federal law sets out the minimum of citizens' rights.²²⁷ But, the delineation of these rights is not always clear, and, unfortunately, courts have provided little guidance as to the admissibility of evidence obtained

219. *Id.*

220. Sottek, *supra* note 4.

221. *Id.*; see Nakashima, *supra* note 113.

222. Dominic Rushe, *Zuckerberg: U.S. Government 'Blew It' on NSA Surveillance*, GUARDIAN (Sept. 11, 2013, 8:18 PM), <http://www.theguardian.com/technology/2013/sep/11/yahoo-ceo-mayer-jail-nsa-surveillance>.

223. Kravets, *supra* note 184 (emphasis added).

224. *See infra* Part IV.A.

225. *See infra* Part III.C.2.

226. U.S. CONST. art. VI, cl. 2.

227. *See id.*; see also KAMISAR ET AL., *supra* note 37, at 25.

via online investigations—and this lack of guidance applies not only to gang investigations, but to other criminal (and civil) actions.²²⁸

Data garnered from “social media sites presents a unique challenge for [defendants] as well as the government, because information is often maintained by third-party providers, and there is developing law that treats certain information stored on social media websites as ‘private’ and subject to [ECPA].”²²⁹ For example, in *Hubbard v. MySpace, Inc.*,²³⁰ the court held that a search warrant served by state authorities on MySpace to turn over account information, including the Internet protocol address, the inbox contents, and sent e-mail, was sufficient to satisfy the requirements of the SCA.²³¹ However, a California federal court, in *Crispin v. Christian Audigier, Inc.*,²³² while acknowledging the privacy settings of the user, quashed subpoenas seeking private messages on Facebook and MySpace as being protected under the Stored Communications Act.²³³

3. Sharing Private Online Information with the Government Through CISA

On February 12, 2013, President Barack Obama released an executive order regarding Internet privacy, data-collection, and cybersecurity.²³⁴ The purpose of President Obama’s executive order was to “strengthen the cybersecurity of critical infrastructure by increasing information sharing and by jointly developing and implementing a framework of cybersecurity practices with our industry partners.”²³⁵ The executive order was released, in part, in response to repeated cyber intrusions of federal government agencies.²³⁶ Clearly, the cybersecurity of the nation’s critical infrastructure is of the utmost importance to the nation’s security, and, ultimately, its continued survival.²³⁷ But, the

228. Murphy & Esworth, *supra* note 14, at 34.

229. *Id.*

230. 788 F. Supp. 2d 319 (S.D.N.Y. 2011).

231. 18 U.S.C. §§ 2701–2712 (2006 & Supp. II 2002); *Crispin*, 788 F. Supp. 2d at 321, 324–25.

232. 717 F. Supp. 2d 965 (C.D. Cal. 2010).

233. *Id.* at 991. It is important to note that, “[u]nder this developing law, a civil subpoena would not be sufficient, or for that matter, appropriate to obtain ‘private’ information such as e-mails or instant message communications stored on a social media website or a private web-based e-mail account.” Murphy & Esworth, *supra* note 14, at 34.

234. Improving Critical Infrastructure Cybersecurity, Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 19, 2013).

235. Press Release, White House, Office of the Press Sec’y, Executive Order on Improving Critical Infrastructure Cybersecurity (Feb. 12, 2013), <http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity-0>.

236. *See id.*

237. *See* Improving Critical Infrastructure Cybersecurity, Exec. Order No. 13,636, 78 Fed.

possible consequences of this executive order could further infringe upon the privacy rights of American citizens; one such consequence is the recent re-introduction, in Congress, of the Cyber Intelligence Sharing and Protection Act of 2011 ("CISPA").²³⁸

A version of CISPA was previously introduced in Congress in late 2011.²³⁹ Despite strong opposition from privacy-rights advocates and a promise by President Obama to veto it, should it pass, the bill passed the House of Representatives, though it ultimately died in the Senate—much to the delight of civil rights groups and Internet-privacy think tanks.²⁴⁰ The new CISPA, introduced a day after President Obama's executive order, is nearly identical to the original CISPA.²⁴¹

The stated purpose of the bill is "[t]o provide for the sharing of certain cyber threat intelligence and cyber threat information between the intelligence community and cybersecurity entities, and for other purposes."²⁴² This proposed bill will eliminate the liability of—that is, insulate from criminal prosecution or civil suit—any business that shares customer or employee information with intelligence agencies.²⁴³ This

Reg. at 11,739.

238. H.R. 3523, 112th Cong.; see Tony Romm, *Rebirth of CISPA—But 'Concerns Haven't Gone Away*, POLITICO (Feb. 15, 2013, 4:39 AM), <http://www.politico.com/story/2013/02/rebirth-of-cispa-but-concerns-havent-gone-away-87690.html> (implying that the re-introduction of CISPA was a logical consequence of President Obama's executive order). But see Michelle Richardson, *President Obama Shows No CISPA-Like Invasion of Privacy Needed to Defend Critical Infrastructure*, ACLU (Feb. 13, 2013, 1:48 PM), <http://www.aclu.org/blog/national-security-technology-and-liberty/president-obama-shows-no-cispa-invasion-privacy-needed> (emphasizing that President Obama's executive order did not specifically endorse CISPA—or even mention it—thus suggesting that the re-introduction of CISPA was not a consequence intended by the executive order).

