PROTECTING VIOLENT FREE SPEECH AND COMBATTING TRUE HOMICIDAL THREATS IN CYBERSPACE

Aimee N. Lillie

Helms School of Government 2022 Conference

Liberty University

March 24, 2022

Introduction

Recent phenomena like the global COVID-19 pandemic and evolving trends toward the increasing digitization of everyday and criminal activities have created unique and unprecedented challenges for the United States criminal justice system. Experts have argued that the internet has transformed criminal behavior by changing the landscape of risks and opportunities, citing creative and rapidly escalating uses of digital technology in crimes like homicide, sexual assault, mass murder, and cannibalism.[1] These changes in risks and vulnerabilities have accelerated since 2019 due to widespread stay-at-home orders and quarantine mandates that have forced individuals and organizations to transition toward conducting many activities of daily life and business in digital environments with little to no guidance about how to navigate this transition safely. Despite predictions that crime rates would fall due to decreased social contacts resulting from stay-at-home orders and business closures, many United States cities have reported substantial increases in major crimes like homicides, aggravated assaults, and gun assaults.[2] Perhaps even more concerning research indicates that international and domestic terrorists are effectively using digital technology to exploit the chaos and uncertainty caused by the pandemic in numerous nefarious ways including fomenting civil rebellion and challenging trust in government agencies.[3]

One particularly effective tactic used by domestic terrorists during the pandemic involves the inflammation and exploitation of citizen fears of tyranny in the form of mass surveillance and violations of their rights to free speech and privacy.[4] The transition to conducting daily life in cyberspace that was precipitated by the pandemic has contributed to a blurring of boundaries between public and private, forcing criminal justice professionals to think critically about how to balance the oft conflicting goals of safeguarding free speech while protecting citizens from threats like domestic terrorism and stranger-perpetrated homicide. The Supreme Court has thus far declined to provide adequate guidance about the types of online threat speech that are not constitutionally protected, and the guidance that the Court has communicated about standards of reasonableness and intent is murky at best.[5] This lack of clear guidance is problematic because research

---

[1] M.C.A. Liem and M.E.F. Geelen, "The Interface Between Homicide and the Internet," *Aggression and Violent Behavior* 48 (2019): 65.
[2] Ernesto Lopez and Richard Rosenfeld, "Crime, Quarantine, and the U.S. Coronavirus Pandemic," *Criminology & Public Policy* 20 (2021): 401-403.
[3] Arie W. Kruglanski et al., "Terrorism in Time of the Pandemic: Exploiting Mayhem," *Global Security: Health, Science and Policy* 5, no. 1 (2020): 121-122.
[4] Ibid., 123.
[5] Alison J. Best, "Elonis v. United States: The Need to Uphold Individual Rights to Free Speech While Protecting Victims of Online True Threats," *Maryland Law Review* 75, no. 4 (2016): 1128.

supports the claim that many violent crimes like stranger-related homicides, mass killings, and domestic terror attacks could be disrupted and even prevented if internet communications in domains like social media platforms were employed more effectively as tools for intelligence gathering and threat assessment.[6] It is clear that criminal justice professionals and researchers at multiple levels of government will need to collaborate to clarify free speech guidance and bolster safeguards, to pursue a more complete understanding about the role of digital communications in violent crime, and to improve tactical threat assessment and response capabilities.[7]

Misconstrual of Privacy in Cyberspace

The issue of privacy in online communications is complex in part because the intuitions, expectations, beliefs, and felt experiences of users often conflict with legal realities. Online spaces like social media platforms typically feel to users as though they are private, in part because users often access these platforms from physically private locations like home offices, bedrooms, and even bathrooms; yet legal precedent dictates that social media spaces are equivalent to public spaces.[8] In its 2017 *Packingham v. North Carolina* ruling, the Supreme Court equated the internet to a public square, stating that only minimal restrictions should be imposed on public use, and acknowledging that social media play a vital role in many aspects of contemporary life.[9] While the designation of social media as public spaces seems straightforward from a purely legal standpoint, there is substantial concern that broadly defining the internet as a public forum creates unanticipated opportunities for exploitation of information that citizens intend and make efforts to protect as private.[10] These concerns are grounded in the notion that the internet is a qualitatively different type of space from physical public or private realms; therefore, it requires a different legal and ethical approach to privacy that accounts for the different types and quantities of personal data that exist in cyberspace.[11]

