U.S. CITIZENSHIP AND IMMIGRATION SERVICES’ EFFORT TO IDENTIFY TERRORISM THREATS: IS SOCIAL MEDIA INTELLIGENCE (SOCMINT) THE NEXT TOOL?

by

Erik M. Thompson

December 2019

Co-Advisors: Erik J. Dahl
Lynda A. Peters (contractor)

Approved for public release. Distribution is unlimited.
U.S. CITIZENSHIP AND IMMIGRATION SERVICES’ EFFORT TO IDENTIFY TERRORISM THREATS: IS SOCIAL MEDIA INTELLIGENCE (SOCMINT) THE NEXT TOOL?

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

Terrorists use the internet to facilitate every aspect of their nefarious activity. This use creates a novel research question. To what degree can an open-source social media intelligence (SOCMINT) gathering and analysis capability assist U.S. Citizenship and Immigration Services (USCIS) in accomplishing its homeland security mission? The critics of SOCMINT argue it is an unnecessary, problematic, and ill-advised effort based on efficacy, data management, and constitutional grounds. Therefore, the thesis explores the past efforts, necessity, and efficacy of open-source SOCMINT in identifying potential fraud, public safety, and/or national security concerns (threats) from immigrants seeking immigration benefits. The research consists of qualitatively examining issue rhetoric—the debate and discussion—between the critics and supporters of SOCMINT. The Profiles of Individual Radicalization in the United States dataset provides a quantitative, evidence-grounded means to gain insight on radicalized immigrants’ use of the internet and social media in plotting attacks and the potential for threat detection. The research demonstrates threats among immigration benefit seekers exist, and that SOCMINT is a viable means to identify and mitigate the threats. The thesis concludes the propositions for SOCMINT are valid and the critics’ objections should not impede the effort. The thesis recommends USCIS continue SOCMINT, ensuring the endeavor observes a balance between security and liberty.

social media, analysis, Department of Homeland Security, DHS, screening, vetting, Twitter, Facebook, YouTube, threats, sentiment analyzer, law enforcement, big data analytics, terrorist, terrorism, babel street, Open-Source Intelligence, OSINT, social media intelligence, SOCMINT, Giant Oak, U.S. Citizenship and Immigration Services, USCIS, Fraud Detection National Security, FDNS

Approved for public release. Distribution is unlimited.

Approved for public release. Distribution is unlimited.

PUBLIC REPORTING BURDEN FOR THIS COLLECTION OF INFORMATION IS ESTIMATED TO AVERAGE 1 HOUR PER RESPONSE, INCLUDING THE TIME FOR REVIEWING INSTRUCTION, SEARCHING EXISTING DATA SOURCES, GATHERING AND MAINTAINING THE DATA NEEDED, AND COMPLETING AND REVIEWING THE COLLECTION OF INFORMATION. SEND COMMENTS REGARDING THIS BURDEN ESTIMATE OR ANY OTHER ASPECT OF THIS COLLECTION OF INFORMATION, INCLUDING SUGGESTIONS FOR REDUCING THIS BURDEN, TO WASHINGTON HEADQUARTERS SERVICES, DIRECTORATE FOR INFORMATION OPERATIONS AND REPORTS, 1215 JEFFERSON DAVIS HIGHWAY, SUITE 1204, ARLINGTON, VA 22202-4302, AND TO THE OFFICE OF MANAGEMENT AND BUDGET, PAPERWORK REDUCTION PROJECT (0704-0188) WASHINGTON, DC 20503.

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.
U.S. CITIZENSHIP AND IMMIGRATION SERVICES’ EFFORT TO IDENTIFY TERRORISM THREATS: IS SOCIAL MEDIA INTELLIGENCE (SOCMINT) THE NEXT TOOL?

Erik M. Thompson
Immigration Officer, U. S. Citizenship and Immigration Services/Fraud Detection and National Security, Department of Homeland Security
BS, Georgetown University, 2003
JD, University of Missouri -Kansas City, 2012

Submitted in partial fulfillment of the requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
December 2019

Approved by: Erik J. Dahl
Co-Advisor

Lynda A. Peters
Co-Advisor

Erik J. Dahl
Associate Professor, Department of National Security Affairs

iii
ABSTRACT

Terrorists use the internet to facilitate every aspect of their nefarious activity. This use creates a novel research question: To what degree can an open-source social media intelligence (SOCMINT) gathering and analysis capability assist U.S. Citizenship and Immigration Services (USCIS) in accomplishing its homeland security mission? The critics of SOCMINT argue it is an unnecessary, problematic, and ill-advised effort based on efficacy, data management, and constitutional grounds. Therefore, the thesis explores the past efforts, necessity, and efficacy of open-source SOCMINT in identifying potential fraud, public safety, and/or national security concerns (threats) from immigrants seeking immigration benefits. The research consists of qualitatively examining issue rhetoric—the debate and discussion—between the critics and supporters of SOCMINT. The Profiles of Individual Radicalization in the U.S. dataset provides a quantitative, evidence-grounded means to gain insight on radicalized immigrants’ use of the internet and social media in plotting attacks and the potential for threat detection. The research demonstrates threats among immigration benefit seekers exist, and that SOCMINT is a viable means to identify and mitigate the threats. The thesis concludes the propositions for SOCMINT are valid and the critics’ objections should not impede the effort. The thesis recommends USCIS continue SOCMINT, ensuring the endeavor observes a balance between security and liberty.
# TABLE OF CONTENTS

## I. INTRODUCTION

A. RESEARCH QUESTION ............................................................... 1
B. PROBLEM STATEMENT ............................................................ 1
C. BACKGROUND ................................................................. 4
D. LITERATURE REVIEW ............................................................. 8
  1. Technology Experts .......................................................... 9
  2. Security Experts ............................................................... 12
  3. Critics ................................................................................ 16
E. RESEARCH DESIGN .............................................................. 19
F. CHAPTER OVERVIEW ......................................................... 22

## II. PROPOSITIONS FOR SOCMINT

A. MISSION ..................................................................................... 26
B. LEGAL AUTHORITIES ............................................................. 28
C. TERRORISM ON SOCIAL MEDIA ................................................ 28
  1. Propaganda ............................................................................. 29
  2. Communication ...................................................................... 30
  3. Recruiting .............................................................................. 30
  4. Radicalization ........................................................................ 31
  5. Plotting ................................................................................... 31
  6. Experts .................................................................................. 32
  7. Profiles of Individual Radicalization in the United States ..... 32
D. OPEN-SOURCE NECESSITY .................................................... 47
E. LAW ENFORCEMENT SOCMINT USE ..................................... 48
F. SOCMINT SUCCESSES ............................................................ 49
G. CONCLUSION ........................................................................... 50

## III. SOCMINT PROBLEMATIC EFFORT AND NECESSITY CONCERNS

A. A PROBLEMATIC EFFORT ..................................................... 53
  2. USCIS FOIA Documents ..................................................... 61
B. WE ARE SAFE ENOUGH .......................................................... 63
C. CONCLUSION ........................................................................... 67

## IV. SOCMINT EFFICACY CONCERNS

A. YIELD ...................................................................................... 69

vii
LIST OF FIGURES

Figure 1. Residency status of the radicalized at the time of exposure .......... 34
Figure 2. Location of latter period radicalization ........................................ 35
Figure 3. Role of the internet in radicalization ........................................... 36
Figure 4. Role of social media in radicalization ......................................... 38
Figure 5. Use of the internet for logistics or communication in preparation of a violent plot ................................................................. 39
Figure 6. Gravity of threat from social media users ................................... 40
Figure 7. Attempts to hide or conceal preparation for the plot (Operational Security) ................................................................. 42
Figure 8. Frequency of social media use related to radicalization or mobilization .............................................................. 43
Figure 9. Social media activities ................................................................. 45
Figure 10. History of involvement in non-ideologically motivated criminal activities ............................................................... 46
Figure 11. Profiles of individual radicalization in the United States, Keshif data visualization tool ....................................................... 111
<table>
<thead>
<tr>
<th>ACRONYM</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACLU</td>
<td>American Civil Liberties Union</td>
</tr>
<tr>
<td>CBP</td>
<td>U.S. Customs and Border Protection</td>
</tr>
<tr>
<td>CENTRIC</td>
<td>Centre of Excellence in Terrorism, Resilience, Intelligence &amp; Organised Crime Research</td>
</tr>
<tr>
<td>COE</td>
<td>center of excellence</td>
</tr>
<tr>
<td>CSTAB</td>
<td>Center for the Study of Terrorism and Behavior</td>
</tr>
<tr>
<td>DANTE</td>
<td>Detecting and ANalysing TErrorist-related online contents and financing activities</td>
</tr>
<tr>
<td>DARPA</td>
<td>Defense Advanced Research Projects Agency</td>
</tr>
<tr>
<td>DHS</td>
<td>Department of Homeland Security</td>
</tr>
<tr>
<td>DoD</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>DOJ</td>
<td>Department of Justice</td>
</tr>
<tr>
<td>EOIR</td>
<td>Executive Office for Immigration Review</td>
</tr>
<tr>
<td>EPIC</td>
<td>Electronic Privacy Information Center</td>
</tr>
<tr>
<td>EPS</td>
<td>egregious public safety</td>
</tr>
<tr>
<td>FBI</td>
<td>Federal Bureau of Investigation</td>
</tr>
<tr>
<td>FDNS</td>
<td>Fraud Detection and National Security</td>
</tr>
<tr>
<td>FOIA</td>
<td>Freedom of Information Act</td>
</tr>
<tr>
<td>FY</td>
<td>fiscal year</td>
</tr>
<tr>
<td>GAO</td>
<td>Government Accountability Office</td>
</tr>
<tr>
<td>HSSEDI</td>
<td>Homeland Security Systems Engineering &amp; Development Institute</td>
</tr>
<tr>
<td>HUMINT</td>
<td>human intelligence</td>
</tr>
<tr>
<td>I&amp;A</td>
<td>Office of Intelligence and Analysis</td>
</tr>
<tr>
<td>ICE</td>
<td>U.S. Immigration and Customs Enforcement</td>
</tr>
<tr>
<td>IMINT</td>
<td>imagery intelligence</td>
</tr>
<tr>
<td>INA</td>
<td>Immigration and Nationality Act</td>
</tr>
<tr>
<td>IO</td>
<td>immigration officer</td>
</tr>
<tr>
<td>ISIS</td>
<td>Islamic State of Iraq and Syria</td>
</tr>
<tr>
<td>ISO</td>
<td>immigration services officer</td>
</tr>
<tr>
<td>LEAs</td>
<td>law enforcement agencies</td>
</tr>
<tr>
<td>Acronym</td>
<td>Full Form</td>
</tr>
<tr>
<td>---------</td>
<td>-----------</td>
</tr>
<tr>
<td>LRBAAY</td>
<td>Long Range Broad Agency Announcement</td>
</tr>
<tr>
<td>NTA</td>
<td>Notices to Appear</td>
</tr>
<tr>
<td>OIG</td>
<td>Office of the Inspector General</td>
</tr>
<tr>
<td>OSINT</td>
<td>Open-source intelligence</td>
</tr>
<tr>
<td>PART</td>
<td>Action Plan Against Radicalization and Terrorism</td>
</tr>
<tr>
<td>PIRUS</td>
<td>Profiles of Individual Radicalization in the United States</td>
</tr>
<tr>
<td>RAND</td>
<td>Research and Development Corporation</td>
</tr>
<tr>
<td>RFI</td>
<td>Request for Information</td>
</tr>
<tr>
<td>ROSM</td>
<td>Real-time Open Source Analysis of Social Media</td>
</tr>
<tr>
<td>SIGINT</td>
<td>Signals Intelligence</td>
</tr>
<tr>
<td>SMD</td>
<td>Social Media Division</td>
</tr>
<tr>
<td>SMTF</td>
<td>Social Media Task Force</td>
</tr>
<tr>
<td>SOCMINT</td>
<td>Social Media Intelligence</td>
</tr>
<tr>
<td>S&amp;T</td>
<td>Science and Technology</td>
</tr>
<tr>
<td>START</td>
<td>National Consortium for the Study of Terrorism and Responses to Terrorism</td>
</tr>
<tr>
<td>TENSOR</td>
<td>ReTriEval and aNalysis of heterogeneous online content for terrorOrist activity Recognition</td>
</tr>
<tr>
<td>TRIG</td>
<td>Terrorism-related Inadmissibility Grounds</td>
</tr>
<tr>
<td>TSA</td>
<td>Transportation Security Administration</td>
</tr>
<tr>
<td>UK</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>USCIS</td>
<td>U.S. Citizenship and Immigration Services</td>
</tr>
</tbody>
</table>
EXECUTIVE SUMMARY

Terrorists use the internet to disseminate propaganda, solicit new members, communicate, gather intelligence, seek money, and inspire and plan attacks.¹ In 2015, the San Bernardino, California, terrorist attack brought the use of social media intelligence (SOCMINT) by the Department of Homeland Security (DHS) and U.S. Citizenship and Immigration Services (USCIS) to vet immigration benefit seekers under scrutiny. Republicans and Democrats in both the House and Senate indicated support for using SOCMINT to screen individuals entering the United States.² In 2016, DHS expanded its use of SOCMINT under Secretary Johnson’s command.

USCIS “administers the nation’s lawful immigration system, safeguarding its integrity and promise by efficiently and fairly adjudicating requests for immigration benefits while protecting Americans, securing the homeland, and honoring our values.”³ USCIS began conducting SOCMINT research and development projects to test the automation of “bulk screening of social media information” supplemented with human analyst review “across a number of high-priority populations.”⁴ The Office of the Inspector General (OIG) investigated and reported on DHS’ preliminary efforts as if they were pilots rather than research and development projects.⁵ Based, in part, on the OIG

findings and Freedom of Information Act (FOIA) releases, the skeptics of SOCMINT argue against its use. These critics contend that the number of social media platforms, posts, and foreign languages used, context ambiguities, constitutional implications, data management issues, and targets’ evasion efforts make the DHS open-source SOCMINT capability unviable.⁶

A. RESEARCH QUESTION

Terrorists’ use of the internet, DHS’ response, and the critics’ claims create a novel research question. To what degree can an open-source SOCMINT gathering and analysis capability assist USCIS in accomplishing its homeland security mission? Determining if open-source SOCMINT is viable for DHS and identifying how to maintain a successful open-source SOCMINT capability requires answers to various questions. For example, how can DHS analyze the large volume of social media content

on hundreds of social media platforms efficiently? How can DHS maintain an open-source SOCMINT capability consistent with constitutional requirements? How can DHS differentiate the context of social media content, e.g., legitimate threat versus satire? How can DHS efficiently navigate an endeavor involving numerous languages? Do targets’ evasion efforts make the DHS open-source SOCMINT efforts futile? This thesis answers these related questions during the effort to answer the research question.

B. PURPOSE

This thesis seeks to fill a gap in the literature—the lack of immigration-related SOCMINT scholarship—by exploring the necessity and efficacy of open-source SOCMINT in identifying potential fraud, public safety, and/or national security concerns (threats) from immigrants seeking immigration benefits from USCIS. In terms of practical implications, the thesis provides policymakers an inventory of the critics’ objections to SOCMINT. It offers insights into DHS’ policy and procedural safeguards to avoid the perils related to the critics’ objections. It evaluates and rebuts the critics’ claims, where possible, by providing a more fulsome review of the applicable documents about the DHS SOCMINT efforts than exists in the public discourse.

C. RESEARCH METHODS

This thesis examines the qualitative data of the issue rhetoric—the debate and discussion—between the critics and supporters of implementing SOCMINT. This rhetoric exists in the open-source literature, e.g., books, scholarly journals, articles, news stories, FOIA-released documents, and government reports and memorandums. In addition, quantitative data from the Profiles of Individual Radicalization in the United States (PIRUS) dataset provides insight into the viability of using SOCMINT to identify threats among immigration benefit seekers.

D. RESULTS AND CONCLUSIONS

The research results show that the critics’ objections are mostly unpersuasive. Open-source SOCMINT is a viable means for USCIS to identify and mitigate threats among immigration benefit seekers for the following reasons:
• The PIRUS dataset confirms that the propositions for SOCMINT are valid.7

• A broader analysis of the OIG report and FOIA-released documents undermines the allegation that efforts to deploy a SOCMINT capability to date have been fraught with problems.

• Insights from the 9/11 Commission, other experts, a rational, objective reading of the OIG and FOIA reports, and the PIRUS dataset undermine the argument that the nation is safe enough without SOCMINT.

• A broader analysis of the OIG report and FOIA-released documents refutes the claims about yield in identifying threats. The critics’ automation arguments about scope and scale are unpersuasive because USCIS is not relying on automated SOCMINT for the process of reviewing posts. Safeguards are in place to mitigate language and context misinterpretation and any potential derivative adverse outcomes. The PIRUS dataset contradicts the critics’ encryption claim for both internet users and social media users. The critics’ claim about identity resolution is questionable.

• The critics’ arguments about misinterpretation from data sharing are unpersuasive because there is no reasonable expectation of privacy in open-source social media data.