239. See Josh Levy, *Meet the New CISPA. Same as the Old CISPA*, COMMON DREAMS (Feb. 18, 2013), <https://www.commondreams.org/view/2013/02/18-5> (warning that "[t]he 'new' version [of CISPA] is in fact identical to the original CISPA," which stalled in the Senate in 2012); Michelle Richardson, *CISPA Claws Back to Life*, ACLU (Feb. 10, 2013, 1:54 PM), <http://www.aclu.org/blog/technology-and-liberty-national-security/cispa-claws-back-life> [hereinafter Richardson, *CISPA*] (referring to the new version of CISPA as an "encore appearance"). Representatives Mike Rogers and Dutch Ruppersberger co-sponsored the original version of the bill. See Romm, *supra* note 238. Their work on the bill was part of a collaborative effort to "help the federal government and private sector share data in real time and better defend against crippling cyberattacks." *Id.*

240. Romm, *supra* note 238; Matthew J. Schwartz, *CISPA Passes House: What's Next?*, INFO. WEEK (Apr. 27, 2012, 12:36 PM), <http://www.informationweek.co.uk/government/policy/cispa-passes-house-whats-next/232901107>.

241. See Romm, *supra* note 238 (quoting Representative Adam Schiff as stating that, "[t]he text [of the newly proposed CISPA] is largely the same as last year, and the concerns haven't gone away" (internal quotation marks omitted)). Compare Cyber Intelligence Sharing and Protection Act, H.R. 624, 113th Cong. (Apr. 15, 2013), with Improving Critical Infrastructure Cybersecurity, 78 Fed. Reg. at 11,739.

242. H.R. 624 pmb1.

243. *Id.* § 2(a) (declaring that, absent bad faith, "[n]o civil or criminal cause of action shall lie

information includes employees' and customers' Internet usage, social media activity, and e-mail content.²⁴⁴ Likewise, intelligence agencies are allowed to collect data from businesses as needed "to protect the national security of the United States."²⁴⁵

As with the previous version of CISA, and, like most of the laws on Internet privacy and data-collection, the new CISA is vague.²⁴⁶ It lacks explicit language and does not guarantee that personally identifying information will be redacted before private companies pass along the data to the government.²⁴⁷ Furthermore, it permits the government to use the information shared with it for any lawful purpose, assuming it: (1) is not used for a regulatory purpose; and (2) is used for at least one lawful purpose that is related to (a) cybersecurity or (b) "protect[ion] [of] the national security of the United States."²⁴⁸ These ambiguities in the statutory language, like the lack of oversight of law enforcement's gang investigations on social media, are dangerous.²⁴⁹ It is not difficult to imagine the possible intrusions of constitutionally protected privacy rights—specifically, the rights to keep one's personal thoughts and information private, and to freely speak and associate.²⁵⁰

A suspected gang member, whose social media account was brought to police attention solely through a network administrator, who had previously instituted his internal investigation based upon a user's report of abuse to the network—a report that could have been based solely on an unreliable, unauthentic post or photograph—might also be subject to the sharing of his data between the government and private

or be maintained in Federal or State court against a protected entity, self-protected entity, cybersecurity provider, or an officer, employee, or agent of a protected entity, self protected entity, or cybersecurity provider" for sharing information, using a cybersecurity system, or not acting on such information received or obtained); *see also* Matthew J. Schwartz, *CISA Cybersecurity Bill, Reborn: 6 Key Facts*, INFO. WEEK (Feb. 14, 2013, 1:24 PM), <http://www.informationweek.com/security/cybercrime/cispa-cybersecurity-bill-reborn-6-key-fa/240148600> [hereinafter Schwartz, *Key Facts*].

244. See H.R. 624 § 2(a); Schwartz, *Key Facts*, *supra* note 243.

245. H.R. 624 § 2(a).

246. See *id.* For example, the stated purpose of the bill is to encourage and facilitate more efficient communication of cyber threat information between government agencies and between private sector entities and the government, but also includes the nebulous phrase "and for other purposes." *Id.*

247. See *id.* § 2 (requiring only that information be shared in accordance with restrictions provided by the very entity sharing the information).

248. *Id.* The quoted text has been the subject of much criticism, and could be interpreted to fit nearly any type of online investigation, of many types of suspected criminals—including gang members. Richardson, *CISA*, *supra* note 239 (criticizing the language, "to protect the national security of the United States," as being "undefined and incredibly expansive" (internal quotation marks omitted)).