Some researchers contend that the use of social media intelligence as a policing tool is tantamount to deliberately exploiting public ignorance because people who erroneously believe that they can selectively protect their online communications or create private nooks in cyberspace are more likely to

---

[6] Patricia R. Recupero, "Homicide and the Internet," *Behavioral Sciences & the Law* 39 (2021): 223-225.
[7] Ibid.
[8] Kira Vrist Rønn and Sille Obelitz Søe, "Is Social Media Intelligence Private? Privacy in Public and the Nature of Social Media Intelligence," *Intelligence and National Security* 34, no. 3 (2019): 366.
[9] Packingham v. North Carolina, 137 S.Ct. 1730 (2017).
[10] Rønn and Søe, "Privacy in Public," 366-367.
[11] Ibid.

unwittingly trap and incriminate themselves.[12] While this seems like a rational criticism, it would set a dangerous and worrisome precedent to decide that ignorance of the law constitutes a valid excuse for breaking it, and this argument represents a rather bleak view of the collective public intellect that is hopefully unwarranted. Additionally, while government interests should not trump individual civil liberties, even opponents of social media intelligence recognize its tremendous value as a mechanism for prosecuting, disrupting, and preventing serious threats to public safety including mass violence and terror.[13] Given the fraught nature of this issue, the best way forward will likely involve a multipronged strategy that prioritizes educating citizens about the public nature of the internet and about how to protect their data from unintended use or exploitation by others in their social networks, online companies, their employers, and government agencies. It is also critical for law enforcement agencies to be transparent about their online data collection and surveillance practices while being able to articulate how these practices keep the public safe without endangering civil liberties, and for researchers to continue exploring and instigating dialogs about the evolving nature of privacy in online spaces and its influence on liberty, safety, and security.

Demystifying True Online Threats vs. Protected Violent Speech

The internet is used by violent criminals like domestic terrorists for multiple purposes including to explicitly state their intentions to harm and kill others, to engage in and share violent fantasies, to communicate with and threaten victims, and to share content like manifestos that can signify escalation.[14] The ability to quickly identify and respond to credible threats that are communicated in cyberspace could help police to disrupt and even prevent crimes that often result in mass injuries and casualties, but the legal definition of credible online threat speech remains unresolved.[15] The context of global pandemic and criminality in cyberspace make this appear to be a novel issue, but it simply represents a new direction in the decades-old debate about the types of incendiary speech that should be protected by the Constitution and the types of speech that are heinous and threatening enough to warrant prosecution. The Supreme Court has consistently held for decades that threatening speech that falls outside constitutional protections must be narrowly defined, but the Court has also steadily refused to provide clear and specific guidance regarding how credible threats should be identified.[16] This is an inherently difficult issue to decide from a juridical standpoint, because

[12] Rønn and Søe, "Privacy in Public," 369-371.
[13] Ibid., 367-368.
[14] Recupero, "Homicide and the Internet," 217.
[15] Ibid., 224.
[16] Best, "Need to Uphold Individual Rights," 1136-1138.

threatening communications involve both the original intent and behavior of the communicator and the beliefs and reactions of the message recipient

The Supreme Court's 1942 opinion in *Chaplinsky v. New Hampshire* established the "fighting words" doctrine, holding that speech that is intended to provoke another person to commit violent acts in the public square is not protected by the Constitution.[17] In its 1969 *Watts v. United States* decision the Court set a draconian standard for successfully identifying and prosecuting threatening speech, holding that a public statement that the defendant would kill the President of the United States if drafted into the Army did not constitute a true threat because the statement was conditional and lacked at least some of the necessary elements of an intentional threat.[18] Also in 1969, the *Brandenburg v. Ohio* majority opinion held that speech encouraging others to commit violent crimes is protected by the First Amendment of the Constitution unless that speech incites immediate criminal actions.[19] Interestingly, the history of legal precedent surrounding the issue of protected speech versus true threats indicates that the boundary between freedom of expression and criminal interpersonal violence is often tested by domestic extremist groups like violent protesters and the Ku Klux Klan. While the *Watts* and *Brandenburg* decisions were intended to protect citizens from being prosecuted for voicing unpopular social and political views, they also increased the difficulty of preventing murder, terror, and insurrection by shielding broad categories of violent and threatening speech under the umbrella of the First Amendment.[20]