---

7 “Profiles of Individual Radicalization in the United States (PIRUS),” National Consortium for the Study of Terrorism and Responses to Terrorism (START), accessed June 8, 2019, https://www.start.umd.edu/data-tools/profiles-individual-radicalization-united-states-pirus. “The bulk of data collection for PIRUS was supported by the National Institute of Justice, Office of Justice Programs, Department of Justice, through Award Number 2012-ZA-BX-0005. In addition, an effort to review and update information in the PIRUS dataset has been supported with funding from the Department of Homeland Security through the Center for the Study of Terrorism and Behavior (CSTAB) Partner grant. The PIRUS dataset and any findings derived from the dataset do not represent the official positions of the National Institute of Justice, the Department of Justice, the Department of Homeland Security, or any other funding agency.” “PIRUS—Frequently Asked Questions,” National Consortium for the Study of Terrorism and Responses to Terrorism, accessed August 12, 2019, https://www.start.umd.edu/pirus-frequently-asked-questions.
The nature of the social media data collected, privacy rules, and the information collected from non-social media data collection efforts undermine the argument about SOCMINT privacy intrusiveness.

E. RECOMMENDATIONS

This thesis offers SOCMINT policymakers a number of recommendations:

• USCIS should continue to use open-source SOCMINT to identify fraud, public safety, and/or national security threats. Agile leveraging of authorities and technology to meet threat identification needs is critical. It is important to look broadly beyond DHS for expertise and best practices on SOCMINT among law enforcement agency partners’ initiatives, e.g., Social Media the Internet and Law Enforcement conferences, Five Eyes members, and Real-time Open Source Analysis of Social Media.8

• DHS should use care in appropriately designating efforts as pilots or research and development projects and ensure a unified understanding, management, and messaging across DHS components. DHS components should resist merely concurring with OIG findings to silence concerns versus defending actions on their merits. Senior DHS leadership should publicly defend ill-informed narratives from critic and media echo chambers that confound fact-based public interpretation of DHS initiatives.

• DHS should consider supplementing the open solicitation and commercial tool approach for SOCMINT tool development in favor of a model more aligned with the United Kingdom’s Detecting and ANalysing TERRORist-related online contents and financing activities and reTRiEval and aNalysis

---

of heterogeneous online content for terrorist activity Recognition project approaches.9

- DHS should research the viability of creating a centralized Center of Excellence for DHS’ SOCMINT capability modeled on the United Kingdom’s Centre of Excellence in Terrorism, Resilience, Intelligence & Organised Crime Research Open-source Intelligence Hub.10

- USCIS should ensure data and constitutional protections are robust. Policies, procedures, and training are in place to prevent problems. However, as with any human-based system, efforts at the front end may not guarantee employee conduct during execution. Policies, procedures, and training are not 100 percent effective, despite best intentions. Consequently, USCIS must also remain equally vigilant in its oversight efforts to protect the principles of the U.S. homeland.

---


ACKNOWLEDGMENTS

For Adeline,
May your world be a safer place.

For Laura and Bryan,
In gratitude and memory.

Mom and Sarah:
Thank you for your understanding, patience, and support.

Rob and Vas:
Thank you for making this opportunity possible.

Fred, John, Mike, Brett, and Linda:
Thank you for your confidence in me, and your endorsement and encouragement.

Frank and Nathaniel:
Thank you for your wisdom and guidance.

David, Troy, and Matt:
Thank you for your support and encouragement.

Lynda, Erik, Nancy, and Aileen:
Thank you for your expertise and guidance.

All my colleagues in DHS and Cohort 1803/1804, especially Julie, Guani, Sarah, Carl, Corey, Drew, Nick, Brandon, Wes, Holly, Elizabeth, Rebecca, J. Rieger, Shawn, Gene, Marie-Claire, David, Matt, Max, Greg, and Gary:
Thank you for being such great sounding boards.

The CHDS faculty and staff, especially Lauren, Greta, Marianne, Scott, and Eric:
Thank you for your assistance.
THIS PAGE INTENTIONALLY LEFT BLANK
I. INTRODUCTION

In this respect, the Internet has proved to be an especially beneficial communications medium for terrorists—a key means for both external propaganda and internal command and control and information purposes.

—Bruce Hoffman, author, *Inside Terrorism*

Ninety percent of intelligence comes from open sources. The other ten percent, the clandestine work, is just the more dramatic. The real intelligence hero is Sherlock Holmes, not James Bond.

—General Sam Wilson, USA Retired, former Director, Defense Intelligence Agency

A. RESEARCH QUESTION

To what degree can an open-source social media intelligence (SOCMINT) gathering and analysis capability assist U.S. Citizenship and Immigration Services (USCIS) in accomplishing its homeland security mission?

B. PROBLEM STATEMENT

Terrorists use the internet to disseminate propaganda, solicit new members, communicate, gather intelligence, seek money, and inspire and plan attacks.\(^1\) Suspects openly boasting on social media venues of their nefarious intentions prior to acting upon them has proven to be an invaluable roadmap of radicalization and detection—an upside

for law enforcement and intelligence entities.\(^2\) State, local, international, and numerous federal law enforcement agencies (LEAs) are using social media to identify potential terrorists.\(^3\)

The Department of Homeland Security (DHS) is leveraging the analytic generation of intelligence from open-source social media sources—SOCMINT—to identify and deter terrorists.\(^4\) The DHS’ implementation of an open-source SOCMINT capability seeks to leverage the efficient and effective use of open-source information and analysis to help secure the homeland.\(^5\) However, the skeptics argue that the number of social media platforms, posts, and foreign languages used, context ambiguities, constitutional implications, data management issues, and targets’ evasion efforts create a

---


complex terrain of challenges that make the DHS open-source SOCMINT capability unviable.6

Identifying the challenges in this terrain, assessing the skeptics’ concerns, and offering DHS’ policy makers a set of recommendations provides a path forward as DHS’ SOCMINT efforts expand. Determining if open-source SOCMINT is viable for DHS and identifying how to maintain a successful open-source SOCMINT capability requires answers to various questions. For example, how can DHS analyze the large volume of social media content on hundreds of social media platforms efficiently? How can DHS maintain an open-source SOCMINT capability consistent with constitutional requirements? How can DHS differentiate the context of social media content, e.g., legitimate threat versus satire? How can DHS efficiently navigate an endeavor involving numerous languages? Do targets’ evasion efforts make the DHS open-source SOCMINT

---

efforts futile? This thesis answers these related questions during the effort to answer the research question.

C. BACKGROUND

Criminals have exploited data networks for as long as the networks have existed.7 The most powerful network—the internet—attracting billions of users inevitably became the wrongdoers’ focus.8 Al-Qaeda established its first website in the 1990s.9 In a 2012 survey, approximately 80 percent of federal, state, and local law enforcement investigators acknowledged using social media for intelligence collection.10 One editor explained, “We’re not talking about collecting metadata or compelling companies to turn over information, but good, old-fashioned subterfuge and digital legwork.”11

In 2015, the San Bernardino, California, terrorist attack brought the SOCMINT discussion relating to DHS’ and USCIS’ vetting efforts into the media spotlight. When the radicalized Muslim couple killed 14 people and injured nearly two dozen others at an office party, the wife, Tashfeen Malik, a Pakistani national, became the focus of attention.12 In 2014, she used a K-1 visa, the type for people who intend to marry a U.S. citizen, to gain admission into the United States.13 Malik passed two background checks prior to being admitted and a third check in the summer of 2015, when USCIS, a DHS

---


8 Economist.


13 Brotman.
component, granted her lawful permanent residency (a green card). During the early stages of the post-attack investigation, investigators initially concluded that Malik, prior to her K-1 visa approval, had discussed violent jihad on her social media. As a result, officials in Washington, District of Columbia, made improving the visa application screening process urgent. The State Department and DHS announced they were contemplating stricter scrutiny of visa applicants’ social media use. Democrats and Republicans launched initiatives in the Senate and House that would require heightened social media screening in the visa adjudication process.

Several congressional Republicans, including former Senator John McCain and former House Judiciary Committee Chairman Bob Goodlatte, prepared legislation that would require DHS to conduct SOCMINT on all foreigners submitting applications for entry to the United States. McCain said, “It is unacceptable that Congress has to legislate on this, and that it wasn’t already the Department of Homeland Security’s practice to take such commonsense steps when screening individuals entering this country.” Democrats joined in the growing congressional scrutiny. Senator Chuck Schumer, the third-ranking Senate Democrat, and Senator Jeanne Shaheen led a group of 22 Senate Democrats who sent Jeh Johnson, then Secretary of DHS, a request to establish a policy promptly that mandated conducting SOCMINT on all foreigners seeking visas to enter the United States. Secretary Johnson’s remarks in a POLITICO interview mark the first time that he publicly discussed the merits of vetting social media for immigration

14 Brotman.
15 Brotman. The social media conversations were private direct messages and would not have been uncovered through open-source SOCMINT efforts.
16 Brotman.
17 Brotman.
18 Brotman.
20 Kim.
21 Kim.
22 Kim.
cases. He indicated that DHS had initiated an experimental program months earlier to examine social media accounts of those seeking immigration benefits. Former President Barack Obama instructed both the State Department and DHS to evaluate the K-1 visa screening process for “possible program enhancements.”

In 2016, DHS expanded its use of social media to include more than 30 different investigative and operational uses. The DHS Social Media Task Force (SMTF) recommended expanding the department’s use of social media in the vetting and screening mission initiatives. Secretary Johnson concluded, in accordance with applicable privacy and other laws, that this expansion was imperative. DHS officials testified that DHS limits the use of social media to publicly available information, in accordance with the DHS authorities, and handles and maintains the information consistent with the relevant System of Records Notices and the Privacy Act. Collaborating with the Science and Technology (S&T) directorate, DHS tested the automation of “bulk screening of social media information” supplemented with human analyst “review across a number of high-priority populations,” including Electronic System for Travel Authorization and refugee applicants. S&T continued to “work with industry to leverage the billions of dollars of private sector investment in social media analytics to identify solutions that can best support DHS screening and vetting.”

23 Kim.
24 Kim.
25 Kim.
27 Department of Homeland Security.
29 Department of Homeland Security.
30 Department of Homeland Security.
31 Department of Homeland Security.
USCIS “administers the nation’s lawful immigration system, safeguarding its integrity and promise by efficiently and fairly adjudicating requests for immigration benefits while protecting Americans, securing the homeland, and honoring our values.” USCIS adjudicates more than 26,000 applications and petitions for a variety of immigration benefits on an average day. The benefits sought include applications for lawful permanent resident status (green cards), U.S. citizenship through naturalization, employment authorization, travel documents, etc. In each of these immigration benefit request-processing scenarios, USCIS vets applicants and petitioners by conducting security checks to identify any potential derogatory information that may indicate threats. According to the *DHS Operational Use of Social Media*, “USCIS uses social media, as defined in the Privacy Policy, to gather information for the purpose of benefits determinations and in support of administrative investigations into alleged violations of the immigration laws.” USCIS’ Fraud Detection and National Security (FDNS) directorate achieves the USCIS mission, in part, by discovering national security and public safety threats and identifying, investigating, and preventing immigration benefit fraud.

Congress, under a legal mechanism known as the Terrorism-related Inadmissibility Grounds (TRIG), has established that terrorists should be prohibited from entering the United States. For example:

---


generally, any individual who is a member of a “terrorist organization” or who has engaged or engages in terrorism-related activity as defined by the Immigration and Nationality Act (INA) is “inadmissible” (not allowed to enter) the United States and is not eligible for most immigration benefits.  

USCIS defines egregious public safety (EPS) cases as those in which “information indicates the alien is under investigation for, has been arrested for (without disposition), or has been convicted of,” more serious offenses, e.g., “murder, rape, sexual abuse of a minor, illicit trafficking in firearms or destructive devices,” etc.  

USCIS defines a non-EPS criminal case “as a case where information indicates the alien is under investigation for, has been arrested for (without disposition), or has been convicted of any crime not listed” in the EPS offenses.  

Both types of public safety concerns, EPS and non-EPS, can affect inadmissibility. The result of committing immigration benefit fraud is succinctly defined in the INA, “Any alien who, by fraud or willfully misrepresenting a material fact, seeks to procure (or has sought to procure or has procured) a visa, other documentation, or admission into the United States or other benefit provided under this chapter is inadmissible.”  

If the applicant’s social media reveals a potential fraud, public safety, and/or national security concern, then SOCMINT opens a line of inquiry that DHS can investigate in its mission to secure the homeland.

D. LITERATURE REVIEW

This literature review assesses the state of knowledge about the viability of using open-source social media to identify potential threats to national security. The authors generally fall into three camps: the “technology experts” who explain the means, the “security experts” who condone using social media for vetting on safety grounds, and the

37 U.S. Citizenship and Immigration Services.


39 Cisna, 7.

“critics” who oppose using social media for vetting based on necessity, efficacy, or constitutional grounds.

1. Technology Experts

A thorough explanation of the detailed, complex technology behind a successful SOCMINT capability is beyond the scope of this literature review; however, a brief, high-level overview will greatly assist the reader in understanding SOCMINT. Optimally gathering large amounts of social media data requires a programmatic versus manual harvesting approach. Application programming interfaces provide a connection to the social media platform data source. After accessing the data, the analyst can mine the data for content of potential interest.

Analysts use machine learning, text analytics, deep neural networks, and various techniques to sift through the data programmatically. These techniques can improve the analysts’ timely collection of data about potential terrorist threats. The data may yield intelligence on terrorists’ activities, identities, and locations. For example, content-based analysis focuses on what was said. Subject-based analysis focuses on what a particular person or group is saying. The analysts can use social media data to create maps based on interactions and relationships among users that may reveal previously unknown connections. However, accessing and analyzing social media data presents unique technology challenges.

---


42 Bartlett and Miller, 16.


44 Marcellino et al., *Monitoring Social Media*, 11.

45 Marcellino et al., 11.

46 Marcellino et al., 11.


48 Correa and Sureka, 14.

49 Marcellino et al., *Monitoring Social Media*, 11.
The first challenge is identifying content that may have a nexus to terrorism. Much of the literature focuses on addressing the scope, scale, language, and context challenges. Over 100 English-language social networks are in existence. Twitter users post 500 million tweets every day. Users on Facebook share almost five billion pieces of content every day. YouTube users upload over 18,000 hours of video every hour. The enormous quantity of user content posted to these websites creates a challenge, but is a potentially fertile source to identify terrorism content. Omand et al. argue that it would not be difficult or cost prohibitive to increase the throughput of current social media data collection technologies. Social media platforms are inherently transnational. Social media content from Facebook includes more than 80 languages from across the world. Correa and Sureka posit that language creates challenges for content-based analysis methods because not all languages are written from left to right and some social media posts contain more than one language. Successfully extracting meaning from social media posts requires more than machine translation. For example, a potential for misinterpretation occurs when context is not considered. Duarte et al. recognize this limitation and argue that automated content analysis tool approaches must

54 Marcellino et al., Monitoring Social Media, 10–11.
55 Omand, Bartlett, and Miller, “Introducing Social Media Intelligence (SOCMINT),” 817.
58 Correa and Sureka, “Solutions to Detect and Analyze Online Radicalization,” 12.
59 Omand, Bartlett, and Miller, “Introducing Social Media Intelligence (SOCMINT),” 810.
60 Omand, Bartlett, and Miller, 812.
be supplemented with human validation.\textsuperscript{61} Despite the challenges, the technology experts agree that content with a nexus to terrorism can be identified.

The second challenge is identifying the author of the content who may have a nexus to terrorism. The literature addresses how identity resolution, platform content removal, and evasion tactics complicate this identification endeavor. Yeung and his co-authors see identity resolution—the task of matching an individual’s offline and online identities—as DHS’ biggest obstacle in SOCMINT.\textsuperscript{62} Identity resolution is challenging when users seek anonymity. Social media companies often remove terrorism-related content. However, deleting terrorism-related content can frustrate law enforcement efforts.\textsuperscript{63} Consequently, some agencies have requested that social media platforms refrain from removing terrorism-related content so that investigators can monitor terrorists and use undercover tactics to dupe terrorists into revealing information.\textsuperscript{64} Goodman, embracing a less cooperative approach, argues that social media platforms should be held liable for material support of terrorism.\textsuperscript{65} Malik raises the point that terrorists can move to the Darknet, which is “more difficult to police than the surface and deep webs, meaning they have the potential to function as a jihadist virtual safe-haven.”\textsuperscript{66} In general, the technology experts concur that identity resolution is difficult and that going dark exacerbates the identity problem.

Each of these technology challenges—scope, scale, language, context, identity resolution, and evasion tactics—have to be overcome to create a viable SOCMINT


\textsuperscript{64} Perlroth and Isaac.


\textsuperscript{66} Malik, \textit{Terror in the Dark}, iv.
capability. Identifying technology challenges, though, is only half of the journey. Sensible solutions also have to be identified. The literature, other than the Yeung et al. contribution, offers little insight that is directly on point with how DHS can overcome these challenges.

2. Security Experts

The literature from the security experts is diverse, but can be examined with four lenses: terrorists’ use of the internet, characterizations of that use, the implications on policing, and the experts’ value judgments regarding SOCMINT. EUROPOL, Coats, Akhgar, Staniforth, and Ines von Behr et al. agree that terrorists use the internet for disseminating propaganda, recruiting, plotting, funding, communicating, radicalizing, etc.67 The experience of the technology experts at the social media platforms validates this assessment. In the first quarter of 2018, Facebook identified almost two million pieces of al-Qaeda and Islamic State of Iraq and Syria (ISIS) material, nearly double the amount in the previous quarter.68 In the last two quarters of 2017, Twitter banned almost 275,000 accounts for promoting terrorism.69 Terrorists have no qualms about using open-source platforms. An al-Qaeda training manual discovered in Afghanistan advised that 80 percent of the information needed for attacking an enemy could be found in open


68 Bickert and Fishman, “Hard Questions: How Effective Is Technology in Keeping Terrorists Off Facebook?”

sources. Terrorists synthesize this research into instructions. The 600-page *Encyclopedia of Jihad* is widely circulated online and includes chapters, such as “how to kill,” “explosive devices,” “manufacturing detonators,” and “assassination with mines.”