249. See *infra* Part IV.

250. See *supra* Part III.A–B; *infra* Part IV.

cybersecurity entities under CISA.²⁵¹ In fact, the government could even share this individual's private Internet data with other countries.²⁵² Due to CISA's vagueness, the extent of the information to be shared, and whether such information is stored, kept, or destroyed, is unclear.²⁵³ The government is not opposed to sharing American citizens' online information with other governments,²⁵⁴ and, due to CISA's liability exemption clause, a suspected gang member (or, more significantly, his innocent family, friends, and acquaintances) would have no available legal redress for the resulting privacy intrusions, false prosecutions, or the stigmatizing effects of the public embarrassment stemming from such government conduct.²⁵⁵

4. Putting It All Together

Thus, under current law, a suspected gang member—known only to law enforcement through his social media network and related online persona,²⁵⁶ who was brought to police attention coincidentally, and where the only incriminating evidence is a photograph indicating possible gang affiliation from his social media account—can be easily identified through a NSL, the use of which has greatly expanded since the enactment of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("USA PATRIOT Act").²⁵⁷ It is not hard to imagine that the disclosed subscriber information can easily be used to obtain more personal, intimate information²⁵⁸—even information about family members and friends, which could subsequently be shared with private

251. See Schwartz, *Key Facts*, *supra* note 243; *supra* Part III.A.

252. Glenn Greenwald et al., *NSA Shares Raw Intelligence Including Americans' Data with Israel*, *GUARDIAN* (Sept. 11, 2013, 10:40 AM), <http://www.theguardian.com/world/2013/sep/11/nsa-americans-personal-data-israel-documents>.

253. See *supra* notes 246-47 and accompanying text.

254. See Greenwald et al., *supra* note 252.

255. See Cyber Intelligence Sharing and Protection Act, H.R. 624, 113th Cong. § 2 (2013).

256. See Ortutay, *supra* note 91.

257. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56 (Oct. 12, 2001) (codified as amended in scattered sections of the U.S. Code); see *National Security Letters*, ACLU (Jan. 10, 2011), <http://www.aclu.org/national-security-technology-and-liberty/national-security-letters> (cautioning that, subsequent to the enactment of the USA PATRIOT Act, law enforcement can "compile vast dossiers about innocent people and obtain sensitive information such as the web sites a person visits, a list of e-mail addresses with which a person has corresponded, or even unmask the identity of a person who has posted anonymous speech on a political website").

258. See Van Namen, *supra* note 6, at 563-64; see also IACP SURVEY, *supra* note 3; Obtaining and Using Evidence, *supra* note 3.

companies providing cybersecurity to critical infrastructure, if CISPA becomes enacted law.²⁵⁹

While such tactics are helpful for investigating and preventing gang crime, and for the apprehension of gang members for specific crimes, little is known about how often NSLs are issued for information on suspected gang members who have not been linked to a specific crime.²⁶⁰ More importantly, little is known about the scope of law enforcement investigations of gang members and their families, friends, and acquaintances.²⁶¹ There is no positive law authorizing such investigations, limiting the scope and breadth of information to be obtained, or providing procedures for the destruction of the collected private information once an investigation is extinguished.²⁶² Without such a statute, it is difficult for the judiciary to review this ongoing conduct.²⁶³ Thus, the potential for violations of the freedoms of speech and association in this arena is great, as is the risk of chilling these rights.²⁶⁴ The government can still violate the freedoms of speech and association, even if it is not violating a specific statute, as the breach of a statute is not required for government actions to violate the Constitution.²⁶⁵

IV. CLEARING THE PATH: CONGRESSIONAL DIRECTION IS NEEDED TO PROHIBIT ARBITRARY DATA-COLLECTION

There is a lack of transparency with respect to law enforcement's gang investigations that exploit social media networks.²⁶⁶ It is easy to imagine information being compiled into digital dossiers on suspected gang members for which the only probable cause is a photo or post suggesting gang sympathies or affiliations, and the only "crime" being suspected membership in a gang.²⁶⁷ It is similarly easy to imagine that this information could one day be shared with other government agencies, private companies, and even other countries.²⁶⁸

259. See H.R. 624 § 2; Yu, *supra* note 4.

260. See *National Security Letters*, *supra* note 257.

261. See *supra* note 212 and accompanying text.

262. See Murphy & Esworth, *supra* note 14, at 35-36 (discussing the Fourth Amendment as the only limit on law enforcement's investigations of electronically stored information).

263. See *supra* note 113 and accompanying text.

264. See *supra* Part III.A-B; *infra* Part IV.

265. See Nakashima, *supra* note 113 (explaining that a NSA surveillance program was unconstitutional despite having been authorized by Congress).