In the more recent 2003 *Virginia v. Black* decision, the Supreme Court decided that the First Amendment protects cross burnings, asserting that true threats involve elements of serious intent to perpetrate criminal violence targeting a specific person or group.[21] While it is typically not difficult to determine whether a specific individual or group of persons has been targeted, the concept of serious intent to cause harm is very subjective and it is easy to imagine how difficult it might be for a jury to evaluate, especially in the context of digital communications. As contemporary cases illustrate, there are qualitative nuances that affect the threatening nature of online activities like posting savage and murderous fantasies about specific people on social media, creating posts that advocate violence against an individual and sharing that person's identifiers and locational data, or describing why a particular school or residence might represent a soft target for a mass killing. The Supreme Court's 2015 *Elonis v. United States* decision illustrates just how difficult it is to convict an individual for communicating true threats in

[17] Chaplinsky v. New Hampshire, 315 U.S. 568 (1942).
[18] Watts v. United States, 394 U.S. 705 (1969).
[19] Brandenburg v. Ohio, 395 U.S. 444 (1969).
[20] Best, "Need to Uphold Individual Rights," 1136-1138.
[21] Virginia v. Black, 538 U.S. 343 (2003).

cyberspace.[22] The case syllabus describes how Anthony Douglas Elonis used his Facebook page to produce explicitly violent fantasies in the form of rap lyrics targeting his wife, his co-workers, and a group of kindergarten children; but his conviction was overturned because the jury in the original case had been instructed to use a reasonableness standard rather than the stricter intent standard.[23]

The *Elonis* case is troubling because his wife believed his threats were credible and she pursued a restraining order, his employer believed his threats were credible and terminated his employment, the Federal Bureau of Investigation believed his threats were credible and began surveilling his online communications, and a jury decided that a reasonable person would find his threats credible; yet Elonis's stated intention of achieving catharsis through creating rap lyrics ultimately decided the case in his favor.[24] *Elonis* is an illustrative example of the nexus between reasonableness, intent, and context that makes identifying and prosecuting threats in cyberspace so complex. Elonis was correct that a reasonable person standard is too broad for threat speech cases because it does not account for the mental state of the speaker, and it could result in the punishment of innocent people for unknowingly or unwilfully communicating in ways that a jury might find unacceptable.[25] However, it also appears that a serious intent standard is likely too narrow given that Elonis was able to post diagrams of his wife's house including statements describing how easy it would be to shoot her with specific weapons from specific locations and pass these horrifying communications off as lyrical art.[26] Perhaps the most critical challenge posed by *Elonis* is the need for criminal justice practitioners and researchers to improve their skills in effectively analyzing context when evaluating potentially threatening social media communications.[27]

In light of the problems raised within *Elonis*, experts have recommended two potential solutions that the court system might adopt in order to make it easier to identify and prosecute true threats in cyberspace while maintaining strong safeguards protecting the innocent from punishment and shielding free speech that the majority might find inflammatory, needlessly graphic, and violent. The first recommendation involves the development of a dual reasonable-recipient and reasonable-speaker standard that integrates the intent of the speaker and the reactions of their audiences.[28] This proposed hybrid standard is likely the best way

---

[22] Elonis v. United States, 575 U.S. ___ (2015).
[23] Ibid.
[24] Ibid.
[25] Best, "Need to Uphold Individual Rights," 1144.
[26] Elonis, 575 U.S. ___ (2015); see Chief Justice Roberts opinion of the Court.
[27] Lyrissa Barnett Lidsky and Linda Riedemann Norbut, "#I U: Considering the Context of Online Threats," *California Law Review* 106, no. 7 (December 2018): 1885.
[28] Best, "Need to Uphold Individual Rights," 1151-1152.

to provide the court system with a practicable standard for appraising credible threats that effectively reconciles the opposing goals of safeguarding free speech while protecting victims from true threats.[29] The second recommendation describes the creation of a context defense specific to online threat cases that would permit defendants to introduce contextual evidence demonstrating nonthreatening intent and incorporating special jury instructions describing distinctions between true credible threats and constitutionally protected speech that is violent or distasteful.[30] Incorporating these types of recommendations could represent a critical step toward protecting free speech while better equipping police and prosecutors to protect citizens from threats like stranger-initiated homicide, mass killings, and terrorism.