The security experts concur unanimously that terrorists use the internet.

Despite consensus about terrorists’ use of the internet, the experts’ characterizations about that use vary. Nissen argues that terrorists have weaponized social media and that this phenomenon is not receiving the level of academic study necessary to supplement the existing body of research within traditional war-studies. The Australian government describes the internet as “the command and control networks of choice for terrorists.” Some counterterrorism experts label the internet as a “terrorist university, a place where terrorists can learn new techniques and skills to make them more effective in their attack methodologies.” Governor Kean, former chairman of the 9/11 Commission, reports in a recent Bipartisan Policy Center piece from the Task Force on Terrorism and Ideology that “many experts predict that the decline of the Islamic State’s territorial caliphate will lead it to redouble its efforts in the digital realm, seeking to remotely inspire and direct violence in the West.” Despite the nuances in articulation, each characterization agrees that the internet should be a priority for national security practitioners.

Security experts recognize that this prioritization has profound implications on policing efforts. Spence and Gardham frame the issue as a paradigm shift—historically,

---


stakeouts, wiretaps, and letter intercepts were sufficient tools to gain intel on potential terrorists. Terrorists’ use of the internet has changed that notion. Domestically, LEAs are using social media for investigations. The 2016 Annual Social Media Survey by the International Association of Chiefs of Police reports that 70 percent of the 539 agencies responding use social media for intelligence gathering. The trend internationally is similar. The Australian government, however, says that social media creates a significant challenge. France has made it a priority to strengthen its efforts in cyberspace. According to Public Security Minister Gilad Erdan in 2018, Israel thwarted over 200 Palestinian terrorist attacks by using intelligence gathered on social media platforms. Consensus exists among the security experts that the internet has changed policing.

In 2012, Omand et al. appear to have introduced the term SOCMINT and argued for its inclusion in the intelligence framework. The security experts now contend that SOCMINT is “integral” to ensuring national security. Marzell explains SOCMINT’s fit in the wider intelligence mix and its “essential” role in informed decision making.

---

76 Spence and Gardham, “How Jihadists ‘Go Dark’ to Avoid Detection.”
77 Kim, Oglesby-Neal, and Mohr, 2016 Law Enforcement Use of Social Media Survey, 3.
80 Times of Israel, “Police Minister.”
81 Omand, Bartlett, and Miller, “Introducing Social Media Intelligence (SOCMINT),” 801.
82 Akhgar, “OSINT as an Integral Part of the National Security Apparatus,” 3; Marcellino et al., Monitoring Social Media, 14.
Akhgar, Staniforth, and Taipale go as far as to contend that using SOCMINT in the fight against terrorism is “mandatory” or part of the “duty” to safeguard the homeland.84

Security experts in the United Kingdom (UK) view the terrorists’ use of the internet as a global risk that affects its security daily and directly.85 In 2016, the UK’s Centre of Excellence in Terrorism, Resilience, Intelligence & Organised Crime Research (CENTRIC) launched the Open-source Intelligence (OSINT) Hub, “which has been gaining momentum as a physical and virtual space for the operational exploitation, dissemination, and development of CENTRIC capabilities.”86 The OSINT Hub’s secure physical environment facilitates collaboration between investigators, the CENTRIC team and their tools, and developers who seek input for creating future capabilities.87 The UK pursued a collaborative approach to tool development with reTriEval and aNalysis of heterogeneous online content for terrOrist activity Recognition (TENSOR) and Detecting and ANalysing TEErrorist-related online contents and financing activities (DANTE). The UK partnered with different countries, different LEAs, academia, and industry forming consortiums and using advisory boards.

One apparent gap in the security expert literature concerns the role SOCMINT plays in immigration. Karasek argues that immigration officials have an advantage in the SOCMINT terrorist discovery endeavor—the officials have relatively complete and reliable sets of personal data submitted by the applicants themselves on immigration

86 Akhgar, “OSINT as an Integral Part of the National Security Apparatus,” 8.
87 Akhgar, 8.
forms. Thus, the security experts agree SOCMINT has significant value, but some minor variance exists among experts concerning the extent of that value.

3. Critics

The literature from those who object to SOCMINT, the critics, can be parsed into three camps—those who object because the effort has been problematic and is unnecessary, those who object on efficacy grounds, and those who object because of data and constitutional concerns. The first group in the critics’ camp contends that DHS’ efforts to develop a SOCMINT capability have been problematic and that it is unnecessary. Patel et al. argue that the prior DHS SOCMINT efforts are an inadequate basis to expand the initiative. The authors allege that DHS’ efforts were problematic because the efforts did not evaluate effectiveness, lacked policies and procedures, and found little value from the undertaking. Bier argues that vetting failures are infrequent, especially after 9/11. He provides a detailed analysis to make the case that the United States is safe enough and that new vetting initiatives are unnecessary. Inserra also dismisses the risk from those abroad. He posits:

Given that since the start of 2015, all 30 Islamists plots and attacks against the U.S. homeland have involved a homegrown terrorist, the U.S. must not shift resources away from countering such threats in order to start broad social media vetting efforts.

---


90 Patel et al., 31.


92 Bier.

93 Inserra, “The U.S. Should Tread Carefully on Social Media Vetting.”

94 Inserra.
Patel et al. challenge the notion that value exists in focusing resources on this initiative based on a low hit rate in previous efforts.Absent from these three views is the reality that the war against terrorism is dynamic. What worked yesterday may not work in the future. Sagarin agrees with this non-stasis view and asserts that the answer to security threats lies in understanding nature, specifically adaptability because terrorism threats are constantly evolving. McChrystal, the former Commander of the Joint Special Operations Command and former Commander of U.S. forces in Afghanistan, contends it is futile to rely on historic principles in wars where a unique enemy and innovations are at play. This disagreement is a critical because if the absence of risk forecloses SOCMINT’s necessity, the efficacy and data and constitutionality questions become irrelevant.

The second group in the critics’ camp takes issue with the efficacy of SOCMINT. The American Civil Liberties Union (ACLU) fears SOCMINT vetting will slow down visa processing. The ACLU also argues there is “no reason to believe collecting and retaining this kind of social media information will improve our security.” The ACLU asserts, “Anyone actually engaged in terrorism will simply take additional steps to hide their communications, making this information collection ineffective.” The ACLU warns of the subjectivity of social media vetting and the lack of transparency and redress for benefit denials. The Electronic Privacy Information Center (EPIC) contends SOCMINT potentially causes irreversible harm and tells the story of a Facebook algorithm erroneously machine translating the Arabic post “good morning” to “attack

---

98 Shakir and Waheed, “ACLU Comment on State Department Notices,” 1.
99 Handeyside, “The Many Problems with the Trump Administration’s Plan to Hold on to Some Immigrants’ Social Media Posts.”
100 Shakir and Waheed, “ACLU Comment on State Department Notices,” 9.
101 Shakir and Waheed, 5.
them” and “hurt them.” However, EPIC neglected to disclose that the mishap occurred because the Israeli police failed to consult an Arabic speaker to confirm the machine translation prior to the arrest. Inserra contends that the United States’ use of social media for vetting “may be unwise because of retaliatory or reciprocal actions taken by other countries” that may demand social media information of travelers from the United States. Inserra also argues that based on events, such as the breach of the Office of Personnel Management, travelers to the United States would have substantial cause to be apprehensive about the security of their social media data once in the government’s hands.

The last group in the critics’ camp warns of data and constitutional concerns. Patel et al. raise concerns that SOCMINT data use, retention, and sharing will risk data misinterpretation. The ACLU asserts that using SOCMINT to vet immigrants raises constitutional concerns regarding the rights to due process, free speech and expression, and it impacts the privacy of millions of people living in the United States, including U.S. citizens. Levinson raises concerns about SOCMINT and the First, Fourth, and Fourteenth Amendments, but is silent on SOCMINT’s use for immigration vetting. EPIC echoes the others’ concerns on privacy and civil liberties being at risk in a number of scenarios including immigration vetting. Patel et al. raise efficacy, data, and constitutional concerns. Marthews and Tucker present a paper arguing that a chilling

---


104 Inserra, “The U.S. Should Tread Carefully on Social Media Vetting.”

105 Inserra.


107 Shakir and Waheed, “ACLU Comment on State Department Notices,” 1; Handeyside, “The Many Problems with the Trump Administration’s Plan to Hold on to Some Immigrants’ Social Media Posts.”


effect occurs in Google search behavior based on increased awareness of government surveillance.\textsuperscript{111} Mund explores government monitoring of social media in Fourth Amendment terms.\textsuperscript{112} In an ACLU Freedom of Information Act (FOIA) request, Handeyside and Cagle contend that DHS’ social media screening lacks protections against discrimination and profiling and warn of the risks of abuse.\textsuperscript{113} The purported constitutional concerns have caused strong opposition by the critics.

\section*{E. RESEARCH DESIGN}

This thesis explores the necessity and efficacy of open-source SOCMINT in identifying potential fraud, public safety, and/or national security concerns (threats) from immigrants seeking immigration benefits from USCIS. This study contributes to the research literature in the field by filling the gap in the literature on open-source SOCMINT threat detection necessity and efficacy among immigrants seeking immigration benefits. A mixed-method research approach is used in this thesis that is both quantitative and qualitative. This approach assists in answering the research question and related questions, and evaluating the underlying evidence supporting those answers. This research is both theoretical and applied. It is theoretical in the sense that it explores the critics’ beliefs and assumptions concerning their objections to SOCMINT. This research is applied because it explores how USCIS can use SOCMINT to assist in fulfilling its mission.

Data is collected from open-sources for both the quantitative and qualitative facets of this research. In order to gain better insight into the viability of using SOCMINT to identify threats among immigration benefit seekers, quantitative data from the Profiles of Individual Radicalization in the United States (PIRUS) dataset is used. The PIRUS dataset contains “deidentified individual-level information on the backgrounds, attributes, and radicalization processes of over 2,100 violent and non-violent extremists who adhere

\begin{itemize}
\item \textsuperscript{111} Alex Mathews and Catherine Tucker, “Government Surveillance and Internet Search Behavior,” Social Science Research Network Electronic Journal, February 17, 2017, 40, \url{https://dx.doi.org/10.2139/ssrn.2412564}.
\item \textsuperscript{112} Mund, “Social Media Searches,” 241.
\item \textsuperscript{113} Handeyside and Cagle, “Freedom of Information Act Request,” 3.
\end{itemize}
to far right, far left, Islamist, or single issue ideologies in the United States covering 1948–2017,” which was coded entirely using information from public sources. Access to the full PIRUS downloadable dataset was acquired by completing an end user license agreement with the University of Maryland. A public, limited version of the PIRUS dataset is also available online for use with the Keshif data visualization tool as shown in Figure 11 in the Appendix.

To gain better insight on the arguments for and against SOCMINT, qualitative data is used. This qualitative data is secondary source data on the issue rhetoric—the debate and discussion—between the critics and supporters of implementing SOCMINT. This rhetoric exists in the open-source literature, e.g., books, scholarly journals, articles, news stories, FOIA-released documents, and government reports and memorandums. The collection of the issue rhetoric data is limited to the post-San Bernardino attack literature, spanning the period of December 22, 2015 to May 22, 2019. The research also includes pre- and post-San Bernardino literature that contains general, non-issue rhetoric insights on SOCMINT. Collectively, the research literature includes over 150 sources.

The method used to analyze the data varied by the data type, quantitative and qualitative. For the quantitative data, the narrow scope and reasonable size of the PIRUS dataset eliminated the need for Statistical Package for the Social Sciences data analysis. Instead, the author was able to use Microsoft Excel’s sort, filter, count, and sum features to manipulate and graph the raw data. The author confirmed the dataset did not contain any outliers or missing data values. The existing PIRUS coded variables were sufficient for the thesis research. All coded variables and their associated response values were defined based on the October 2018 public release version of the PIRUS Codebook.

Compound aggregating and excluding filters were applied among the coded variables. These filtering rules are explicitly stated in Chapter II’s PIRUS variable analysis sections 7(a)–(i). As the research focuses on radicalized immigrants who would have interacted with the lawful immigration process, the “Residency_Status” variable

---

was used to eliminate U.S.-born subjects and those who were undocumented residents. The details of any exclusion and revision to the subject population and filtered sub-populations are explicitly stated in Chapter II’s PIRUS variable analysis sections 7(a)–(i). When coded variable data values were reported as “unknown,” those cases were excluded from the analysis. These exclusions are explicitly stated in Chapter II’s PIRUS variable analysis sections 7(a)–(i). When data values were logically unresponsive to specific questions, e.g., internet analysis before 1995 and social media analysis before 2005, those cases were excluded from the analysis. These exclusions are explicitly stated in Chapter II’s PIRUS variable analysis sections 7(a)–(i).

For the qualitative data, the specific objections of the critics were identified and attributed. The objections were grouped by type, e.g., problematic effort, necessity, efficacy, data concerns, and constitutional concerns. The evidence that the critics provide for each objection is presented. The evidence supporting each objection is traced to its original source. Any direct contradictions in the evidence are identified and the contradictions cited, often in direct quotes to eliminate any potential interpretive bias from paraphrasing. The author identifies when select statements offered by the critics as supporting evidence are taken in isolation and ignore broader contradicting context. In addition, direct quotes are used liberally to eliminate any potential interpretive bias from paraphrasing. Using the identified contradictions and other scholarly research, rebuttals to the critics’ objections are proffered.

The mixed-method research approach was beneficial. The quantitative methodology was ideal for measuring and identifying patterns among the PIRUS cases. The methodology provided a practical, evidence-grounded means to gain insight into radicalized immigrants’ use of the internet and social media in plotting violent attacks and the potential for threat detection. The qualitative methodology was ideal for interpreting and gaining fact-based insight on the critics’ objections and offering plausible rebuttals. Collectively, the quantitative and qualitative methods provided answers to the central research question and related questions. The methods facilitated a deeper understanding of SOCMINT and provided a framework for analyzing the merit of the critics’ objection narratives.
F. CHAPTER OVERVIEW

Chapter II describes the USCIS mission and the authorities permitting SOCMINT. The chapter provides insight into how terrorists, in general, use social media and the experts’ assessments of it as a tool. The PIRUS section examines radicalized immigrants’ social media use. The chapter contemplates open-source necessity, current law enforcement use, and SOCMINT success stories.

Chapter III introduces the issue rhetoric as objections from those in the first camp of critics in the literature review. The chapter details why the critics label SOCMINT problematic based on the Office of the Inspector General (OIG) report and FOIA-released documents. The chapter explores the claim that SOCMINT is not necessary because the United States is safe enough. The chapter explains how the objections, if not overcome, make the case for not using SOCMINT. The chapter analyzes each of the objections and the supporting evidence offered by the critics. Where available, the chapter provides rebuttals to the specific objections of those opposing SOCMINT. The rebuttals derive from a detailed analysis of the OIG and FOIA-released documents’ text cited by the critics and other open-source government documents.

Chapter IV analyzes the efficacy issues identified in the second camp of critics. The chapter examines each of the objections and the supporting evidence offered by those who object to SOCMINT on efficacy grounds. The chapter informs how the merits of the objections affect the propositions for SOCMINT. The chapter relies on quantitative analysis of the PIRUS dataset, experts’ opinions, a detailed analysis of the OIG and FOIA-released documents’ text cited by the critics, and other open-source government documents to provide counterarguments, where feasible.

Chapter V addresses the data and constitutional concerns identified by those in the last camp who oppose SOCMINT. Each of the objections and supporting evidence are evaluated on their merit. The chapter describes how the objections, if not overcome, persuade against using SOCMINT. Rebuttals that stem from open-source government documents detailing DHS policy, procedure, and training are offered.
Chapter VI presents recommendations and conclusions based on the propositions for SOCMINT and the analysis of objections and rebuttals contained in Chapters III through V. The chapter synthesizes the propositions for SOCMINT and the objections to it into legal, ethical, implementation, technology, and organizational recommendations. The chapter concludes by proposing facets of SOCMINT warranting further study.
II. PROPOSITIONS FOR SOCMINT

Before the advent of the internet, extremists had to peddle hate on the street corner or through phone conversations to convince people to accept literature or attend meetings. Now, hate and terrorist propaganda can easily be posted on blogs or social media where it spreads exponentially and has immeasurable impact.

—Samuel G. Estes, author, *Hate: The Shared Heritage of International and Domestic Extremism*

For terrorists this struggle isn’t about how many terrorists exist today; it’s about how many will be created tomorrow. Their recruitment efforts entirely depend on how we act.

—Mike German, author, *Thinking Like a Terrorist: Insights of a Former FBI Undercover Agent*

Proposition: An open-source SOCMINT gathering and analysis capability will critically assist USCIS in accomplishing its homeland security mission.

Assessing this claim requires understanding the context and environment within which USCIS operates. First, a SOCMINT capability must advance the objectives of USCIS’ mission. Second, USCIS must operate under legal authorities that allow SOCMINT. Third, social media needs to be a fertile source for threats. Fourth, the open-source information discovered using SOCMINT should not be taken for granted in efforts to identify threats. Fifth, while not entirely determinative of USCIS’ SOCMINT success, it is beneficial if other LEAs also operate in this space, which indicates viability and provides opportunities for partnering and sharing best practices. Lastly, the SOCMINT endeavor must be capable of moving beyond threat identification to successful intervention. A review of these considerations reveals that SOCMINT can offer a significant contribution to USCIS’ efforts to fulfill its homeland security mission.
A. MISSION

Identifying fraud, public safety, and/or national security threats is central to achieving the USCIS mission. The SOCMINT initiative should complement the objectives of the USCIS mission. USCIS “administers the nation’s lawful immigration system, safeguarding its integrity and promise by efficiently and fairly adjudicating requests for immigration benefits while protecting Americans, securing the homeland, and honoring our values.”\(^{115}\) In 2004, USCIS formed the FDNS directorate to enhance the integrity of the U.S. immigration system and to safeguard against individuals receiving or eligible to receive immigration benefits that may constitute a threat to national security and/or public safety.\(^{116}\) Immigration benefit fraud prevention also falls within the FDNS mandate.\(^{117}\) Individuals who constitute a national security and/or public safety threat may use fraud in an attempt to hide their identity, immigration history, criminal history, person and group associations, immigration benefit eligibility issues, etc.