266. See *supra* Part III.C.

267. See *supra* Part III.C.

268. See *supra* Part III.C.3.

This data-collection is a form of punishment in and of itself, when it is conducted without a proper warrant based on credible probable cause.²⁶⁹ Even in the rare instance that a warrant is issued, such issuance may often be based upon probable cause that is, in reality, nothing more than an unauthenticated social media post or photograph.²⁷⁰ While there is not a statute directly on point that law enforcement must either comply with or violate through its practices, this Note argues that government data-mining practices themselves may essentially constitute a violation of the freedom of speech, freedom of association, or both—not to mention the chilling effects such practices may have on these freedoms.²⁷¹

Inherent in these First Amendment rights, and protections embedded in other Amendments, is the unenumerated right to privacy.²⁷²

269. See *infra* Part IV.A.

270. See *People v. Beckley*, 110 Cal. Rptr. 3d 362, 366-67 (Ct. App. 2010) (holding that the trial court erred in admitting evidence of the defendant flashing a gang symbol on her MySpace page because, “with the advent of computer software programs such as Adobe Photoshop ‘it does not always take skill, experience, or even cognizance to alter a digital photo’” (quoting Parry, *supra* note 13, at 183)). It is not hard to imagine someone hacking into a law-abiding citizen’s social media account and posting potentially incriminating pictures related to gangs and gang crime, or, perhaps, creating a fake account about a real person, and posting gang related posts. See e.g., *id.* More commonly, though, is the scenario in which an ordinary citizen posts something that appears, either intentionally or not, to demonstrate a gang affiliation or full-fledged membership (for example, a wayward youth, though not a gang member or a criminal, posts a self-portrait in a blue bandana, displaying a hand signal in the shape of a “C”—the universal indicators of Crip gang membership). See *id.* at 365-66. Whether or not this person is an actual gang member would be difficult to verify simply from this social media evidence. Orenstein, *supra* note 13, at 207. When addressing evidence gathered online:

Courts generally address four types of authentication concerns: (1) general lack of proper foundation; (2) the possibility that the entire social networking page is a fake; (3) the possibility that a genuine existing page has been hacked; and (4) the possibility that someone has appropriated the site of another by obtaining the password through friendship, phishing, or a computer left logged on and unattended in a place where third parties could post in the owner’s name.

Id. (footnotes omitted). While these concerns regard the admissibility of evidence at trial, this Note argues that these issues can be problematic as early as the investigation stage. See *infra* Part IV.A. The privacy of unknowing and innocent citizens is violated in these situations, and there is no oversight by independent, aboveboard agencies; it is not known where this collected information goes once an investigation based on a social media “tip” is deemed meritless—or whether such investigations are halted once the person is no longer deemed a suspect. See *supra* Part III.C. Still, the government can investigate this person (to an unspecified extent), as well as their friends and friends of those friends, for evidence of criminality. Yu, *supra* note 4. But, there is nothing criminal about solely being a gang member, so evidence of such alone is deficient probable cause, and, the investigation and dossier-compiling is punishment because it invades privacy—social media administrators are handing over to law enforcement private information without warrants at an alarming rate, because the public information is still different when it is collected by the government and the consequences can be much more severe. See *infra* Part IV.A.

271. See *infra* Part IV.A.

272. See *Griswold v. Connecticut*, 381 U.S. 479, 482-86 (1965) (discussing the constitutionally

Justice Louis Brandeis succinctly summarized the principles underlying the Constitution's unenumerated privacy rights, in his dissenting opinion in *Olmstead v. United States*,²⁷³ a case that has since been criticized and essentially overturned by the landmark case, *Katz v. United States*.²⁷⁴ The Court in *Olmstead* explained:

The protection guaranteed by the [Fourth and Fifth] Amendments is much broader in scope. The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men.²⁷⁵

Through the Due Process Clause of the Fourteenth Amendment,²⁷⁶ the implicit rights to privacy found in the Fourth and Fifth Amendments have been interpreted as also extending to state citizens.²⁷⁷ These rights are deemed incorporated into the Fourteenth Amendment, and, as such, must not be invaded by state action—for example, state and local police investigations—without due process of law.²⁷⁸ Therefore, these

protected zone of privacy created by the penumbral rights of the First, Third, Fourth, and Fifth Amendments); SOLOVE & SCHWARTZ, *supra* note 99, at 941–43 (discussing privacy challenges to NSLs based on the First and Fourth Amendments); *see also* U.S. CONST. amends. I, III, IV, V. One could also argue that the right to privacy is additionally implied by the Sixth Amendment's right to counsel provision, because that right, which attaches as soon as formal judicial proceedings have begun, prevents law enforcement from deliberately eliciting incriminating information from a suspect without an attorney present, absent a knowing, valid, and intelligent waiver of this constitutional protection. *See* U.S. CONST. amend. VI, cl. 4; *Massiah v. United States*, 377 U.S. 201, 206 (1964).

273. 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

274. 389 U.S. 347, 353 (1967).

275. *Olmstead*, 277 U.S. at 478.

276. U.S. CONST. amend. XIV, § 1.

277. *See Griswold*, 381 U.S. at 481–86 (holding that the right to privacy in the Bill of Rights invalidated a state statute under the Due Process Clause). The Seventh Amendment has been held not to apply to the states. *Minneapolis & St. Louis R.R. v. Bombolis*, 241 U.S. 211, 217 (1916). The Supreme Court has not yet determined whether the Third Amendment is incorporated into the Fourteenth Amendment (and, therefore, applicable to the states); however, the Second Circuit has held that it does apply to state citizens. *Engblom v. Carey*, 677 F.2d 957, 961 (2d Cir. 1982).