Cyberspace is a Hunting Ground

Since context is such a central component of threatening speech in cyberspace, it is vital for criminal justice practitioners and policymakers to understand the multifarious ways in which the internet in general and social media in particular are commonly employed in the commission of specific types of violent crimes. Some violent criminals use the internet as a platform for engaging with a larger audience and communicating their intent to kill, sharing ideological beliefs, inspiring followers, and even livestreaming crimes like sexual assaults and homicides.[31] The internet also contains uncountable spaces and opportunities for violent criminals to acquire knowledge about topics like how to make bombs or how to kill a person without leaving evidence, as well as sources to purchase tools like body armor, poison, and illegal weapons.[32] One of the more chilling affordances the internet provides to violent criminals involves its use as a hunting ground where criminals can target, stalk, and interact with victims from a position of relative anonymity.[33] Future research about the role of the internet in specific types of violent crime is urgently important because behavioral patterns can be used to develop profiles, inform threat assessments, and demonstrate proof of intent.[34]

It has been argued that internet-facilitated homicides should occupy their own special category as a distinct subtype of homicide, but it seems more likely that there is an online component to the majority of contemporary homicides given the rapid global digitization of many aspects of everyday life.[35] In fact, federal and state law enforcement agencies have long recognized that the internet has given

---

[29] Best, "Need to Uphold Individual Rights," 1151-1152.
[30] Lidsky and Norbut, "Context of Online Threats," 1885-1887.
[31] Recupero, "Homicide and the Internet," 220.
[32] Ibid., 218-219.
[33] Ibid., 219.
[34] Ibid., 224-225.
[35] Ibid., 225.

criminals a huge technological advantage, provided them with easy access to a limitless population of potential victims, and rapidly transformed patterns like the methodology and victimology of traditional violent crimes.[36] Given this knowledge, the internet and social media should be conceptualized as a networked support system that is transmogrifying the way violent crimes are fantasized about, planned, and committed rather than as a completely new environment signifying a new type of crime.[37] This perspective makes it possible to examine the constituent components of a violent crime - offender, victim, behavior, motive, modus operandi, and harm - with the goal of understanding whether discrete patterns of internet use commonly affect any or all of these components during the perpetration of specific types of violent crimes.[38] A brief investigation of some of the ways in which violent offenders use the internet will provide concrete real-world examples showing the kind of information that can be gleaned from internet surveillance and used to inform risk assessments and to establish dangerous intent.

Lone-actor or lone-wolf terrorists are individuals who commit violent crimes that are ideologically motivated and that are designed to spread fear without the support or direction of a larger group or organization.[39] The title lone-wolf is a bit of a misnomer because these individuals are often involved with extremist groups through social media, they typically undergo a radicalization process through exposure to online extremist ideologies, and they may view themselves as representatives of a group rather than as lone actors.[40] These individuals often spend a great deal of time fantasizing about and planning their attacks, and many solo mass shooters have posted comprehensive bodies of online content prior to their attacks including lengthy written manifestos, videos, and letters openly declaring their intentions to perpetrate attacks and identifying specific targeted individuals or locations.[41] While manifestos riddled with hate speech and asinine videos detailing violent fantasies are protected by the First Amendment unless they signify imminent harm to a specific person or persons, these communications exist within a public forum, and they can be used to identify a person as a credible risk to the safety of others and to place that person under surveillance. Consistent expression of violent fantasies and hatred against individuals and groups can also be used to

---

[36] John E. Douglas et al., *Crime Classification Manual: A Standard System for Investigating and Classifying Violent Crime* (Hoboken: John Wiley & Sons, Inc., 2013), 44-45.
[37] Liem and Geelen, "Homicide and the Internet," 70.
[38] Aldona Kipane, "Meaning of Profiling of Cybercriminals in the Security Context," *SHS Web of Conferences* 68 (2019): 1-15.
[39] Mohammadmoein Khazaeli Jah and Ardavan Khoshnood, "Profiling Lone-Actor Terrorists: A Cross-Sectional Study of Lone-Actor Terrorists in Western Europe (2015-2016)," *Journal of Strategic Security* 12, no. 4 (2019): 26.
[40] Ibid., 29.
[41] Recupero, "Homicide and the Internet," 220.

establish a pattern of behavior consistent with intent to commit a violent crime and used to prosecute individuals and to inform profiles to guide resource allocation.[42]