Internally, to carry out FDNS directives, FDNS immigration officers (IOs) work with Field Operations Directorate adjudications immigration services officers (ISOs).\(^{118}\) IOs are tasked with performing administrative inquiries regarding suspected benefit fraud and assisting with the resolution of criminal or national security concerns.\(^{119}\) Therefore, IOs conduct administrative investigations to identify pertinent information necessary to provide sound adjudication decisions.\(^{120}\) IOs report their investigative findings to the ISOs who make the final adjudicative decisions in granting immigration benefits.\(^{121}\)

\(^{115}\) U.S. Citizenship and Immigration Services, “About Us.”


\(^{117}\) U.S. Citizenship and Immigration Services Office of Privacy, 1.

\(^{118}\) U.S. Citizenship and Immigration Services Office of Privacy, 2.

\(^{119}\) U.S. Citizenship and Immigration Services Office of Privacy, 4.

\(^{120}\) U.S. Citizenship and Immigration Services Office of Privacy, 2.

\(^{121}\) U.S. Citizenship and Immigration Services Office of Privacy, 2.
IOs and ISOs collaborate to investigate fraud, public safety, and/or national security concerns thoroughly before USCIS grants immigration benefits.\textsuperscript{122}

Externally, FDNS serves as the principal conduit for collaboration and information sharing among other state and federal government agencies.\textsuperscript{123} As the 9/11 Commission contends, information sharing is critical to connecting the dots.\textsuperscript{124} FDNS is the liaison between USCIS and the intelligence and law enforcement agencies.\textsuperscript{125} This role requires collaboration to ensure that fraudsters, criminals, and terrorists who pose a threat to the integrity of the system, public safety, and/or national security cannot “exploit the immigration system to gain access to, or remain in, the United States.”\textsuperscript{126}

In performing these internal and external functions, FDNS consults various publicly available and open source internet-based resources during its investigations.\textsuperscript{127} These sources include the “internet, social media, news feeds, and state and local public records.”\textsuperscript{128} Access to these resources allows the IOs to verify personal, biographical, historical, and financial information and to identify potential immigration benefit fraud, public safety, and/or national security concerns.\textsuperscript{129} As social media is a potentially rich source of information on applicants, beneficiaries, and petitioners, it may provide IOs with indicators of potential fraud, public safety, and/or national security threats contemplated by the USCIS mission.

\textsuperscript{122} U.S. Citizenship and Immigration Services Office of Privacy, 2.
\textsuperscript{123} U.S. Citizenship and Immigration Services Office of Privacy, 2.
\textsuperscript{126} U.S. Citizenship and Immigration Services Office of Privacy, 2.
\textsuperscript{127} U.S. Citizenship and Immigration Services Office of Privacy, 13.
\textsuperscript{128} U.S. Citizenship and Immigration Services Office of Privacy, 13.
\textsuperscript{129} U.S. Citizenship and Immigration Services Office of Privacy, 13.
B. LEGAL AUTHORITIES

USCIS has the legal authority to operate a SOCMINT capability. FDNS’ collection and analysis of social media data used for adjudicating immigration benefits must meet its security needs, but must also be permissive under U.S. law. The authority to accomplish these ends derives from the INA and delegations from the Secretary of Homeland Security. The INA, 8 U.S.C. § 1101, et seq. grants USCIS the authority to adjudicate immigration benefits. The Secretary delegated USCIS the authority to administer the immigration laws, investigate alleged civil and criminal violations of the immigration laws, make prosecutorial recommendations, maintain files and records systems, interrogate aliens, issue subpoenas, administer oaths, and take and consider evidence. The Appropriations Act of 2005 authorizes USCIS to conduct background and law enforcement checks on applicants, beneficiaries, and petitioners before granting immigration benefits. Collectively, these authority grants provide the legal basis for allowing FDNS IOs to search open-source internet and social media information while conducting administrative inquiries.

C. TERRORISM ON SOCIAL MEDIA

Social media is a fertile domain to identify fraud, public safety, and/or national security threats. Spence and Gardham frame the issue as a paradigm shift—historically, stakeouts, wiretaps, and letter intercepts were sufficient tools to gain intel on potential terrorists. Terrorists’ use of the internet has changed that notion. Terrorists use the internet to disseminate propaganda, solicit new members, communicate, gather

---


133 Spence and Gardham, “How Jihadists ‘Go Dark’ to Avoid Detection.”
intelligence, seek money, and inspire and plan attacks. A review of some specific examples of how terrorists have used the internet indicates support for the claim that FDNS should not be overlooking social media in its quest to identify fraud, public safety, and/or national security threats.

1. Propaganda

A long established and growing trend of terrorist propaganda has appeared on social media. Pro-al-Qaeda supporters created their first website in the 1990s. In mid-2015, ISIS produced “38 individual batches of propaganda each day,” which concentrated on various themes, such as “victimhood, war, and utopia,” with lesser themes involving “mercy, belonging, and brutality.” A review by Bloomberg Businessweek shows that “at least a dozen U.S.-designated terror groups maintain a presence on Facebook” including “Hamas and Hezbollah in the Middle East, Boko Haram in West Africa, and the Revolutionary Armed Forces of Colombia.” In the first quarter of 2018, Facebook identified almost two million pieces of al-Qaeda and ISIS material, nearly double the amount in the previous quarter. In the last two quarters of 2017, Twitter banned almost 275,000 accounts for promoting terrorism. Terrorist propaganda on social media potentially presents FDNS an opportunity to identify fraud, public safety, and/or national security threats.

---

134 Coats, Worldwide Threat Assessment of the U.S. Intelligence Community, 6.
135 Bickert and Fishman, “Hard Questions: How Effective Is Technology in Keeping Terrorists Off Facebook?”
138 Bickert and Fishman, “Hard Questions: How Effective Is Technology in Keeping Terrorists Off Facebook?”
139 Twitter Public Policy, “Expanding and Building #TwitterTransparency.”
2. Communication

Aside from generalized propaganda, terrorists use social media to communicate directly. In 2018, the Federal Bureau of Investigation (FBI) said “its investigation found that [Waheba Issa] Dais used hacked social media accounts to discuss possible attacks with self-proclaimed members of the IS [Islamic State].”140 The FBI reported, “Dais suggested using the deadly toxin ricin in a government building or a reservoir somewhere in the U.S. during one of her conversations with an informant.”141 Also, “she suggested street festivals and summer celebrations as possible targets.”142 Such dialog on social media potentially offers FDNS a means to identify fraud, public safety, and/or national security threats.

3. Recruiting

Social media exponentially extends the communication reach of users, which can play a critical role in recruiting. A Saudi program, the Sakina Campaign for Dialogue, scrutinized the Twitter accounts of Saudis who back extremist groups, and based on the analysis of 200 Twitter accounts and hashtags related to the Islamic State and al-Qaeda in Saudi Arabia, uncovered a “dangerous movement” organized by Saudis supporting the militant groups on Twitter.143 The campaign director stated, “An average of 90 tweets per minute (129,600 per day) call for violence, to join terrorist groups, to attack others verbally or physically, or to destabilize security.”144 The flurry of recruiting efforts on social media may assist FDNS in its mission to thwart fraud, public safety, and/or national security threats.


141 Moreno.

142 Moreno.


4. Radicalization

Social media recruiting plays a decisive role in radicalization. In 2014, social media was “cited prominently in the FBI’s criminal complaint” for terrorist Nicholas Teausant.145 Teausant posted “pictures under the name ‘bigolsmurf,’ declaring his desire to ‘join Allah’s army’ and seeking ‘The Mujahid’s Handbook,’ identified by the FBI as a ‘how-to guide for becoming a lone wolf terrorist,’ compiled from Al Qaeda’s Inspire magazine.”146 On ask.fm, a question and answer social network platform, “he allegedly told strangers of his desire to ‘go fight in Syria.’”147 Daveed Gartenstein-Ross, an assistant professor in Georgetown University’s security studies program said, “You can really trace this guy’s evolution through his social media postings, you can see exactly what he was thinking during parts of his radicalization, it’s really striking.”148 Signals of radicalization on social media may help FDNS uncover fraud, public safety, and/or national security threats.

5. Plotting

Social media can aid terrorists in planning attacks, both for materials acquisition and tactics discovery. In 2016, “[b]efore Ahmad Khan Rahami planted bombs in New York and New Jersey, he bought bomb-making materials on eBay” and “linked to jihad-related videos from his public social-media account.”149 In 2017, Uzbek immigrant Sayfullo Saipov was “charged with the death of eight people after ploughing into them with a truck in downtown Manhattan.”150 Saipov is also “‘accused of providing material support and resources’ to the terror group ISIS.”151 John Miller, the New York Police

---

145 Serwer, “Accused Student Terrorist.”
146 Serwer.
147 Serwer.
148 Serwer.
150 Patrikarakos, “Social Media Networks Are the Handmaiden.”
151 Patrikarakos.
Department’s Deputy Commissioner of Intelligence and Counterterrorism, told reporters that “Saipov appeared to have followed almost exactly to a ‘T’ the instructions that ISIS has put out in its social media channels before, with instructions to their followers on how to carry out such an attack.” How terrorists use social media for planning potentially presents FDNS an opportunity to identify fraud, public safety, and/or national security threats.

6. Experts

Security experts agree about the viability of using SOCMINT to identify terrorists. Nick Rasmussen, former Director of the National Counterterrorism Center, believes, “Increasingly, what connecting the dots means to me is dealing with the huge, huge volume of publicly available or open source or unclassified information that’s out there that may have terrorism relevance.” William Roper, former Director of the DoD’s Strategic Capabilities Office said, “Data is going to be the fundamental fuel for national security in this century.” Isaac Porche, a Research and Development Corporation (RAND) researcher, argues “the potential is huge, especially if the information can be combined with other databases.” The aforementioned examples and the experts’ assertions leave little doubt that a potential opportunity exists to identify terrorists on social media.

7. Profiles of Individual Radicalization in the United States

The experts and the previous examples support the notion that terrorists use social media and an opportunity exists to intervene, but this offers little insight on FDNS’ principal focus, immigrants. PIRUS, a project by the National Consortium for the Study of Terrorism and Responses to Terrorism (START), is somewhat instructive on the nexus

152 Patrikarakos.
154 Strohm, “Predicting Terrorism.”
155 Duncan, “Social Media Is a Rich Source.”
between immigrants and use of the internet and social media in the terrorism context. PIRUS is a dataset that “contains deidentified individual-level information on the backgrounds, attributes, and radicalization processes of over 2,100 violent and non-violent extremists who adhere to far right, far left, Islamist, or single issue ideologies in the United States covering 1948–2017.” The PIRUS dataset leads to some conclusions regarding the role the internet and social media played in the radicalization and terrorist plots of immigrants.

a. Radicalized Immigrants

A small percentage of individuals who have radicalized have had contact with the lawful immigration system. This phenomenon is important because it indicates FDNS may have an opportunity to identify fraud, public safety, and/or national security threats among immigration benefit seekers. The PIRUS variable “Residency_Status” reports, “What was the individual’s residency status in the United States at the time of exposure?” In this context, exposure means the date the “activity/plot first came to public attention...usually time of incident or arrest, or earliest mention of individual in sources, so long as these are related to the plot/radicalization.” The residency status variable’s categorical descriptors include Born Citizen, Naturalized Citizen, Legal [sic]

156 “About PIRUS,” National Consortium for the Study of Terrorism and Responses to Terrorism, accessed June 8, 2019, https://www.start.umd.edu/data-tools/profiles-individual-radicalization-united-states-pirus. “The bulk of data collection for PIRUS was supported by the National Institute of Justice, Office of Justice Programs, Department of Justice, through Award Number 2012-ZA-BX-0005. In addition, an effort to review and update information in the PIRUS dataset has been supported with funding from the Department of Homeland Security through the Center for the Study of Terrorism and Behavior (CSTAB) Partner grant. The PIRUS dataset and any findings derived from the dataset do not represent the official positions of the National Institute of Justice, the Department of Justice, the Department of Homeland Security, or any other funding agency.” “PIRUS—Frequently Asked Questions,” National Consortium for the Study of Terrorism and Responses to Terrorism, accessed August 12, 2019, https://www.start.umd.edu/pirus-frequently-asked-questions.

157 “Profiles of Individual Radicalization in the United States (PIRUS),” National Consortium for the Study of Terrorism and Responses to Terrorism (START).


159 National Consortium for the Study of Terrorism and Responses to Terrorism, 8.
The subjects in this population of particular interest to FDNS are those who would have had interaction with the lawful immigration process. Eliminating subjects whose residency status is unknown reduces the PIRUS dataset’s population from 2,148 to 2,024. Filtering out the subjects who were U.S.-born and those who were undocumented residents further revises the population size to 206. Therefore, 206 of the 2,024 subjects (10.18 percent), hereinafter “radicalized immigrants,” interacted with the lawful immigration system, as shown in Figure 1.

![Figure 1. Residency status of the radicalized at the time of exposure](image)

The PIRUS dataset’s focus on subjects who radicalized within the United States does not foreclose applying conclusions from this dataset to subjects seeking entry into the United States, which is the focus of USCIS’ SOCMINT efforts. The 206 radicalized immigrants radicalized within the United States, but the subjects would have had multiple contacts with USCIS after arriving as they progressed through the immigration benefit system, from lawful permanent resident to naturalized citizen. In addition, the “External_Rad” variable reports, “Did any latter period of the individual’s radicalization

---

160 National Consortium for the Study of Terrorism and Responses to Terrorism, 30.

161 Adapted from National Consortium for the Study of Terrorism and Responses to Terrorism (START), “Profiles of Individual Radicalization in the United States (PIRUS).”
occur outside the United States?" The results of this query are known for 114 of the 206 radicalized immigrants. Research indicates, “at least some part of the radicalization process occurred outside the United States” for 44 of the subjects (38.6 percent), as shown in Figure 2. The external radicalization and contact with USCIS makes the subjects in the PIRUS dataset reasonably analogous to the subjects of SOCMINT’s focus.

![Figure 2. Location of latter period radicalization](image)

**b. Internet Radicalization**

The internet played a significant role with the aforementioned 206 radicalized immigrants. Secondary research with the PIRUS dataset supports this conclusion. This finding is relevant because use of the internet in the radicalization process may create an opportunity for FDNS to identify fraud, public safety, and/or national security threats. The “Internet_Radicalization” variable reports, “What role did the internet play in the individual’s radicalization?” Adjusting for radicalization that occurred before 1995 and cases in which the internet’s role in radicalization is unknown reduces the 206

---

162 National Consortium for the Study of Terrorism and Responses to Terrorism, Profiles of Individual Radicalization in the United States (PIRUS) Codebook, 23.

163 National Consortium for the Study of Terrorism and Responses to Terrorism, 23.

164 Adapted from National Consortium for the Study of Terrorism and Responses to Terrorism (START), “Profiles of Individual Radicalization in the United States (PIRUS).”

165 National Consortium for the Study of Terrorism and Responses to Terrorism, Profiles of Individual Radicalization in the United States (PIRUS) Codebook, 17–18.
radicalized immigrant subpopulation to 118 subjects. Isolating the “Internet_Radicalization” variable reveals that the “Internet played a role but was not the primary means of radicalization (e.g., internet resources were used to reaffirm or advance pre-existing radical beliefs)” in 72 of 118 of the subjects (61.02 percent). Manipulating the “Internet_Radicalization” variable reveals that the “Internet was the primary means of radicalization for the individual (e.g., initial exposure to ideology and subsequent radicalization occurred online)” in 31 of 118 of the subjects (26.27 percent), as shown in Figure 3. The internet played at least some role for over a majority of the radicalized immigrants, which potentially creates an opportunity for threat identification.

Figure 3. Role of the internet in radicalization

Social Media Radicalization

Social media played a significant role with the aforementioned 206 radicalized immigrants. Secondary research with the PIRUS dataset supports this conclusion. While FDNS investigations do involve open-source content on the internet, the SOCMINT

166 The removal of the last restrictions on the use of the internet to carry commercial traffic in 1995 is generally considered the birth of the modern internet.

167 National Consortium for the Study of Terrorism and Responses to Terrorism, Profiles of Individual Radicalization in the United States (PIRUS) Codebook, 17–18.