278. *See Griswold*, 381 U.S. at 486–88 (1965) (Goldberg, J., concurring) (noting that the concept of liberty in the Due Process Clause incorporates guarantees in the Bill of Rights that contain “fundamental” personal rights); *see also* U.S. CONST. amend. XIV, § 1 (“[N]or shall any State deprive any person of life, liberty, or property, without due process of law” (emphasis added)).

protections should be extended to state citizens so that they can enjoy the appropriate protections and safeguards.²⁷⁹

It is important to note that, while some of the mined information may include public posts and photos on social media networks, network administrators and ISPs can disclose more intrusive, truly private information, seemingly without a warrant or a subpoena.²⁸⁰ The triggering evidence (that is, the tip) in these instances might be public speech, but the end result is that personal subscriber information (and the contents of private e-mails and messages) are mined, analyzed, recorded, and stored in law enforcement offices and digital systems throughout the United States.²⁸¹ This is especially troubling because the investigation of a suspected gang member can further lead to the investigation of the suspect's friends, families, and—more concerning—friends of friends; all people who likely have no reason to suspect that they are targets of government surveillance.²⁸² Allowing law enforcement to surreptitiously monitor and collect the detailed personal data of innocent and unsuspecting citizens creates a perilous slope that could transform Orwellian science fiction into a dreadful reality.²⁸³ Indeed, such unjustified, unregulated, and undisclosed data-collection practices could serve as precursors to a shift towards a totalitarian government, not unlike the one harrowingly depicted by Orwell in *Nineteen Eighty-Four*, but the government's present impetus is the dilution of privacy rights that once provided the bedrock for our Constitution and cultural identity.²⁸⁴

Additionally, law enforcement's intrusive practices²⁸⁵ are, from a policy standpoint, contrary to both American jurisprudence and society's

279. See *Griswold*, 381 U.S. at 481-86 (majority opinion).

280. See *National Security Letters*, *supra* note 257; see also Obtaining and Using Evidence, *supra* note 3.

281. See *Knox*, *supra* note 3; see also Obtaining and Using Evidence, *supra* note 3.

282. See *Kravets*, *supra* note 184 (explaining that Google requires probable cause warrants to hand over the content of users' e-mails, but will hand over non-content portions of e-mail, such as the "from," "to," and "date" fields without probable cause); *Yu*, *supra* note 4 (revealing that local police departments watch social media websites at suspected gang members' "friends and friends of friends" (emphasis added) (internal quotation marks omitted)).

283. *Richards, Dangers of Surveillance*, *supra* note 99, at 1934, 1948; Neil M. Richards, Essay, *The Information Privacy Law Project*, 94 GEO. L.J. 1087, 1132-33 (2006) [hereinafter *Richards, Privacy Project*] (suggesting that, although it does not capture all of the nuances of real-world surveillance, the Orwell metaphor retains some validity as a tool to understand electronic surveillance).

284. See *ORWELL*, *supra* note 17, at 28; see, e.g., Raymond Shih Ray Ku, *The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance*, 86 MINN. L. REV. 1325, 1327-45 (2002); *Richards, Dangers of Surveillance*, *supra* note 99, at 1937, 1949-56; *Richards, Privacy Project*, *supra* note 283, at 1132-33.

285. See *supra* Part III.C; see also *ORWELL*, *supra* note 17, at 28.

expectation of a free state.²⁸⁶ The need for regulation in this area is great, as is explained in more detail in Subpart A.²⁸⁷ Accordingly, Subpart B proposes a federal statute designed to quell these serious concerns, while still facilitating necessary online investigations of gang crime—thereby balancing the protection of fundamental constitutional rights with the national interest in keeping communities safe.²⁸⁸

A. Tottering on the Edge of Unconstitutionality

There are certainly situations satisfying the “imminent lawless action” prong of *Brandenburg* which would permit the government to use online speech to conduct intrusive investigations of suspected gang members, collect data, and, if warranted, subsequently prosecute suspects.²⁸⁹ Law enforcement’s use of social media to investigate crime, where there is probable cause to believe a crime has been or will be committed, must be permitted to effectively police and protect the community.²⁹⁰ The same is true for prosecutors’ use of social media to gather incriminating evidence against suspects for whom they are seeking indictments, or who have already been charged with a crime.²⁹¹

However, it is clear that these are not the only situations in which law enforcement and prosecutors are using social media to obtain intelligence.²⁹² It is not inconceivable that many of the pictures, posts, and messages collected by law enforcement also implicate non-suspects.²⁹³ Based on the suspicion of a criminal act, law enforcement entities may be compiling digital dossiers on countless social media users as authorized by the ECPA and the expanded scope of NSLs under

286. See Declan McCullagh, *Opposition Grows to CISPA ‘Big Brother’ Cybersecurity Bill*, CNET (Apr. 23, 2012, 4:31 PM), http://news.cnet.com/8301-31921_3-57419540-281/opposition-grows-to-cispa-big-brother-cybersecurity-bill (comparing CISP to an ultra-intrusive surveillance government, and suggesting that CISP abridges constitutionally guaranteed freedoms).