Crime statistics indicate that the United States has a high rate of stranger-perpetrated homicides when compared with other industrialized nations, and research suggests that the internet plays a pivotal role in many stranger-perpetrated homicides including serial offenses.[43] Killers who target strangers often do so for instrumental reasons, meaning they are motivated by the desire to obtain something from their victims such as renown, sexual gratification, money, or material objects.[44] These predators use the cloak of cyberspace to hunt and lure their victims using strategies like designing fake social media accounts, offering to meet for sexual encounters, advertising jobs or services, promising to provide some sort of assistance, and engaging in various other forms of deception about their true identities and intentions.[45] Although human behavior is dynamic and continuously evolving, violent criminals learn to use techniques that consistently help them to achieve their goals while minimizing undesirable risks; therefore, it is possible to identify and track indicators of online hunting, stalking, and luring behavior patterns with the aims of disrupting and preventing violent predation.[46] These hunting behaviors are certainly more surreptitious than hate speech and open declarations of intent to kill on social media, but they still represent discernable behavior patterns that can be used in building offender typologies, guiding surveillance strategies, and establishing criminal intent, motive, and premeditation.

Shrinking Big Data

Researchers exploring the antecedent behavior of public mass killers[47] and intimate partner homicide offenders[48] have identified numerous indicators of online threatening behavior that typically precede these violent crimes including expressing homicidal thoughts, acquiring weapons, articulating specific plans, and engaging in surveillance and cyberstalking of intended victims via social media. It

---

[42] Douglas et al., *Crime Classification Manual*, 3-7.
[43] F. Jeane Gerard, Norair Khachatryan, and Bethany Browning, "Exploration of Crime Scene Characteristics in Cyber-Related Homicides," *Homicide Studies* 24, no. 1 (2020): 46-47.
[44] Ibid., 47.
[45] Ibid., 59.
[46] Douglas et al., *Crime Classification Manual*, 22-23.
[47] Adam Lankford, Krista Grace Adkins, and Eric Madfis, "Are the Deadliest Mass Shootings Preventable? An Assessment of Leakage, Information Reported to Law Enforcement, and Firearms Acquisition Prior to Attacks in the United States," *Journal of Contemporary Criminal Justice* 35, no. 3 (2019): 316-317, 323-324.
[48] Chris Todd, Joanne Bryce, and Virginia N. L. Franqueira, "Technology, Cyberstalking and Domestic Homicide: Informing Prevention and Response Strategies," *Policing and Society* 31, no. 1 (2021): 82-83.

appears that law enforcement agencies should be able to prevent or disrupt a substantial number of violent crimes like lone actor killings, stranger-perpetrated homicides, and intimate partner homicides by leveraging online behavioral threat indicators, but the sheer magnitude of data that individuals produce and share on social media makes this seem like a herculean challenge. Fortunately, there are many nascent big data strategies and systems that have tremendous potential as tools for strategic and tactical criminal intelligence, and these tools often have cross-functional capabilities across different types of crisis situations like preventing mass killings and allocating resources during the COVID-19 pandemic.[49] Crowdsourcing data, the practice of engaging with a community as valued partners and teaching interested citizens about online behavioral threat indicators that should be shared with law enforcement, can be an effective and flexible strategy for expanding limited resources, maintaining police transparency, and building trusting relationships.[50] The value of crowdsourcing is supported by specific online behaviors that have been reported to law enforcement prior to successful mass shooting attacks including website evidence that the 1999 Columbine School shooters made specific advance threats and purchased weapons, and email evidence revealing that the 2009 Fort Hood Army Base shooter was communicating with extremists and might be planning a "heroic" suicide attack.[51]

While crowdsourcing is certainly a useful resource, it does not allow law enforcement to proactively search for specific behavioral indicators, and a more targeted instrument would be better suited for guiding decisions about surveillance and resource allocation. Social media data mining techniques like link analysis and sentiment analysis can equip law enforcement to actively search for specific types of information and even to analyze and classify the sources of that information.[52] Link analysis uses specialized types of search algorithms to explore interconnected links and map related content, while sentiment analysis uses machine-learning methods to identify peoples' attitudes or opinions about particular topics and to evaluate the relative strength and positive or negative quality of those opinions.[53] Social media link analysis can be a particularly powerful tool toward the prevention, disruption, and prosecution of crimes like domestic terror, gang violence, and mass killing because it can be used to map social networks and to chart threatening behavioral indicators like frequenting extremist or violent fetishist websites, and liking or sharing memes that represent fascination with or incitement