168 National Consortium for the Study of Terrorism and Responses to Terrorism, 17–18.

169 Adapted from National Consortium for the Study of Terrorism and Responses to Terrorism (START), “Profiles of Individual Radicalization in the United States (PIRUS).”
initiative is more focused on open-source data from social media sites. Therefore, use of social media sites by radicalized immigrants may present an opportunity for FDNS to identify fraud, public safety, and/or national security threats. The “Social_Media” variable in the PIRUS dataset reports, “Is there evidence that online social media played a role in the individual’s radicalization and/or mobilization?” PIRUS defines online social media as “any form of electronic communication through which users create online communities to share information, ideas, personal messages, and other content, such as videos and images.” Adjusting for radicalization that occurred before 2005 and cases in which social media’s role in radicalization is unknown reduces the 206 radicalized immigrant subpopulation to 113 subjects. Isolating the “Social_Media” variable identifies that social media “played a role but was not the primary means of radicalization or mobilization” in 55 of the 113 subjects (48.67 percent), as shown in Figure 4. Analyzing the “Social_Media” variable reveals that social media “was the primary means of radicalization for the individual (e.g., initial exposure to ideology and subsequent radicalization occurred over online social media)” in 14 of the 113 subjects (12.39 percent), as shown in Figure 4. Social media played at least some role for 69, a majority, of the radicalized immigrants, which potentially creates an opportunity for threat identification.

---

170 National Consortium for the Study of Terrorism and Responses to Terrorism, Profiles of Individual Radicalization in the United States (PIRUS) Codebook, 18.
171 National Consortium for the Study of Terrorism and Responses to Terrorism, 18.
172 The PIRUS dataset does not report data on social media use before 2005.
173 National Consortium for the Study of Terrorism and Responses to Terrorism, Profiles of Individual Radicalization in the United States (PIRUS) Codebook, 18.
174 National Consortium for the Study of Terrorism and Responses to Terrorism, 18.
d. Internet Plotting by Social Media Users

The internet plays a role in terrorist plots for radicalized immigrants who use social media. The PIRUS variable “Internet_Use_Plot” contemplates if the “extremist activity involved a violent plot, did the individual use the internet for communications or logistics while preparing for and undertaking the plot?” For example, “using the internet to communicate with group members or other extremists, threatening targets, researching the target and tactics, and ordering supplies.” Coupling this variable with “Social_Media” may provide some insight on the extent of FDNS opportunities to intervene when radicalized immigrants who use social media also use the internet for plotting terrorist attacks. Adjusting the group size of the 69 radicalized immigrants that social media played at least some role in their radicalization to include only those subjects whose internet plot use was known and the plot occurred after 1995 reduces this group to 23 subjects. Isolating the “Internet_Use_Plot” variable identifies that 20 of the subjects (86.96 percent) used the internet in conjunction with their plot preparations,

Figure 4. Role of social media in radicalization

175 Adapted from National Consortium for the Study of Terrorism and Responses to Terrorism (START), “Profiles of Individual Radicalization in the United States (PIRUS).”
176 National Consortium for the Study of Terrorism and Responses to Terrorism, Profiles of Individual Radicalization in the United States (PIRUS) Codebook, 11.
177 National Consortium for the Study of Terrorism and Responses to Terrorism, 11.
178 The removal of the last restrictions on the use of the internet to carry commercial traffic in 1995 is generally considered the birth of the modern internet.
as shown in Figure 5. This finding supports that the internet is fertile ground for FDNS potentially to identify threats among radicalized immigrant social media users.

![Use of the internet for logistics or communication in preparation of a violent plot](image)

Figure 5. Use of the internet for logistics or communication in preparation of a violent plot\(^{179}\)

e. **Gravity of Threat from Social Media Users**

Radicalized immigrant social media users, regardless of internet plot use, pose a serious threat. Of this group of 69 subjects, one-third of the subjects were doers versus talkers. The variable “Extent_Plot,” explores, “If the individual’s extremist activity involved a violent plot, to what extent did the plot progress? I.e., how far did the planning and execution proceed?”\(^{180}\) The extent of the plot was known for the entire group of 69 radicalized immigrants that social media played at least some role in their radicalization. Seven of the 69 subjects (10.14 percent), the talkers, had a “Nebulous plot (general ideas only, threats made to targets in the absence of an [y] planning or preparation).”\(^{181}\) One of the 69 subjects (1.45 percent) “Attempted acquisition of materials for plot.”\(^{182}\) Eleven of the 69 subjects (15.94 percent) successfully acquired and possessed materials for their

---

\(^{179}\) Adapted from National Consortium for the Study of Terrorism and Responses to Terrorism (START), “Profiles of Individual Radicalization in the United States (PIRUS).”

\(^{180}\) National Consortium for the Study of Terrorism and Responses to Terrorism, *Profiles of Individual Radicalization in the United States (PIRUS) Codebook*, 11.

\(^{181}\) National Consortium for the Study of Terrorism and Responses to Terrorism, 11.

\(^{182}\) National Consortium for the Study of Terrorism and Responses to Terrorism, 11.
plot.\textsuperscript{183} Five of the 69 subjects (7.25 percent) attempted, but failed in executing their plot.\textsuperscript{184} Six of the 69 subjects (8.7 percent) successfully executed their plot.\textsuperscript{185} Collectively, 23 of the 69 subjects (33.33 percent), the doers, took action on carrying out their terrorist plots. The significant number of cases that posed a serious threat highlights the need for FDNS to deploy SOCMINT, as shown in Figure 6.

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{figure6.png}
\caption{Gravity of threat from social media users\textsuperscript{186}}
\end{figure}

\textbf{f. Operational Security}

Operational security efforts do not completely foreclose the opportunity to identify threats when a terrorist plot exists. FDNS efforts to identify fraud, public safety,

\textsuperscript{183} National Consortium for the Study of Terrorism and Responses to Terrorism, 11.
\textsuperscript{184} National Consortium for the Study of Terrorism and Responses to Terrorism, 11.
\textsuperscript{185} National Consortium for the Study of Terrorism and Responses to Terrorism, 11.
\textsuperscript{186} Adapted from National Consortium for the Study of Terrorism and Responses to Terrorism (START), “Profiles of Individual Radicalization in the United States (PIRUS).”
and/or national security threats are potentially frustrated by the operational security efforts of the nefarious to hide or conceal their plots. The “Op_Security” variable identifies, “If the individual’s first publicly known extremist activity involved a violent plot, did the individual attempt to hide or conceal preparation for the plot?”\(^{187}\) The operational security efforts are known for 20 of the 23 doers—those who took steps to execute their terrorist plots. Secondary research based on the “Op_Security” variable reveals that of the doers, two subjects (10 percent) were “openly vocal about the plot (discussed it with friends and associates, procured suspicious supplies—like explosives or weapons—without being discrete, etc.).”\(^{188}\) The PIRUS data indicates that four of the 20 subjects (20 percent) were “neither covert nor overt (did not discuss the plot openly or overtly procure supplies, but also did not attempt to hide activities).”\(^{189}\) The remaining 14 subjects (70 percent) “avoided discussion with friends and associates and used code words when discussing the plot, procured supplies through intermediaries or in areas outside place of habitation or target area, etc.).”\(^{190}\) Nonexistent or lax operational security practices may assist FDNS in identifying fraud, public safety, and/or national security threats, as shown in Figure 7.

\(^{187}\) National Consortium for the Study of Terrorism and Responses to Terrorism, Profiles of Individual Radicalization in the United States (PIRUS) Codebook, 10.

\(^{188}\) National Consortium for the Study of Terrorism and Responses to Terrorism, 10.

\(^{189}\) National Consortium for the Study of Terrorism and Responses to Terrorism, 10.

\(^{190}\) National Consortium for the Study of Terrorism and Responses to Terrorism, 10.
g. **Social Media Frequency**

Over a majority of radicalized immigrants used social media at least once a day for activities related to radicalization and/or mobilization. Arguably, the frequency of this type of activity may affect the likelihood that FDNS can detect a threat via SOCMINT. The “Social_Media_Frequency” variable reports, “If there is evidence that online social media played a role in the individual’s radicalization and/or mobilization, on average how often did the individual engage in social media-related activity related to radicalization and/or mobilization?”\(^{192}\) The variable categories include “Rarely (about once a month or less),” “Sporadically (about 2–3 times per month),” “Occasionally (about once a week),” “Frequently (about once a day),” and “Continually (multiple times per day).”\(^{193}\) PIRUS reports the social media frequency for 34 of the 206 radicalized immigrants, as shown in Figure 8. None of the subjects rarely used social media. Two of the subjects (5.88 percent) used social media sporadically. Eleven of the subjects (32.35 percent) occasionally used social media. Sixteen of the subjects (47.06 percent) had frequent social media use. Only five of the subjects (14.71 percent) continually used social media.

---

\(^{191}\) Adapted from National Consortium for the Study of Terrorism and Responses to Terrorism (START), “Profiles of Individual Radicalization in the United States (PIRUS).”


\(^{193}\) National Consortium for the Study of Terrorism and Responses to Terrorism, 19.
social media. Therefore, over 61 percent of the subjects used social media at least daily in a manner that related to radicalization and/or mobilization. This frequency may assist FDNS in identifying fraud, public safety, and/or national security threats.

Figure 8. Frequency of social media use related to radicalization or mobilization

h. Social Media Activities

The radicalized immigrants are not passive content consumers, which increases the need for SOCMINT. Passive content consumption of terrorism-related social media is not likely to trigger FDNS scrutiny via SOCMINT. However, more nefarious activities would. Consequently, the nature of social media activities affects the likelihood of threat detection. The “Social_Media_Activities” variable considers, “If there is evidence that online social media played a role in the individual’s radicalization and/or mobilization, which types of social media-related activities did the individual participate in?”

---

194 Adapted from National Consortium for the Study of Terrorism and Responses to Terrorism (START), “Profiles of Individual Radicalization in the United States (PIRUS).”

Adjusting for radicalization that occurred before 2005 and cases in which the social media activities were unknown reduces the 206 radicalized immigrant subpopulation to 63 subjects. The PIRUS dataset does not report data on social media use before 2005. Only three of the 63 subjects (4.76 percent) limited their activities to passive content consumption. Participation by “Disseminating content (i.e., sharing, spreading existing content)” was the most prevalent with a total of 41 of the 63 subjects (65.08 percent). Thirty-seven of the 63 subjects (58.73 percent) participated in extremist dialogue (i.e., creating unsophisticated content). Communicating directly with members of an extremist group to facilitate foreign travel accounted for 19 of the 63 subjects’ (30.16 percent) activity. The fourth most common activity, capturing 16 of the 63 subjects (25.40 percent), involved, “Directly communicating with members of extremist group(s) to establish relationship/acquire information on extremist ideology (no communication on specific travel plans or plot).” Fourteen of the 63 subjects (22.22 percent) created propaganda/content (e.g., creating extremist manifestos, propaganda videos, etc.). The act of “Directly communicating with members of extremist group(s) to facilitate domestic attack” came in last, with six of the 63 subjects (9.52 percent) engaged. The nature of social media activities indicates a plethora of activity that can potentially trigger SOCMINT scrutiny, as shown in Figure 9.

196 The PIRUS dataset does not report data on social media use before 2005.
197 National Consortium for the Study of Terrorism and Responses to Terrorism, Profiles of Individual Radicalization in the United States (PIRUS) Codebook, 20.
198 National Consortium for the Study of Terrorism and Responses to Terrorism, 20.
199 National Consortium for the Study of Terrorism and Responses to Terrorism, 20.
200 National Consortium for the Study of Terrorism and Responses to Terrorism, 20.
201 National Consortium for the Study of Terrorism and Responses to Terrorism, 20.
202 National Consortium for the Study of Terrorism and Responses to Terrorism, 20.
Figure 9. Social media activities

Adapted from National Consortium for the Study of Terrorism and Responses to Terrorism (START), “Profiles of Individual Radicalization in the United States (PIRUS).”
### Previous Criminal Activity

SOCMINT may provide FDNS an opportunity to identify threats that otherwise may go undetected during traditional immigration benefit processing. A central means FDNS uses to identify threats is querying immigration benefit seekers against government systems that hold criminal and intelligence records. If the subject had no previous criminal activity and consequently no previous arrests, this method may fail to identify a potential threat. Subjects with no previous criminal activity, but who use social media for nefarious purposes may expose themselves to FDNS SOCMINT threat identification efforts. The variable for “Previous_Criminal_Activity” reports, “Prior to their radicalization, does the individual have a history of involvement in non-ideologically motivated criminal activities?” The previous criminal activity was known for 57 of the 69 radicalized immigrants for whom social media played at least some role in their radicalization. Of this group of 57 subjects, 43 subjects (75.44 percent) had “No previous criminal activity,” as shown in Figure 10. SOCMINT may provide an opportunity to identify threats from subjects not contained in criminal databases.

![Figure 10. History of involvement in non-ideologically motivated criminal activities](image)

---

204 National Consortium for the Study of Terrorism and Responses to Terrorism, *Profiles of Individual Radicalization in the United States (PIRUS) Codebook*, 43.

205 National Consortium for the Study of Terrorism and Responses to Terrorism, 43.

206 Adapted from National Consortium for the Study of Terrorism and Responses to Terrorism (START), “Profiles of Individual Radicalization in the United States (PIRUS).”
D. OPEN-SOURCE NECESSITY

Leveraging open-source methods is a necessary tool in the fraud, public safety, and/or national security threat discovery effort. Terrorists have no qualms about using open-source platforms, nor should FDNS when protecting the homeland. An al-Qaeda training manual discovered in Afghanistan advised that 80 percent of the information needed for attacking an enemy could be found in open sources. Terrorists synthesize this research into instructions. The 600-page *Encyclopedia of Jihad* is widely circulated online and includes chapters, such as “how to kill,” “explosive devices,” “manufacturing detonators,” and “assassination with mines.” This example supports Nissen’s argument that terrorists have weaponized social media.

The Australian government describes the internet as “the command and control networks of choice for terrorists.” Some counterterrorism experts label the internet as a “terrorist university, a place where terrorists can learn new techniques and skills to make them more effective in their attack methodologies.” Governor Kean, former chairman of the 9/11 Commission, reports that “many experts predict that the decline of the Islamic State’s territorial caliphate will lead it to redouble its efforts in the digital realm, seeking to remotely inspire and direct violence in the West.” Harman argues, “The use of spies to gather human intelligence will become less valuable than open-source intelligence, especially information gleaned from social media.” Wilson contends, “Ninety percent of intelligence comes from open sources. The other ten percent, the clandestine work, is just the more dramatic. The real intelligence hero is

---

209 Nissen, #TheWeaponizationOfSocialMedia, 10.
212 Bipartisan Policy Center, “Digital Counterterrorism: Fighting Jihadists Online.”
Sherlock Holmes, not James Bond.”\textsuperscript{214} FDNS would be remiss in its efforts to secure the homeland if it ignored the necessity for detecting threats in open-source social media.

E. LAW ENFORCEMENT SOCMINT USE

LEAs are embracing the SOCMINT capability, which signals viability and provides opportunities for partnering and sharing best practices. State, local, federal, and international LEAs are using social media to identify potential terrorists. The 2016 Annual Social Media Survey by the International Association of Chiefs of Police reports that 70 percent of the 539 agencies responding use social media for intelligence gathering.\textsuperscript{215} In 2016, the White House sent representatives to meet with Silicon Valley executives about social media vetting.\textsuperscript{216} The Department of Defense (DoD) created Information Volume and Velocity, which scrapes social media, identifies trends, and provides troops with real-time information.\textsuperscript{217} SocioSpyder harvests and stores social media posts, maps connections between users, and identifies possible targets for FBI investigation.\textsuperscript{218} The Central Intelligence Agency’s Open Source Enterprise gathers and analyzes social media content.\textsuperscript{219} In 2018, the Department of State’s Bureau of Consular Affairs announced its intent to review social media data as a part of the vetting process for visas.\textsuperscript{220} USCIS is not the only DHS component with an interest in this capability. The Secret Service requested funding in 2016 to increase its monitoring of social media during the presidential election campaign.\textsuperscript{221} In 2017, Immigration and Customs Enforcement explored social media vetting at its extreme vetting industry day to enhance

\begin{itemize}
\item \textsuperscript{214} Statement by Lieutenant General Sam Wilson, USA Retired, former Director, Defense Intelligence Agency, reported by David Reed, “Aspiring to Spying,”\textit{Washington Times}, November 14, 1997.
\item \textsuperscript{215} Kim, Oglesby-Neal, and Mohr, \textit{2016 Law Enforcement Use of Social Media Survey}, 3.
\item \textsuperscript{216} Duncan, “Social Media Is a Rich Source.”
\item \textsuperscript{217} Duncan.
\item \textsuperscript{218} Handeyside, “To the Government, Your Latest Facebook Rant Is Raw Intel.”
\item \textsuperscript{219} Handeyside.
\item \textsuperscript{220} Cadman, “‘Extreme Vetting’ and Social Media Inquiries.”
\item \textsuperscript{221} Duncan, “Social Media Is a Rich Source.”
\end{itemize}
its capabilities. The National Fusion Center Association, with federal support, is managing an effort to share Real-time Open Source Analysis of Social Media (ROSM). Andrew Parker, the Director-general of MI5, Britain’s intelligence service, said, “Information gathered from the technology terrorists use, often in the same way as the rest of us, may sometimes be the only way to stop them. We use data to save lives.” A diverse cross section of LEAs is leveraging SOCMINT in the fight against terrorism. FDNS’ desire to deploy SOCMINT aligns with other agencies’ efforts and may provide opportunities for sharing SOCMINT tradecraft.