287. See *infra* Part IV.A.

288. See *infra* Part IV.B.

289. *Brandenburg v. Ohio*, 395 U.S. 444, 447 (per curiam) (1969); see, e.g., Watkins, *supra* note 2 (describing a case in which gang members used Twitter to call a rival gang member a “snitch,” and planned a retaliatory attack for his alleged testimony, though police were able to use online investigations to arrest three gang members).

290. See *id.* (discussing how gang investigations on social media help law enforcement to crackdown on gangs involved in hate crimes).

291. See Van Namen, *supra* note 6, at 563-65.

292. See, e.g., Yu, *supra* note 4 (discussing the use of social media to investigate friends of gang members not suspected of a particular crime); see also, e.g., Watkins, *supra* note 2 (discussing the use of social media to identify gang associates and learn about their organizations, and stating that law enforcement can “find out about people you never would have known about before” (internal quotation marks omitted)).

293. See, e.g., Watkins, *supra* note 2; Yu, *supra* note 4.

the USA PATRIOT Act.²⁹⁴ It is more troubling that these law enforcement entities may be compiling digital dossiers based on the mere suspicion that the target has an affiliation or association with a gang—no matter how tenuous—or simply because the target harbors sympathy for a particular gang or its values.²⁹⁵

While some speech on social media networks is certainly public in nature, such as status posts or self-posted photographs (assuming that the account-holder who posts is the actual person behind the computer screen), the traditional freedom of speech exceptions cannot be fairly applied to online speech.²⁹⁶ In the days of *Brandenburg*, if the police were made aware of a type of speech that might fall outside the ambit of First Amendment protection, they would likely conduct an investigation to determine whether a crime was being committed.²⁹⁷ In situations where the First Amendment did apply, and the speech could not be punished, the investigation would end; the patrolmen would merely stand by while the speech continued, or choose to leave the scene and respond to other calls for assistance.²⁹⁸

But, the above scenario is something wholly different from gang-member speech made via social media. Today, when the police are made aware of potential gang-speech online, they investigate—just as police did in the days of *Brandenburg*.²⁹⁹ However, contemporary investigations may include gathering the most intimate details about the potential suspect, and details about his family, friends, and friends of friends, including public information, such as photographs, lists of hobbies, or even a timeline covering years of that person's activities—and “private” information, obtained through the ECPA, the SCA, undercover operations, and, perhaps soon, the CISPA, including information such as addresses, billing information, bank records, phone records, private message content, e-mail information, private online

294. See *supra* Part III. Here, the term “suspicion” represents a lesser standard than probable cause, as investigations may begin merely upon the reporting of the activity by a third-party citizen. See BLACK’S LAW DICTIONARY, *supra* note 55, at 599, 736 (defining “probable cause” and “suspicion”); Van Namen, *supra* note 6, at 552-53. In other cases, this “suspicion” could be characterized as an even lesser standard of proof when a person may have committed a crime, or may be an associate of a particular gang (that is, “a police hunch”). See Watkins, *supra* note 2.

295. See Watkins, *supra* note 2.

296. See *supra* Part III.

297. See, e.g., *Feiner v. New York*, 340 U.S. 315, 316-17 (1951).

298. See, e.g., *id.* at 317 (noting that, initially, patrolmen “made no effort to interfere with [defendant]’s speech, but were first concerned with the effect of the crowd on both pedestrian and vehicular traffic,” implying that if defendant’s speech had not reached the requisite level of incitement—presenting a clear and present danger—the police would not have intervened and arrested him).

299. See *supra* Part III.C.

journals, and so forth.³⁰⁰ Rather than investigating, deciding whether the speech remains protected by the First Amendment, and then moving on, the police can virtually enter the minds of these alleged gang members, and invade the privacy of their innocent friends and friends of friends.³⁰¹

This is clearly relevant information, and a goldmine for law enforcement when they discover actual gang members (and their associations), when they are actually committing gang crimes—charges can be brought, crimes can be prevented, and lives can be saved.³⁰² But, what is not clear is what law enforcement is doing for those situations where the gang speech is not, in fact, criminal—when it does not fall within one of the highly regulated exceptions to the First Amendment³⁰³ and must not be subject to punishment or censorship.³⁰⁴ Where is the information stored and for how long?³⁰⁵ More importantly, for how long do the investigations continue, and at what point, if any, are they abandoned—for instance, should it become clear that the tip regarding the gang speech was frivolous, or the conduct did not amount to a crime?³⁰⁶ Finally, does the investigation of a person's entire life (including non-public information), which is based solely upon purported evidence of gang membership, come dangerously close to violating the freedom of association?³⁰⁷ If it is not a crime to be a gang member, why should evidence of mere affiliation (and not actual criminality) be grounds for a criminal investigation?³⁰⁸ This is particularly relevant when such investigations, due to the nature of society and social media generally, can uncover intimate details of that person's life—and the lives of his friends and friends of friends—which can be stored by police without statutory regulations or limitations, in accordance with any number of different department-specific policies.³⁰⁹

300. See, e.g., Van Namen, *supra* note 6, at 564-65; Obtaining and Using Evidence, *supra* note 3; *supra* Part III.C.

301. See Van Namen, *supra* note 6, at 564 (explaining that users of social media publically post what they feel and think on the public forum); *supra* Part III.C.