[49] Konstantinos Domdouzis et al., "A Social Media and Crowdsourcing Data Mining System for Crime Prevention During and Post-Crisis Situations," *Journal of Systems and Information Technology* 18, no. 4 (2016): 379.
[50] Ibid., 367.
[51] Lankford, Adkins, and Madfis, "Deadliest Mass Shootings Preventable," 324-326.
[52] Domdouzis et al., "Data Mining for Crime Prevention," 368-370.
[53] Ibid.

to commit violent crimes. This information can be strengthened by sentiment analysis designed to expose online behavior patterns that reflect threatening attitudes like misogyny, depersonalization of outgroup members, glorification of violence, and strong positive sentiments about lawlessness and chaos.

Behavioral Profiling and Human Judgment

Algorithms and machine learning undoubtedly have exciting and immense potential to empower law enforcement to combat violent crimes, but these tools must be used with careful consideration and transparency because they can also create mistrust among citizens who fear the dawning of a science fiction-inspired surveillance state policed by indifferent machines. Additionally, machine learning is not a substitute for the intuition that experienced police, profilers, and criminology researchers have gained through years of embodied experience about human aspects of violent crime like complex emotional responses, imaginative fantasies, and often aesthetic signatures.[54] These complementary cautions suggest that the best implementation model should take advantage of the nearly unlimited processing power of computers to mine, organize, and map data while maintaining the primacy of human judgment in making decisions about how to deploy assets and about which individuals are likely to constitute authentic threats. A criminal profiling case study investigating a murderer's Facebook page to determine his motive revealed the importance of professional experience and human intuition in understanding threats, motivations, and intentions.[55] In this case, the cumulative evidence that a computer algorithm would have detected overwhelmingly supported a satanic ritualistic motive, but when the forensic investigator conducted an exhaustive review of the offender's social media account he discovered buried clues indicating that the motive was actually to punish a pedophilic abuser.[56]

This case study illustrates the value of an emerging field in profiling and crime analysis called digital behavior analysis. Digital behavior analysis encompasses the investigation of digital criminal footprints using an amalgamation of traditional and novel methods to achieve goals like understanding motives, linking crimes of serial offenders, and designing offender typologies based on modus operandi, victim characteristics, and offender demographics and behaviors.[57] Through the method of idiographic digital profiling, specialists can track a subject's behavior across multiple websites, determine the true identities of

---

[54] Nemanja Radojevic, Ivana Curovic, and Niodrag Soc, "Using a Facebook Profile in Determining the Motive of Homicide," *Journal of Forensic and Legal Medicine* 20 (2013): 575.
[55] Ibid., 575-577.
[56] Ibid., 577.
[57] Chad M. Steel, "Idiographic Digital Profiling: Behavioral Analysis Based on Digital Forensics," *The Journal of Digital Forensics, Security and Law* 9, no. 1 (2014): 7.

anonymous users, map a subject's social network, evaluate the type and quantity of a subject's social interactions, and track a subject's physical movements using tools like geolocation.[58] Innovative techniques like idiographic digital profiling are especially needful within the contemporary context of the digital transformation of traditional violent crime and ongoing public safety and peacekeeping challenges stemming from the global COVID-19 pandemic. These digital profiling methods will better equip law enforcement to counter the technologically advanced strategies used by many violent criminals by combining computing power and human judgment to exploit behavioral traces hidden in cyberspace.[59]

Conclusion

The past few years have ushered in unprecedented challenges to the criminal justice system caused by global crises and runaway trends like the COVID-19 pandemic, the digitization of everyday life, and the rise in violent crimes facilitated by technology. The present situation has created an imperative for criminal justice practitioners and researchers to develop and implement better tools, systems, and strategies for using internet data to combat violent crimes like mass killings and stranger-imitated homicides while safeguarding the free speech and privacy rights of citizens. While the Internet is legally recognized as a public space, the courts need to more clearly define the specific kinds of online speech that are not protected by the Constitution, and they need to adopt a practicable intent standard for prosecuting credible threats while protecting innocent individuals from being punished for unpopular or offensive constitutionally protected speech. Citizens rights can be protected, and their privacy concerns can be addressed by law enforcement through several strategies including educating citizens about their online rights and vulnerabilities, partnering with communities and integrating their input into threat assessments, and maintaining transparency as much as possible about digital surveillance and data mining tools employed. Finally, the growing field of digital behavior analysis shows great promise as a mechanism for protecting citizens from dual threats of tyranny and violent crime by capitalizing on the data mining and organizing capacities of machine intelligence while relying on human intuition, judgment, and professional experience to guide decisions.