F. SOCMINT SUCCESSES

The previously articulated value propositions have transcended the theoretical and translated into real-word terrorism intervention successes based on SOCMINT. While critics have questioned the efficacy of using open-source SOCMINT to stop terrorism, proponents of the method have achieved results for years. Since 2012, shipping companies have used Twitter and Facebook posts by al-Shabaab affiliated Somali pirates to comprehend better how criminals target ships and plan their attacks. In 2015, a geotagged social media post by an enemy fighter alerted the U.S. Air Force and led to the bombing of an Islamic State in Iraq and the Levant headquarters building. Suspects’ publicly bragging of their plans before acting upon them has been a helpful roadmap of radicalization and benefit for LEAs. Suspects’ radicalizing in real-time and in plain sight on social media has led to FBI arrests related to the Islamic State. According to

---

222 Biddle and Woodman, “These Are the Technology Firms.”
224 Spence and Gardham, “How Jihadists ‘Go Dark’ to Avoid Detection.”
226 Everstine, “Carlisle.”
227 The Soufan Group, “TSG IntelBrief.”
228 The Soufan Group.
Public Security Minister Gilad Erdan in 2018, Israeli authorities have used SOCMINT to thwart over 200 Palestinian terror attacks.\textsuperscript{229} These examples are just a few that unequivocally support the claim that SOCMINT has progressed from theory to successful practice. SOCMINT’s success in identifying and mitigating threats will strengthen FDNS’ efforts to secure the homeland.

G. CONCLUSION

Deploying a SOCMINT capability will play a vital role in USCIS’ obligation to secure the homeland. A review of USCIS’ objectives, the terrorism-social media nexus, and SOCMINT’s viability validate this claim. Core to USCIS’ mission is protecting the homeland from fraud, public safety, and/or national security threats in the context of those seeking immigration benefits. USCIS has the legal authority to use SOCMINT in support of this mission. Evidence demonstrates that terrorists use social media in a variety of ways to achieve their nefarious ends, but the security experts identify opportunities for intervention. Research on radicalized immigrants’ interaction with social media and the internet demonstrates that this intervention is not only plausible in the immigration benefit context, but necessary. Open-source SOCMINT is capable of meeting this imperative. The variety of LEAs’ SOCMINT initiatives and their successes demonstrate this capability. These factors are strong propositions for SOCMINT. The next three chapters explore the arguments against USCIS’ use of SOCMINT, and whether and to what extent they should be of concern.

\textsuperscript{229} Times of Israel, “Police Minister.”
IIIIIII. SOCMINT PROBLEMATIC EFFORT AND NECESSITY
CONCERNS

I think this puts the lie to the idea that wide-scale automated social media
analysis is useful.

—Rachel Levinson-Waldman, Senior Counsel,
Liberty and National Security Program at the Brennan Center for Justice

We don’t know what they are looking for. And they don’t seem to know
either.

—Manar Waheed, Legislative and Advocacy Counsel,
American Civil Liberties Union

This chapter introduces the issue rhetoric as objections from those in the first
camp of critics in the literature review. Despite the propositions for SOCMINT, critics
assert the initiative will not assist USCIS in accomplishing its mission of securing the
homeland. These critics put forth a series of objections that call into question the
sensibility of USCIS efforts. First, those who argue against it allege the efforts to deploy
a SOCMINT capability to date have been fraught with problems. Second, they contend
that the program is unnecessary because the United States is safe enough. The merit of
these claims potentially challenges the propriety of the propositions for SOCMINT.
These arguments are two of the concerns that form the basis for the critics’ larger
collective claim that SOCMINT will undermine the USCIS mission.

Wells warns of the adverse effect on the public perceptions of SOCMINT
initiatives when the subjective narratives are not addressed.230 Ignoring the opposing
narratives and failing to engage the grievances and misconceptions fosters a lack of

Source Intelligence Investigation: From Strategy to Implementation, eds. Babak Akhgar, P. Saskia Bayerl,
and Fraser Sampson (Switzerland: Springer International Publishing AG, 2016), 57, http://dx.doi.org/
10.1007/978-3-319-47671-1.
Collectively, the critics’ opposing narratives flourish unchecked in an echo chamber of sorts. They reciprocally quote each other’s staff across the various articles they produce. The bulk of the critics’ arguments and evidence is based on references (direct quotes and cited paraphrases) to the OIG and FOIA-released documents, and their own other articles. Best and Cummings, however, warn of how the repetition from an echo effect can imbue a narrative with more importance and credibility than is warranted.

Some critics admonish DHS for failing to give a full picture and pledge to fill that alleged gap. However, the critics often cherry-pick selective report comments and ignore context. For example, the OIG report contains two parts—the OIG’s findings and DHS’ response. The critics wholesale ignore DHS’ response in their articles. Their oversights often directly contradict or undermine their arguments. Hence, much of this chapter focuses on the explicit text of the OIG and FOIA-released documents.

This chapter seeks to address the first two subjective narratives that oppose SOCMINT by interJECTing a new voice in the echo chamber. A voice that hones in on the OIG report’s explicit language to provide a deeper account of both sides—the OIG’s and DHS’—and looks broadly across the full context of the FOIA-released documents. Those documents contain more information than the critics represent. This deeper and broader review demonstrates that SOCMINT will assist USCIS in accomplishing its mission of securing the homeland. The following rebuttals provide insights into the first two of the critics’ series of objections that attempt to call into question the sensibility of USCIS SOCMINT efforts. First, the critics’ allegation that the efforts to deploy a SOCMINT capability to date have been fraught with problems is unconvincing. Second, the contention that the program is unnecessary because the United States is safe enough is debatable. The claims fail to challenge the propriety of the propositions for SOCMINT.

---

231 Wells, 58–63.


Collectively, these objections fail to form a convincing basis for the critics’ larger claim that SOCMINT will not assist with USCIS’ mission.

A. A PROBLEMATIC EFFORT

Those who do not support this concept allege that the efforts to deploy a SOCMINT capability to date have been fraught with problems. Due to the non-public nature of government activities, documents produced from FOIA requests are often proffered in assessing government programs. The critics offer excerpts from the DHS OIG 2017 report and FOIA-released documents to demonstrate that USCIS’ SOCMINT initiative is problematic. They argue that the extent of any problems encountered thus far in creating a SOCMINT capability foreshadows the future success of the endeavor. Absent evidence to the contrary regarding problems, the critics’ claims paint a troubled picture of the SOCMINT efforts to date.


The critics contend that the OIG’s report demonstrates that USCIS has encountered problems in its attempts to deploy SOCMINT. Those who argue against it seize upon select comments from the OIG as proof that problems plague the SOCMINT undertaking. Failing to establish appropriate policies, procedures, and metrics capable of objectively assessing the efforts and outcomes of the SOCMINT program may adversely affect program operations. If the critics’ assessments are reasonable, they indicate that SOCMINT is a problematic initiative for USCIS.

Patel et al.’s belief that the prior SOCMINT pilot programs are an inadequate basis to expand the effort is unconvincing.234 The authors’ conclusion tracks with the OIG’s report findings. The OIG based its “need increased rigor to ensure scalability and long-term success” conclusion on DHS’ alleged failure to adhere to the Government Accountability Office (GAO) “best practices for an effective pilot phase of a

---

program.” However, there is a problem—DHS did not in fact conduct any social media screening “pilots.”

Word choice matters, especially when a word such as pilot is a term of art. Pilots give the evaluator an opportunity to assess feasibility formally and refine the design before full-scale execution. Pilots are a means to try the innovation in real time and make sure that everything works for preparation to scale up to full production. Gardner clarifies that pilots are not research experiments or proof points that capabilities can be made to work. DHS made a critical word choice error by labeling its exploratory social media screening research activities as pilots. In addition, some personnel in DHS perpetuated that error by continuing, at times, to use the word “pilots” to describe DHS’ initial SOCMINT effort.

DHS recognized its error, albeit after the OIG’s investigation. Taylor, the Under Secretary for Intelligence and Analysis, Chief Intelligence Officer, Counterterrorism Coordinator, and Co-Chair of the DHS SMTF, explained DHS’ error to the Inspector General after the OIG released its draft report. According to Taylor, DHS’ pilots were not pilots, but instead were “research and development projects, referred to as ‘pilots,’ to assess the feasibility of developing such a capability.” Taylor clarified that “DHS chose to pursue these research projects and did not initiate fully operational pilots, as defined by the GAO, because the technology capable of processing DHS’ screening mission sets in a scalable manner was not yet available for such an endeavor to have been successful.” The DHS’ efforts “were designed to assess tool performance and advance


238 Gardner.

239 Roth, DHS’ Pilots for Social Media Screening, 9.

240 Roth, 9–10.
the technical capabilities for large-scale, automated social media screening,” not to serve as pilots amenable to assessing program efficacy. This tool assessment approach aligns with conventional wisdom from the experts.

The DHS word choice error had far-reaching consequences. The DHS’ mislabeling of the research and development projects as pilots and the OIG’s subsequent investigation erroneously evaluating them using pilot assessment standards resulted in the conclusion that activities that were not pilots had not performed adequately as pilots. The critics rely on the OIG findings to inform their arguments about SOCMINT’s viability. Patel et al.’s conclusion that the prior SOCMINT pilot programs are an inadequate basis to expand DHS’ SOCMINT efforts, however, is unsupported. The OIG’s mistaken conclusion actually undermines Patel et al.’s belief that prior SOCMINT pilot programs are an inadequate basis to expand.

Patel et al. also allege, “DHS has made no effort to evaluate [the pilots’] effectiveness.” This allegation, however, is problematic on three facets: a misplaced reliance, a flawed presumption, and omission of material facts. First, Patel et al.’s allegation relies on the OIG’s misleading pilot findings. The GAO explains that the pilot phase allows for an inquiry on whether “program operations” function as expected. However, for the reasons previously explained, DHS’ efforts had not advanced to an operational program. It is illogical to insist that non-pilot activities—research and development projects—satisfy GAO pilot attributes and contain performance measuring criteria. These benchmark criteria are more appropriate when testing a near deployment-ready capability in a pilot phase, not an exploratory discovery and sense making endeavor.

241 Roth, 10.
244 Government Accountability Office, Designing Evaluations, 27.
Second, Patel et al.’s allegation that “DHS has [emphasis added] made no effort to evaluate their [the pilots] effectiveness” is presumptuous.\textsuperscript{245} The authors make this May 2019 pronouncement relying on an OIG investigation that concluded in October 2016, over two and half years prior. Patel et al.’s present day allegation ignores all the DHS activities since October 2016. A review of FOIA-released documents for one DHS component’s division supports a contradictory story. The FDNS’ Social Media Branch, which comprises approximately 20 full-time employees including IOs, supervisors, intelligence research specialists, and management and program analysts, operates at an annual cost of approximately $3,000,000.\textsuperscript{246} Nine FOIA-released reports relating to this division contain detailed, substantive references on “lessons learned,” “next steps,” “challenges,” “accomplishments,” and “milestones” of the SOCMINT initiative.\textsuperscript{247} These references, before and after the OIG investigation, evince a long-standing, clear

\textsuperscript{245} Patel et al., “Social Media Monitoring,” 31.

\textsuperscript{246} Patel et al., 31.

pattern of efforts focused on evaluating and improving effectiveness of the use of SOCMINT.

Lastly, Patel et al. fail to disclose three material facts regarding DHS’ efforts to measure effectiveness. The first relates to the methodology used in the OIG’s investigation. This methodology issue is separate from the aforementioned issue of assessing the research and development activities as de facto pilots. The OIG conducted its inspection between July and October 2016.\(^{248}\) The OIG inspection only references three pilots despite the fact that, as Taylor advises, DHS had actually conducted seven pilots.\(^{249}\) Consequently, the OIG’s report fails to consider over 57 percent of DHS’ SOCMINT activities. Patel et al.’s overlooking this fact insulates from scrutiny the OIG’s conclusions and the authors’ derivative conclusion regarding DHS efforts to measure effectiveness.

The second material fact also relates to the OIG missing information. The OIG explicitly acknowledged that it did not include a key report in its analysis—The Homeland Security Systems Engineering & Development Institute (HSSEDI) report, *Social Media Analytics Capability Testing: Independent Assessment*.\(^{250}\) The report, which memorialized the feasibility testing of 275 social media tools, was rich with the type of evaluation “metrics” that the OIG repeatedly alleged were missing.\(^{251}\) The inspectors did not have the benefit of this report, which was finalized October 28, 2016, and not released to the OIG until January 6, 2017, subsequent to the close of the inspection period.\(^{252}\) However, the OIG noted:

> The assessment included seven steps in conducting evaluations for quantitative analysis: (1) define the purpose of the evaluation; (2) elaborate a task model; (3) define top-level quality characteristics; (4) produce system requirements; (5) define metrics to measure requirements;

\(^{248}\) Roth, *DHS’ Pilots for Social Media Screening*, 9.  
\(^{249}\) Roth, 11.  
\(^{250}\) Roth, 8.  
\(^{251}\) Roth, 5–8, 11.  
\(^{252}\) Roth, 7.
(6) define techniques to measure metrics; and (7) carry out and interpret the evaluation.253

The OIG acknowledged, “This framework was followed for the independent assessment and should be continued with testing pilots.”254 Patel et al.’s oversight of this fact shields from scrutiny the OIG’s conclusions and the authors’ derivative conclusion regarding DHS’ efforts to measure effectiveness.

The third material fact relates to substantive content of the OIG report. As noted earlier, the report contains two sides—the OIG’s discussion and findings, and DHS’ comments to the draft report. Patel et al. only present the OIG’s side of the report. However, Taylor was unambiguous in his comments that DHS did use metrics to evaluate the effectiveness of its efforts properly.255 As support, Taylor provided clarity on feasibility testing and component metrics, the flow of performance measure information, and DHS’ next steps.

Regarding testing and metrics, Taylor explained that the feasibility testing included a market survey to identify whether 275 tools met minimum capability requirements; evaluated tools that met key screening capability requirements; and completed an in-depth quantitative and qualitative evaluation of each tool’s capabilities.256 He explained, “DHS used and will continue to use a rigorous and repeatable qualitative and quantitative criteria for measuring tool performance” with various metrics identified in the HSSEDI assessment report. Taylor cited specific metrics:

DHS components consistently collect and analyze a comprehensive collection of metrics to measure the performance of ongoing research and development pilots, including the (a) processing time per case, (b) number of queries conducted, (c) number of cases where relevant information was returned, (d) number of returned documents for each query, (e) number of social media accounts found, (f) number of documents collected, (g)

253 Roth, 8.
254 Roth, 8.
255 Roth, 10.
256 Roth, 11.
number of travel confirmations, and (h) number of Social Media Assessment reports written when information of interest is found.\(^{257}\)

Taylor also addressed how the allegedly missing performance evaluation information flowed across DHS. He explained, “[P]erformance measures such as project milestones are reported on a weekly basis to the Task Force using a Plan of Action and Milestones reporting function.”\(^{258}\) He described how the “Task Force’s activities and pilots’ performance are memorialized in a weekly agenda, discussed in a weekly conference call with Task Force members, and disseminated to the Task Force and DHS leadership in weekly summaries.”\(^{259}\)

To address the OIG’s concerns about alleged missing metrics, Taylor outlined DHS’ path forward. Taylor said, “DHS will also increase its efforts to improve the transparency and appropriate socialization of metrics used by Components by attaching them to the Task Force’s weekly conference call readouts.”\(^{260}\) He also explained that as the research and development efforts matured to an operational capability, DHS would identify “true benchmarks for future operational pilots’ success.”\(^{261}\) Patel et al.’s oversight of this fact protects the OIG’s conclusions and the authors’ derivative conclusion regarding DHS’ efforts to measure effectiveness from thoughtful, balanced analysis.

Patel et al.’s contention that SOCMINT is problematic because the pilots lacked policies and procedures also is misleading.\(^{262}\) The authors support this claim by citing the OIG’s findings that none existed.\(^{263}\) It is reasonable to expect that pilots have policies and procedures. However, as explained previously, these exploratory social media screening research and development activities were not yet intended to be pilots, let alone

\(^{257}\) Roth, 12.
\(^{258}\) Roth, 12.
\(^{259}\) Roth, 12.
\(^{260}\) Roth, 13.
\(^{261}\) Roth, 12.
\(^{262}\) Patel et al., “Social Media Monitoring,” 31.
\(^{263}\) Roth, \textit{DHS’ Pilots for Social Media Screening}, 6.
an operational capability. Taylor responded to the OIG’s concern, “When the Task Force was established, neither clearly defined processes, nor robust technical capabilities for large-scale, automated social media screening existed in industry or within the Government.” On March 16, 2016, approximately four months before the OIG initiated its investigation, USCIS acknowledged it did “not have any experience in using it [social media] as a large scale screening tool” and “therefore decided to approach this work as an open-ended exploration with very flexible research parameters.” Internally, USCIS researchers characterized the program as “an adaptive learning approach,” not a deployment-ready capability that would need policies and procedures yet. Identifying potentially workable processes was in constant flux. The team used an “adaptive approach to create, implement, and continually revise its social media screening procedures.” Such a flexible and creative approach is typical in this space. The effort had yet to mature from research and development into a process amenable to creating policies and procedures before the OIG’s investigation occurred. This future capability, once the SMTF transitioned its research and development efforts into a functional capability, was slated to reside at the DHS Social Media Center of Excellence (COE). The OIG acknowledged, “We reviewed the task force’s concept of operations for the role of the COE, but could not evaluate the COE at this time because it has not been set up or funded.” In short, the OIG’s 2016 investigation into DHS’ SOCMINT efforts was premature.

264 Roth, 10.
266 U.S. Citizenship and Immigration Services, 21.
267 U.S. Citizenship and Immigration Services, 19.
270 Roth, DHS’ Pilots for Social Media Screening, 9.
2. **USCIS FOIA Documents**

The critics contend that admissions in internal reports demonstrate that USCIS has encountered problems in its attempts to deploy SOCMINT. Those who do not support this concept offer these revelations as primary source proof that SOCMINT is problematic. The FOIA-released findings reported internally within USCIS reveal critical, unknown insights into the viability of SOCMINT. Sans an alternative to the critics’ explanation regarding USCIS’ judgments, these claims lend support to the notion that SOCMINT is a problematic endeavor.