302. See *supra* note 12 and accompanying text.

303. See *supra* Part III.C. That is to say, when the speech is not a "true threat," "inciting speech," or "fighting words." See *supra* Part III.A.

304. See U.S. CONST. amend. I; *supra* Part III.A.

305. See *supra* note 221 and accompanying text.

306. See *supra* Part III.A.

307. See *supra* Part III.B.

308. See *supra* Part III.C.

309. See *supra* Part III.C.

*B. Protecting the Constitution While Investigating Gang Crime:
A Proposed Statute to Balance the Interests*

To quell these serious and legitimate concerns, Congress must act. This action should come in the form of statutes or other regulations that require uniform reporting procedures for investigations of social media accounts that would still allow evidence of gang-related crimes to be reported to ISPs by ordinary citizens.³¹⁰ The ISPs would then be directed to follow internal procedures and potentially notify law enforcement if the evidence of a crime is credible; but, the ISPs' internal policies must be clear—a statute can ensure that there is clarity and a degree of uniformity across the internal procedures of various social media outlets.³¹¹

Because of the lack of regulation of these practices, and the inherent potential for constitutional violations, this Note proposes a statute that grants law enforcement positive authority to collect data from social media if there is probable cause to believe that a crime has occurred, or that there is a reasonable probability of imminent lawless action; data-collection based solely on a user's mere affiliation or association with a gang is prohibited by the statute, with other such limitations and parameters as Congress sees fit.³¹² State legislatures should model their own state statutes after the federal law, choosing to add any additional protections for its citizens as they, in turn, see fit.³¹³ Additionally, state attorney generals might choose to issue executive orders directing agencies to promulgate policies, rules, and regulations outlining the collection and storage of suspected gang members' information obtained through social media tips.³¹⁴ Those regulations should be as uniform as is feasibly possible.

The proposed federal statute—or executive order—which state legislatures should adopt completely or with modifications in compliance with the Supremacy Clause,³¹⁵ follows this general model:

Social media network administrators and Internet Service Providers shall collaborate and establish uniform reporting procedures with respect to reporting suspected criminality, and include a simple channel to indicate specifically the possible indication of gang crime on the Internet. Such policies should also include specific criteria, uniform across all networks, for evaluating alleged gang criminality

310. See *infra* text accompanying notes 312-13; cf. *supra* notes 7-11 and accompanying text.

311. See *infra* text accompanying notes 312-13; cf. *supra* notes 7-11 and accompanying text.

312. See *supra* Part III.C.

313. See *supra* notes 226-27 and accompanying text.

314. Cf. *supra* notes 226-28 and accompanying text.

315. See U.S. CONST. art. VI, cl. 2; *supra* notes 226-27 and accompanying text.

for credibility and authenticity, in making the determination whether to report such accounts to law enforcement.

The purpose of this is requirement to prevent frivolous and meritless investigations of unsuspecting, innocent citizens and their families, as well as to preserve police resources, allowing for a more effective use of police time, energy, and capital. Such policies should be particularly specific when addressing reports of abuse merely indicating an association or affiliation with a particular gang, and shall include provisions for evaluators to use common-sense when deciding whether to bring the user's account to the attention of law enforcement.

Furthermore, law enforcement agencies shall establish similar procedures and disclose them to the public, and to an independent oversight committee. Additionally, law enforcement agencies that investigate criminals (and suspected gang members) via social media shall be required to publish annual reports on the statistics of such investigations, without jeopardizing active investigations; as such, all personal identifying information shall be redacted from these reports, which shall include:

(1) detailed figures regarding the reports of abuse (i.e., tips) from social media administrators, which led to:

- (a) convictions;
- (b) arrests; and
- (c) dismissals;
- (d) leads to evidence of unrelated crimes and their subsequent:
 - (i) convictions;
 - (ii) arrests and;
 - (iii) dismissals,

including the nature of the suspected/charged/convicted crime listed above;

(2) the number and nature of such investigations which resulted in no arrests at all, and the extent of information collected;

(3) details regarding how such information was obtained, gathered, and stored; and

(4) whether it has since been destroyed and if so, the details of such destruction.

No law enforcement agency shall collect and store information on a citizen indicating merely an affiliation with, association with, or sympathy for a particular group or gang, whether criminal or not, unless it has been determined by clear and convincing evidence that such person is providing material support for this group, the evidence reveals sufficient probable cause (to be determined by a neutral and detached magistrate) that a crime has been committed or is likely to be committed, or such evidence is likely to produce imminent lawless action or fall within any other of the few, narrowly defined types of

speech falling outside the ambit of First Amendment protection, as promulgated by this Congress and the Supreme Court.