---

[58] Steel, "Idiographic Digital Profiling," 8-10.
[59] Douglas et al., *Crime Classification Manual*, 45.

Bibliography

Best, Alison J. "Elonis v. United States: The Need to Uphold Individual Rights to Free Speech While Protecting Victims of Online True Threats." *Maryland Law Review* 75, no. 4 (2016): 1127-1158.

Brandenburg v. Ohio, 395 U.S. 444 (1969).

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

Domdouzis, K., Babak Akhgar, Simon Andrews, Helen Gibson, and Laurence Hirsch. "A Social Media and Crowdsourcing Data Mining System for Crime Prevention During and Post-Crisis Situations." *Journal of Systems and Information Technology* 18, no.4 (2016): 364-382.

Douglas, John E., Ann W. Burgess, Allen G. Burgess, and Robert K. Ressler. *Crime Classification Manual: A Standard System for Investigating and Classifying Violent Crime*. Hoboken: John Wiley & Sons, Inc., 2013.

Elonis v. United States, 575 U.S. ___ (2015).

Gerard, F. Jeane, Norair Khachatryan, and Bethany Browning. "Exploration of Crime Scene Characteristics in Cyber-Related Homicides." *Homicide Studies* 24, no. 1 (2020): 45-68.

Khazaeli Jah, Mohammadmoein, and Ardavan Khoshnood. "Profiling Lone-Actor Terrorists: A Cross-Sectional Study of Lone-Actor Terrorists in Western Europe (2015-2016)." *Journal of Strategic Security* 12, no. 4 (2019): 25-49.

Kipane, Aldona. "Meaning of Profiling of Cybercriminals in the Security Context." *SHS Web of Conferences* 68 (2019): 1-15.

Kruglanski, Arie W., Rohan Gunaratna, Molly Ellenberg, and Anne Speckhard. "Terrorism in Time of the Pandemic: Exploiting Mayhem." *Global Security: Health, Science and Policy* 5, no. 1 (2020): 121-132.

Lankford, Adam, Krista Grace Adkins, and Eric Madfis. "Are the Deadliest Mass Shootings Preventable? An Assessment of Leakage, Information Reported to Law Enforcement, and Firearms Acquisition Prior to Attacks in the United States." *Journal of Contemporary Criminal Justice* 35, no. 3 (2019): 315-341.

Lidsky, Lyrissa Barnett, and Linda Riedemann Norbut. "#I U: Considering the Context of Online Threats." *California Law Review* 106, no. 6 (December 2018): 1885-1930.

Liem, M.C.A., and M.E.F. Greelen. “The Interface Between Homicide and the Internet.” *Aggression and Violent Behavior* 48 (2019): 65-71.

Lopez, Ernesto, and Richard Rosenfeld. “Crime, Quarantine, and the U.S. Coronavirus Pandemic.” *Criminology & Public Policy* 20 (2021): 401-422.

Packingham v. North Carolina, 137 S.Ct. 1730 (2017).

Radojevic, Nemanja, Ivana Curovic, and Miodrag Soc. “Using a Facebook Profile in Determining the Motive of Homicide.” *Journal of Forensic and Legal Medicine* 20 (2013): 575-577.

Recupero, Patricia R. “Homicide and the Internet.” *Behavioral Sciences & the Law* 39 (2021): 216-229.

Rønn, Kira Vrist, and Sille Obelitz Søe. “Is Social Media Intelligence Private? Privacy in Public and the Nature of Social Media Intelligence.” *Intelligence and National Security* 34, no. 3 (2019): 362-378.

Steel, Chad. “Idiographic Digital Profiling: Behavioral Analysis Based on Digital Footprints.” *The Journal of Digital Forensics, Security and Law* 9, no. 1 (2014): 7-18.

Todd, Chris, Joanne Bryce, and Virginia N. L. Franqueira. “Technology, Cyberstalking and Domestic Homicide: Informing Prevention and Response Strategies.” *Policing and Society* 31, no. 1 (2021): 82-99.

Virginia v. Black, 538 U.S. 343 (2003).

Watts v. United States, 394 U.S. 705 (1969).