Patel et al.’s allegation that USCIS “explicitly questioned the overall value of the programs” is erroneous. In support of this claim, the authors seize on and isolate a sentence in a FOIA-released document, “Having FDNS personnel dedicated to mass social media screening diverts them away from conducting the more targeted enhanced vetting they are well trained and equipped to do.” Analyzing this sentence in context by examining the adjacent sentences reveals that USCIS is not questioning the value of the program. Conversely, USCIS is identifying challenges, finding solutions, and forging ahead.

The sentence that the critics seize on exists in a FOIA-released report that also says, “There are several technical challenges to semi-automated use and access of social media that DHS is working to overcome.” The report clarifies, “USCIS is working now on developing greater social media vetting capability on that kind of case-by-case referral basis.” The report continues, “Future milestones related to Social Media include: FDNS will continue a risk-based expansion of social media screening [redacted]...” Elsewhere in the director’s presidential transition team documents, USCIS states that as social media screening tools and processes are developed and made

---

273 U.S. Citizenship and Immigration Services, 201.
available through the COE, “USCIS will increasingly turn to the COE to assist USCIS in its social media vetting of immigration applicants.”276

The sentence in question should be read in context to appreciate its true meaning. In addition, the sentence could arguably indicate that social media screening is straining staffing levels and therefore the division needed more social media screening personnel. The fact that the Social Media Division (SMD) began actively hiring additional personnel less than six months after this report supports this interpretation.277 Other FOIA-released documents support this time and labor intensive staffing interpretation.278 A broader contextual analysis contradicts the allegation that USCIS is questioning the overall value of SOCMINT.

Patel et al.’s claim that “USCIS itself found that social media monitoring was not particularly helpful when it tested social media vetting for five programs” is false.279 Patel et al. seize on a sentence in a FOIA-released document. The sentence in question begins, “In a small number of cases, information discovered through social media screening had limited impact on the processing of those cases.”280 Patel et al. mistakenly declare this sentence is evidence that USCIS more broadly discovered “that social media monitoring was not particularly helpful.”281

Nowhere in the report does USCIS actually say, “that social media monitoring was not particularly helpful.”282 Conversely, three sentences after the sentence that Patel et al. rely on, USCIS says it “may be helpful in developing additional lines of inquiry

282 Patel et al., 31.
when adjudicating the benefit request.”

USCIS partner S&T continues its efforts to enhance SOCMINT tools, as confirmed by a solicitation articulated in Long Range Broad Agency Announcement (LRBAA) 18–01, which was released June 4, 2018. In addition, the Science and Technology Directorate Budget Overview: Fiscal Year 2019 Congressional Justification indicates, “Social Media tools [are] the current major investment area” under the Data Analytics Engine. It appears that social media analytics falls under a number of initiatives and that S&T budgeted $5–10 million for fiscal year (FY) 2019. USCIS’ collective comments, its confidence in S&T, and S&T’s agenda and budgeting indicate USCIS sees benefits in using SOCMINT.

B. WE ARE SAFE ENOUGH

The critics claim that the United States is safe enough without SOCMINT. They advance several explanations to support this assertion. The objections are grounded in different rational. However, these objections stand for the proposition that SOCMINT is unnecessary. Without evidence dispelling the safe enough theory, the necessity for SOCMINT wanes.

Bier’s argument that vetting failures are infrequent, especially after 9/11 is true, but does not mean that the United States is safe enough. He provides a detailed numerical analysis of historical vetting failures. Bier argues, “[T]he country has maxed out its capacity to improve immigration vetting.” Assuming the status quo

---


287 Bier, “Extreme Vetting of Immigrants.”

288 Bier.

289 Bier.
vetting procedures make this nation safe enough, though, dangerously ignores three critical considerations.

First, the 9/11 Commission concluded, “The 9/11 attacks revealed four kinds of failures: in imagination, policy, capabilities, and management.” 290 Deciding the sufficiency of current vetting procedures on a historical analysis binds the analysis to the past and guarantees a failure of imagination regarding future possibilities. This practice has proven especially dangerous in immigration matters. The Commission determined, “Both Hazmi and Mihdhar could have been held for immigration violations.” 291 The Commission concluded, “Investigation or interrogation of them, and investigation of their travel and financial activities, could have yielded evidence of connections to other participants in the 9/11 plot.” 292

Second, experts have warned of relying on statistical analysis of historic events after 9/11. RAND concludes, “[T]errorist events occurred in clusters in the period between 1970 and 2002; after that, the distribution of events is statistically random.” 293 Bier provides a thorough numerical analysis, e.g., “[T]he rate for deadly terrorists was 1 for every 379 million visa or status approvals from 2002 through 2016.” 294 However, RAND demonstrates:

[A]nalysis of the historical record of terrorism highlights an observation that is both obvious and salient to security planning: Current assessments of terrorism are driven not by what terrorists have done since 9/11, but rather by what terrorists might do in the future—replicate a 9/11-scale attack or worse using weapons of mass destruction. 295

Bier’s detailed numerical analysis ignores RAND’s central conclusion.

291 National Commission on Terrorist Attacks upon the United States, 272.
292 National Commission on Terrorist Attacks upon the United States, 272.
294 Bier, “Extreme Vetting of Immigrants.”
295 Jenkins, Willis, and Han, Do Significant Terrorist Attacks Increase the Risk of Further Attacks?, 9.
Third, Bier’s arguments assume stasis—that threats and the success of mitigating them do not change. However, front-line practitioners contradict analysts’ speculation. McChrystal urges that the modern terrorism threat is a new kind of threat, bred by a fundamentally new kind of environment spawned from technological and social changes. Bier’s alleged sufficient, maxed out vetting theory is analogous to the Maginot Line that proved so ineffective for France in World War II. As inevitable changes flourish, today’s sufficiency becomes tomorrow’s insufficiency.

Inserra’s theory that we “must not shift resources from countering” homegrown terrorist threats “in order to start broad social media vetting efforts” in the absence of attacks from abroad is debatable. He argues, “Since start 2015, all 30 Islamist plots and attacks against the U.S. homeland have involved a homegrown terrorist.” Therefore, he says, we should not begin broad social media vetting efforts for individuals from abroad. Like Bier, he assumes the past equals the future in terms of threats.

Sagarin claims the answer to security threats lies in understanding nature, not historical trends in attacks. Sagarin contends that nature can be a framework for dealing with security problems that require adaptability. Sagarin bases this claim on the idea that “biological organisms and human societies both face highly variable and highly unpredictable threats.” His central argument is that “no effective security solution can be deployed and not modified or changed with time, because everything around it will be changing.”

---

297 McChrystal, 51.
298 Inserra, “The U.S. Should Tread Carefully on Social Media Vetting.”
299 Inserra.
300 Inserra.
301 Sagarin, *Learning from the Octopus*, xxv.
302 Sagarin, 226.
303 Sagarin, 227.
304 Sagarin, 10.
strategies are unable to solve emerging, contemporary threats. Inserra’s theory ignores the potential for change. His objection to SOCMINT based on it not being necessary in light of current trends in attacks is unpersuasive.

Patel et al.’s challenge to the notion that value exists in focusing resources on this initiative based on a low hit rate is deceptive. Patel et al. cite a report in a FOIA-released document that social media screening had a “limited” impact in “a small number of cases.” This report is only inclusive of results through November 4, 2016. More important is what the report represents: information from a mere five research and development projects. These projects did not comprise a fully deployed operational capability, but rather the first steps into a nascent space where “neither clearly defined processes, nor robust technical capabilities for large-scale, automated social media screening existed in industry or within the Government.” The researchers were just discovering what needed to be done, whether it could be done, how to do it, and what tools might do it best. For Quentin et al., this type of discovery is a crucial step. A meaningful assessment of value regarding a future operational SOCMINT capability should only rely on that program’s merits. Consequently, relying on the hit rate from a newly ventured learning curve involving a handful of research and development projects to be somehow indicative “of the value of focusing resources on collecting and analyzing this type of data” is not very logical.

305 Sagarin, xxiii.
307 Patel et al., 31 citing “U.S. Citizenship and Immigration Services Briefing Book: Social Media,” 201.
308 Patel et al., 201.
309 Patel et al., 200–201.
310 Roth, DHS’ Pilots for Social Media Screening, 10.
C. CONCLUSION

The arguments offered by the critics fail to support their position. SOCMINT is a plausible initiative to leverage in attempting to protect the homeland because the efforts to date have not been problematic. Moreover, misplaced reliance on the nation’s current degree of safety reinforces the need for such a program. In sum, the legitimacy of the claims by those who do not support this concept due to SOCMINT’s alleged problematic nature and non-necessity falters. In other words, the critics’ arguments do not withstand scrutiny. The propositions for SOCMINT as a means to secure the homeland in this context are valid. The next chapter explores the critics’ objections based on efficacy.
IV. SOCMINT EFFICACY CONCERNS

Al Qaeda is executing a time-tested strategy, and its members are doing it by the book. Plus it is much easier now, as the Internet has made communication simple and instantaneous and formal organization all but unnecessary. Terrorists groups of all kinds now use this technology to its fullest capability. Today’s terrorists can recruit, indoctrinate, and communicate without even meeting each other. Terrorism has become an Information Age threat, but our intelligence agencies still examine it through an Industrial Age lens.

—Mike German, author, 
Thinking Like a Terrorist: Insights of a Former FBI Undercover Agent

‘Open source’ was ‘frosting on the cake’ of source material dominated by clandestine collection, SIGINT, IMINT, and HUMINT. Today, open source has expanded well beyond ‘frosting’ deep into the cake. It is indispensable to the production of authoritative analysis.

—John C. Gannon, former Chairman, National Intelligence Council

This chapter analyzes the efficacy issues identified by the second camp of critics in the literature review. Those who argue against SOCMINT assert that it is ineffective at identifying and mitigating threats. The critics identify an assortment of issues that call into question the efficacy of SOCMINT, including yield, scope, scale, language, context, encryption, and identity resolution challenges. A viable SOCMINT capability must be adept at traversing the complex terrain of challenges this environment presents. If the critics’ claims regarding USCIS’ inability to overcome these issues are true, the claims strongly contradict the purported efficacy of SOCMINT.

A. YIELD

The critics contend that SOCMINT is incapable of yielding useful information on threats. As evidence, the critics point to the results from several SOCMINT pilots. The inability of a SOCMINT program to identify and mitigate threats essentially renders it
useless. If the critics’ assessment of the threat identification and mitigation ability is meritorious, it supports that SOCMINT is ineffective.

Patel et al.’s allegation that the DHS SOCMINT pilots have been “notably unsuccessful in identifying threats to national security” is misleading. The authors go as far as to say, “Even more damning are USCIS own evaluations.” In support of this claim, the authors cite a statement from an internal report, “[T]he information in the accounts did not yield clear, articulable links to national security concerns, even for those applicants who were found to pose a potential national security threat based on other security screening results.”

This statement may not be a reliable assessment of whether SOCMINT is beneficial in identifying national security threats for four reasons. First, this statement was made in December 2016 based on only three of the initial research and development projects that were concluded by December 2015. The projects only involved refugees, which is a subset of the different types of immigration benefit requests that USCIS vets. Therefore, drawing conclusions about a future capability that will involve all benefit request types based on initial research and development projects confined to only refugee cases may be unreliable. Second, available information revealed SOCMINT use in 235 cases. USCIS adjudicates more than 26,000 applications and petitions for a variety of immigration benefits on an average day. Therefore, relying on initial research and development project data from such a small sample size of cases may not be a reliable basis to draw conclusions about a future capability. Third, the authors fail to disclose language indicating, “FDNS encountered a number of challenges, limitations, and inefficiencies with the [Defense Advanced Research Projects Agency (DARPA)] tool and

313 Patel et al., 3–4.
314 Patel et al., 4.
317 U.S. Citizenship and Immigration Services, “A Day in the Life of USCIS.”
concluded that it did not meet USCIS needs for social media screening.\textsuperscript{318} Therefore, drawing conclusions about a future capability still in development based on results involving a specific DARPA tool that will not be used by USCIS in the future carries no weight. Fourth, USCIS was transparent about its unfamiliarity with SOCMINT when it embarked on this endeavor.\textsuperscript{319} Failing to identify threats that were confirmed outside of social media in initial research and development projects does not mean that a future SOCMINT capability still in development will not be successful at identifying threats. As optimal tools are discovered and experience improves tradecraft, the success of detection may improve.

The ACLU argument that there is “no reason to believe collecting and retaining this kind of social media information will improve our security” lacks merit.\textsuperscript{320} Security experts’ opinions, LEAs’ use of and their successes with SOCMINT, and PIRUS research do provide multiple reasons to believe that SOCMINT will improve the nation’s security. The Profiles of Individual Radicalization in the United States subsection in Chapter II supports the notion that terrorists who are immigrants use social media and an opportunity exists to intervene. The Experts subsection in Chapter II concludes that the security experts agree about the viability of using SOCMINT to identify terrorists. The Law Enforcement SOCMINT Use section in Chapter II concludes that LEAs are embracing the SOCMINT capability, which signals viability. The SOCMINT Successes section in Chapter II demonstrates that real-word terrorism intervention successes have resulted based on SOCMINT. Collectively, substantial support does exist that SOCMINT can improve security. The ACLU’s argument about the absence of reasons to believe SOCMINT will improve security does not withstand scrutiny.

\textsuperscript{318} U.S. Citizenship and Immigration Services, “U.S. Citizenship and Immigration Services Briefing Book: Social Media,” 198.


\textsuperscript{320} Handeyside, “The Many Problems with the Trump Administration’s Plan to Hold on to Some Immigrants’ Social Media Posts.”
B. SCOPE AND SCALE

Those opposing the SOCMINT initiative maintain that the number of platforms and volume of posts inhibit adept identification of threats. These opponents recognize the complexity of this domain and do not see technology as a silver bullet. Over 100 English-language social networks are in existence. Twitter users post 500 million tweets every day. Users on Facebook share almost five billion pieces of content every day. YouTube users upload over 18,000 hours of video every hour. The enormous quantity of user content posted to these websites creates a challenge in identifying terrorism content. An effective SOCMINT capability must be capable of sorting signals from noise in vast amounts of data, especially when millions of immigration benefits are sought annually. Unless the claim about successfully managing social media post volume is disproved, the efficacy of SOCMINT is suspect.

Patel et al.’s contention that automating the SOCMINT process to review enormous volumes of social media posts compounds the difficulty of correctly interpreting SOCMINT data is misplaced. The vast number of social media platforms (scope) and the enormous quantity of social media posts (scale) may create an opportunity for automated technologies to improve processing efficiency that may be in tension with accuracy. However, any concerns about potential problems associated with automating SOCMINT to review enormous volumes of social media data are irrelevant if USCIS’ process of reviewing posts is not in fact automated. The USCIS “Social Media” issue paper in the December 6, 2016, Briefing Book materials for the presidential transition team explicitly acknowledges the technical challenges with semi-automated use

321 Mehra, “105 Leading Social Networks Worldwide.”
322 Aslam, “Twitter by the Numbers.”
323 Kavanaugh, “Scanning Social Media Could Stop the Next Terror Attack.”
324 Greenemeier, “Social Media’s Stepped-Up Crackdown on Terrorists Still Falls Short.”
325 Marcellino et al., Monitoring Social Media, 10–11.
and access of social media. The “USCIS Social Media & Vetting: Overview and Efforts to Date” report updated on March 2, 2017, unequivocally states, “all social media screening and vetting requires a manual review of information.” USCIS’ research and development projects revealed challenges associated with using semi-automated and automated screening of social media data. Consequently, the SMD’s current SOCMINT capability does not rely on the alleged non-manual review methods for social media posts. Patel et al.’s automation argument is inapt because USCIS is not relying on automated SOCMINT for the process of reviewing posts.

C. LANGUAGE

According to the critics, language presents an insurmountable hurdle for proficient threat identification. They question technology’s ability to overcome interpretation challenges; language challenges are different from context challenges, which are addressed in a different section that follows. A viable SOCMINT program must be capable of processing a diverse mix of different languages to identify threats. If the critics are correct, this contention about interpreting language lends support to the argument that SOCMINT is not effective.

Patel et al.’s argument that SOCMINT will require that government agencies have the ability to understand over 7,000 languages and the cultural norms of 193 countries to avoid misinterpretation issues is misleading. Language and culture do make discerning meaning from social media data difficult. This challenge is typical to intelligence processing and analysis in general, not just SOCMINT. However, safeguards are in place to mitigate misinterpretation and any potential derivative adverse outcomes. The initial research and development projects’ reports indicate that USCIS rejected social media tools that “did not offer an option to flag cases/accounts/social

329 U.S. Citizenship and Immigration Services, 58.
media posts for linguist review.”332 The “USCIS Social Media & Vetting: Overview and Efforts to Date” report reveals that multiple entities are being engaged to assist with expert translation.333 USCIS also utilizes “subject matter expertise in regional culture, religion, and terrorism.”334 Beyond seeking expert support, USCIS has implemented additional safeguards. First, “FDNS incorporates strenuous verification procedures to ensure accuracy of data before an immigration benefit decision is made by adjudications.”335 Second, “As with all derogatory information found from publicly available sources, the applicant and/or petitioner must be provided with an appropriate opportunity to explain or refute any information that conflicts with information he or she provided to USCIS before a decision is made regarding the requested benefit.”336 And third:

All information obtained by FDNS IOs and reviewed by ISOs is reviewed in accordance with a strict set of internal procedures intended to ensure that actionable derogatory information meets the standards for evidence established by the USCIS Administrative Appeals Office, the Department of Justice (DOJ), Executive Office for Immigration Review (EOIR), and the federal court system.337

These safeguard efforts exist to mitigate the potential of misinterpretation of language or cultural norms adversely affecting immigration benefit adjudication. USCIS’ approach to SOCMINT evidence aligns with what the experts recommend.338 Patel et al.’s concerns have not gone unaddressed.