Courts would likely interpret this as comporting with the freedom of association, and the statute should be upheld if challenged.³¹⁶ Furthermore, the statute would create transparency and oversight and help prevent constitutional violations, and would start the discussion about how to best handle the issues discussed in this Note, by first requiring disclosure.³¹⁷ At the same time, legitimate national security efforts will remain unhindered, and authorities will still be able to utilize social media to investigate crimes under the statute.³¹⁸ Requiring disclosure and annual reports will help Congress best modify, amend, or even repeal this statute in the future, depending on its results.³¹⁹

But, without such transparency and regulation, the public will be deprived of the right to freely associate, and there is a real risk that law enforcement will slowly increase the scope of its data-collection from gang-affiliates to their families, friends, and friends of friends, compiling personal information for “intelligence” along the way.³²⁰ These regulations would ensure that this does not occur, while, at the same time, afford law enforcement each of the tools necessary to prevent and solve gang crimes.³²¹ Without such a statute, law enforcement could compile digital dossiers on social media users based on nothing more than their affiliations with, or sympathies for, certain subcultures—creating a slippery slope that could potentially lead to the inherently un-American dystopia predicted in *Nineteen Eighty-Four*.³²²

V. CONCLUSION

The lack of laws regulating online gang investigations is a problem of monumental magnitude.³²³ While it is clearly in the government’s interest to actively pursue criminals by any means possible, gang members pose a potentially problematic paradigm.³²⁴ There is a legitimate risk of Orwellian surveillance with respect to these data-

316. Cf. *supra* Part III.B.

317. Cf. *supra* Part IV.A.

318. Cf. *supra* Part III.C.

319. Cf. *supra* note 113.

320. See, e.g., IACP SURVEY, *supra* note 3; Obtaining and Using Evidence, *supra* note 3; see also Yu, *supra* note 4; *supra* Part IV.A.

321. See *supra* note 154 and accompanying text; *supra* text accompanying notes 315-16.

322. See generally ORWELL, *supra* note 17 (depicting a dystopian future under an oppressive totalitarian government); *supra* Part IV.A.

323. See *supra* Part III.

324. See *supra* Parts II–III.

collection procedures, and while law enforcement practices must be afforded a degree of discretion, they should not be given free reign to scour social media for any connection or affiliation with any group or association, whether criminal or otherwise.³²⁵ Social media reporting procedures ought to be uniform, as well; such uniformity will allow vigilant citizens to effectively report evidence of gang crime to authorities and social media networks.³²⁶

Like the lack of regulation, there is also a lack of scholarly authority in the field.³²⁷ As the social media era treads on, and courts increasingly deal with these issues, more scholarly attention is warranted. This Note does not, in any way, condone gang crime or gang membership; neither does this Note suggest that law enforcement is purposely, or certainly, violating the Constitution. But, the risk of such violations in the future is great, and the individuals' rights involved are even greater.³²⁸

*James R. O'Connor**

325. See *supra* Part IV.A.

326. See *supra* Part IV.B.

327. See *supra* Parts II–III.

328. See *supra* Parts III–IV. “[F]or our system of governance to perform effectively, the legislature and the citizenry must receive sufficient information regarding the actions, policies, and intentions of government officials. The absence of sufficient information undermines accountability, impedes rational decision making, and lays a foundation for misconduct, corruption, and waste.” Lane et al., *supra* note 113, at 771. There is a current lack of sufficient information about the government’s gang-related electronic surveillance programs, but it is clear that they can harm gang members and ordinary citizens alike. See *supra* Parts III–IV. When we ignore this ignorance—and blindly accept secretive practices as beyond constitutional bounds—we “fail[] to protect [our] privacy rights, and permit[] their gradual decay,” while we silently encourage the government to “determine for itself the scope of its own powers.” Ku, *supra* note 284, at 1327.

* J.D. Candidate, 2014, Hofstra University School of Law; B.S., 2010, University of Detroit Mercy. The effort put forth to publish this Note is dedicated to my grandmother, Ann Conway O’Connor, and my grandfather, Charles Breidenstein. I would foremost like to thank my mother, Theresa O’Connor, for her unconditional love over the years (and for teaching me how to read), and my father, Robert O’Connor, for his endless support and encouragement (and for teaching me how to write). I am also indebted to Professor Robin Charlow for her tutelage and guidance throughout this lengthy writing process; Professors Michael J. Witkowski, Erick Barnes, and Thomas Kolpacki for their inspiration and direction; and the entire *Hofstra Law Review* team, especially Brian Sullivan, Sarah Freeman, Megan Law, Erik Harmon, Jonathan Nasca, and Tyler Evans. Finally, I would like to express my gratitude to my siblings, Ann, Jonathan, Kyle, and Kerry, for being the best; thanks for always sticking by my side and never giving up on me.