EPIC’s contention that SOCMINT potentially causes irreversible harm based on language translation failures is unpersuasive. EPIC provides an example of a Facebook algorithm erroneously machine translating the Arabic post “good morning” into “attack them” and “hurt them.” EPIC only tells part of this story, however. EPIC neglects to disclose that the mishap occurred because the Israeli police failed to consult an Arabic speaker to confirm the machine translation prior to making an arrest. As noted previously, USCIS does not exclusively rely on machine translation without expert linguist consultation.

Second, the previously identified safeguards—data accuracy verification procedures, the opportunity to explain or refute, and sound evidentiary standards—protect against the misinterpretation risk. EPIC’s argument about this potential for irreversible harm is unconvincing based on how USCIS manages its SOCMINT program.

Patel et al.’s contention “that 20–30 percent of posts analyzed through natural language processing would be misinterpreted” is unpersuasive. The authors proffer accuracy limitations associated with natural language processing; however, the authors ignore several key considerations. First, this argument assumes that natural language processing outcomes are dispositive, e.g., evaluative efforts stop after natural language processing occurs and that decisions are based solely on the outcome of the natural language processing. The argument ignores that supplemented review by human analysts can increase accuracy rates above the 70–80 percent level achieved by machine-only processing. In addition, USCIS reports make clear that an officer must manually review the content of social media data to identify if any derogatory indicators are present.

---

340 Electronic Privacy Information Center, 14–15.
341 Hern, “Facebook Translates.”
Second, the argument is only relevant if USCIS deploys and solely relies on natural language processing technologies. Again, USCIS says, “all social media screening and vetting requires a manual review of information.” 346 This manual review by human analysts helps mitigate misinterpretation. Third, the argument ignores that safeguards exist to protect against misinterpretation. The previously identified safeguards—data accuracy verification procedures, the opportunity to explain or refute, and sound evidentiary standards—hedge against the misinterpretation risk. 347 Patel et al.’s argument about natural language processing accuracy limitations is unpersuasive based on how USCIS conducts SOCMINT.

Patel et al.’s claim that sentiment analysis is even less accurate is unpersuasive. 348 The argument is only relevant if USCIS is deploying sentiment analysis technologies. Nothing in public records, however, supports that USCIS is using sentiment analysis. The authors cite an article that discusses comments by an official in an unrelated DHS component and the availability of sentiment analysis in the DoD’s DARPA tool that USCIS tested during research and development projects. 349 However, USCIS concluded that the DARPA tool did not meet USCIS’ needs for social media screening. 350 Patel et al.’s argument about sentiment analysis accuracy limitations is unconvincing in light of how USCIS conducts SOCMINT.

D. CONTEXT

The critics argue that attempts at accurate sense making, amid ambiguous context, confound SOCMINT analysts. Those who argue against SOCMINT identify problems that context presents to SOCMINT analysts. Failing to understand a social media post’s

346 U.S. Citizenship and Immigration Services, 58.
context properly can frustrate accurate threat identification and potentially lead to incorrect understanding. If insurmountable, the understanding context dilemma detracts from SOCMINT’s efficacy.

Patel et al.’s argument that misinterpretation problems based on context plague efforts to make judgments using SOCMINT is unconvincing. The authors offer a hypothetical example that purports to present the analyst with ambiguity in determining meaning when a user “loves” an ISIS-related social media post. The authors’ claim ignores USCIS’ procedures for addressing content that may result in misinterpretations based on context. Some of the same DHS safeguards deployed to address language misinterpretation issues are used to mitigate context misinterpretation issues. USCIS documentation reports, “Due to its inherent lack of data integrity, public source information is not used as the sole basis upon which to deny an immigration benefit, investigate benefit fraud, or identify public safety and national security concerns.”

Potentially derogatory information identified in social media checks that relates to an individual “may be helpful in developing additional lines of inquiry when adjudicating the benefit request.” USCIS’ line of inquiry approach is consistent with the experts’ guidance. USCIS gives applicants and/or petitioners an appropriate opportunity to explain or refute any information. The caution observed, manner of use, and validation of social media data resolves concerns about making accurate judgments of SOCMINT data. USCIS’ approach to verification and validation aligns with the experts’

---

352 Patel et al., 5.
guidance. Patel et al.’s claim regarding misinterpretations based on context ambiguity fails when considering how USCIS makes judgments using SOCMINT data.

The EPIC argument that SOCMINT is unreliable because “making decisions based on social media data is complex” in light of context challenges is shortsighted. EPIC supports this claim based on the allegation, “The current systems can’t automatically compute risks of terrorist behavior.” Citing Cohen’s article, EPIC argues that relying on keywords out of context frustrates accurate identification of terrorist behavior. However, this claim ignores the facts regarding SOCMINT’s role in USCIS adjudicative decisions. USCIS reports confirm, “[a]s of November 4, 2016, no immigration benefits have been denied solely or primarily because of information uncovered through social media vetting.” USCIS is not attempting to compute the risks of terrorist behavior based on keyword occurrences. Any potentially derogatory social media information merely opens a line of inquiry regarding terrorist concerns. EPIC’s claim concerning SOCMINT unreliability fails to consider how USCIS actually uses SOCMINT data for adjudicative decisions.

EPIC’s contention citing Lang, “One mistake can result in a wrongful denial of entry, arrest, and worse,” concerning the consequences of misinterpreting context is

---


359 Electronic Privacy Information Center, 14.


misleading. USCIS does not deny immigration benefits solely based on SOCMINT. All information, including social media information, is evaluated “to ensure that actionable derogatory information meets the standards for evidence” discussed previously. These internal procedures are in place to ensure that the extreme outcomes that EPIC warns of may only result when adequately supported with reliable evidence. EPIC’s argument involving haphazard outcomes is contradicted by USCIS’ evidentiary standards practices.

E. ENCRYPTION

Those who argue against SOCMINT claim encryption options available to nefarious actors render open-source SOCMINT efforts moot. The critics see encryption as a countermeasure that eliminates the need for SOCMINT. USCIS’ open-source SOCMINT capability relies exclusively on the ability to access unencrypted social media data. If the critics’ assessment regarding encryption is meritorious, the argument for SOCMINT’s efficacy is severely weakened.

The ACLU assertion that “[a]nyone actually engaged in terrorism will simply take additional steps to hide their communications, making this information collection ineffective” does not pass scrutiny. The PIRUS dataset contradicts this claim for both internet users and social media users. In Chapter II’s Operational Security subsection, the analysis focuses on radicalized immigrants for whom social media played a role in their radicalization and who took action on their plot. Here, the analysis expands beyond radicalized immigrants and social media to address the ACLU’s broader claim. The PIRUS variable “Internet_Use_Plot” contemplates if the “extremist activity involved a violent plot, did the individual use the internet for communications or logistics while

---


preparing for and undertaking the plot.”

For example, “[U]sing the internet to communicate with group members or other extremists, threatening targets, researching the target and tactics, and ordering supplies.” Adjusting the group size of the 2,148 radicalized to include only those subjects whose internet plot use was known and the plot occurred after 1995 reduces this group to 370 subjects. Isolating the “Internet_Use_Plot” variable identifies that 155 of the subjects (41.89 percent) used the internet in conjunction with their plot preparations.

The “Op_Security” variable identifies, “If the individual’s first publically known extremist activity involved a violent plot, did the individual attempt to hide or conceal preparation for the plot?” The operational security efforts are known for 135 of the 155 subjects who used the internet in conjunction with their plot preparations. Secondary research based on the “Op_Security” variable reveals that of the 135 internet plotters, 26 subjects (19.26 percent) were “openly vocal about the plot (discussed it with friends and associates, procured suspicious supplies—like explosives or weapons—without being discrete, etc.).” The PIRUS data indicates that 45 of the 135 subjects (33.33 percent) were “neither covert nor overt (did not discuss the plot openly or overtly procure supplies, but also did not attempt to hide activities).” The data demonstrates that nearly 53 percent of the Internet_Use_Plot subjects did not make efforts to hide what they were doing.

The “Social_Media” variable reports when there is “evidence that online social media played a role in the individual’s radicalization and/or mobilization.” Adjusting
for radicalization that occurred before 2005 and cases in which social media’s role in radicalization is unknown reduces the 2,148 radicalized to 608 subjects.\textsuperscript{373} Isolating the “Social\_Media” variable identifies that social media “played a role but was not the primary means of radicalization or mobilization” in 295 of the 608 subjects (48.52 percent).\textsuperscript{374} Analyzing the “Social\_Media” variable reveals that social media “was the primary means of radicalization for the individual (e.g., initial exposure to ideology and subsequent radicalization occurred over online social media)” in 63 of the 608 subjects (10.36 percent).\textsuperscript{375} Social media played at least some role for 358, a majority (58.88 percent) of the radicalized. The operational security efforts are known for 139 of the 358 subjects who radicalized on social media. Secondary research based on the “Op\_Security” variable reveals that of the 139 social media radicalized, 31 subjects (22.30 percent) were “openly vocal about the plot (discussed it with friends and associates, procured suspicious supplies—like explosives or weapons—without being discrete, etc.).”\textsuperscript{376} The PIRUS data indicates that 58 of the 139 subjects (41.73 percent) were “neither covert nor overt (did not discuss the plot openly or overtly procure supplies, but also did not attempt to hide activities).”\textsuperscript{377} The data demonstrates that 64 percent of the Social\_Media subjects did not make efforts to hide what they were doing. Research on the PIRUS dataset disproves the ACLU’s argument that SOCMINT is ineffective because operational security measures, e.g., using encryption, will prevent identifying terrorists. Moreover, Ramwell et al. argue that even when operational security is deployed, an activity trail is often exploitable.\textsuperscript{378}

\textsuperscript{373} The PIRUS dataset does not report data on social media use before 2005.

\textsuperscript{374} National Consortium for the Study of Terrorism and Responses to Terrorism, \textit{Profiles of Individual Radicalization in the United States (PIRUS) Codebook}, 18.

\textsuperscript{375} National Consortium for the Study of Terrorism and Responses to Terrorism, 18.

\textsuperscript{376} National Consortium for the Study of Terrorism and Responses to Terrorism, 10.

\textsuperscript{377} National Consortium for the Study of Terrorism and Responses to Terrorism, 10.

\textsuperscript{378} Steve Ramwell, Tony Day, and Helen Gibson, “Use Cases and Best Practices for LEAs,” in \textit{Open Source Intelligence Investigation: From Strategy to Implementation}, eds. Babak Akhgar, P. Saskia Bayerl, and Fraser Sampson (Switzerland: Springer International Publishing AG, 2016), 200–1, \url{http://dx.doi.org/10.1007/978-3-319-47671-1}.
F. IDENTITY RESOLUTION

Successful identity resolution, according to the SOCMINT critics, is illusory. They draw on the lessons learned regarding identity resolutions during USCIS’ initial SOCMINT efforts as proof that SOCMINT is ineffective. Merely identifying a potential threat on social media is of little value if authorities cannot correctly attribute that potential threat to a person amenable to investigation. Justifying the efficacy of SOCMINT will be difficult if the critics’ assessment concerning identity resolution is accurate.

The assertion that a “key takeaway from the pilot programs was that they were unable to reliably match social media accounts to the individual being vetted” by Patel et al. is misleading. The authors base this claim on a discussion of challenges that DHS was working to overcome as identified in the “Social Media” issue paper in the December 6, 2016, Briefing Book materials for the presidential transition team. First, the identity resolution concern is not contained in the “Challenges” section of a subsequent March 2, 2017, report. Hence, perhaps DHS was successful at overcoming this challenge. Day et al. argue identity matching is not insurmountable. Second, maybe tradecraft improved and eliminated this challenge. For example, Karasek argues that immigration officials have an advantage in the SOCMINT terrorist discovery endeavor—immigration officials have relatively complete and reliable sets of personal data submitted by the applicants themselves. This reliable data can help resolve identities. The explanation for the absence of the identity resolution challenge in the latest publicly available report and the theory on tradecraft improvements are speculation. However, they are no more speculative than the assertion that the identity resolution

problem identified three years ago in research and development projects persists or remains to the same extent in the current deployed SOCMINT capability. Patel et al.’s claim about identity resolution is questionable.

G. CONCLUSION

The critics’ contention that yield, scope, scale, language, context, encryption, and identity resolution challenges render SOCMINT ineffective at identifying and mitigating threats is incorrect. Examining the facts in public records contradicts the position of those who do not support this concept. The critics’ characterization of automation, natural language processing, and sentiment analysis do not apply to USCIS’ SOCMINT program. USCIS safeguards—data accuracy verification procedures, the opportunity to explain or refute, and sound evidentiary standards—prevent the alleged misinterpretation risk. The position of those who argue against SOCMINT that efficacy challenges have created insurmountable obstacles for SOCMINT is unpersuasive. The next chapter addresses the data and constitutional concerns identified by those in the last camp who oppose SOCMINT.
V. SOCMINT DATA AND CONSTITUTIONAL CONCERNS

We the People of the United States, in Order to form a more perfect Union, establish Justice, insure domestic Tranquility, provide for the common defence, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity, do ordain and establish this Constitution for the United States of America.

—U.S. Constitution, Preamble

The choice is not between order and liberty. It is between liberty with order and anarchy without either. There is danger that, if the [Supreme] Court does not temper its doctrinaire logic with a little practical wisdom, it will convert the constitutional Bill of Rights into a suicide pact.

—Justice Robert Jackson, former Associate Justice,
Supreme Court of the United States

This chapter analyzes the data and constitutional concerns identified by those in the literature review’s last camp who oppose SOCMINT. The opposition to the SOCMINT initiative insists that the endeavor creates a host of ancillary problems related to data management. Aside from collection and analysis challenges inherent in SOCMINT, the opponents predict additional data-related obstacles. They raise concerns over data retention, sharing, and security. A successful SOCMINT capability must adequately address data management problems. Failing to dispel these data concerns weakens the argument that SOCMINT enhances USCIS’ mission. The critics also raise concerns that the SOCMINT capability is incompatible with constitutional protections. Separate from the collection and analysis challenges characteristic of SOCMINT, those opposing SOCMINT warn of constitutional infringements. They cite SOCMINT’s adverse effect on privacy, speech, and discrimination. A viable SOCMINT program must not involve practices that unduly infringe on constitutional protections. Unless mitigated, these alleged constitutional incompatibilities are in tension with USCIS managing a viable SOCMINT capability.
A. DATA CONCERNS

The critics’ arguments that the SOCMINT initiative creates a host of ancillary problems related to data management—data retention and data sharing, which can lead to subsequent misinterpretation, and data hacking risk—are unpersuasive. Sharing protocols and policies disprove the critics’ assertions about data concerns. USCIS adequately addresses the potential data management problems. The critics’ arguments relating to data obstacles are unpersuasive.

1. Data Retention

The critics opine that data retention related to SOCMINT creates perils. These dangers serve as additional grounds to oppose SOCMINT. A sensible SOCMINT program’s data retention policies should be grounded in rational principles. The merit of this claim about data retention would strengthen the critics’ position on data concerns.

Patel et al.’s argument that retaining social media data for long periods of time increases the risk for misinterpretation is not persuasive. The authors opine, “A social media post from 2007 may take on a whole new meaning by 2022, and even more so decades later.” Retention has multiple benefits, and safeguards exist to mitigate the risk of misinterpretation at a later time. First, retention of FDNS data “provides access to information that can be critical to research related to suspected or confirmed fraud, criminal activity, egregious public safety, or national security concerns for applicants/petitioners who may still be receiving immigration benefits.” Second, “should the individual apply for another benefit, retention of the information can eliminate the need for research on concerns that were previously addressed.” Third, retention also ensures “that cases that were reviewed and determined to have no nexus to fraud, criminal activity, egregious public safety, or national security concerns are not opened

---

385 Patel et al., 9.
again because old information is recycled.” In the case of temporal misinterpretations, the previously identified safeguards—data accuracy verification procedures, the opportunity to explain or refute, and sound evidentiary standards—offer protection. Retention provides advantages to both immigration benefit seekers and the agency. Quentin et al. argue ensuring access is imperative in the law enforcement setting because data retention time can span decades. Sensible protections mitigate concerns over social media information susceptibility to misinterpretation. Balancing the retention benefits and acknowledging the safeguards against misinterpretation reduces the merit of the authors’ argument.

EPIC’s allegation that the inclusion of social media data in immigrants’ official files “threatens First Amendment rights, risks abuse, and would disproportionately impact minority groups” fails to convince. The inclusion of social media data in immigrants’ official files actually benefits both the immigrants and agency. It provides the benefits previously discussed—access to critical research data, elimination of duplicate research, and the avoidance of redundant investigations. In addition, including social media data in immigrants’ official files supplements the official record regarding immigration benefit decisions. This evidence would be invaluable to immigrants who sought adjudicative review of any alleged impropriety involving First Amendment rights, abuse, or disparate minority treatment. Inclusion also benefits the agency, and actually protects against the potential harms of which EPIC warns. In light of the advantages to both immigrants and the agency, EPIC’s claim is shortsighted.

---

2. Data Sharing

Concerns over SOCMINT data sharing further fuel the critics’ objection. Those opposing SOCMINT fear that DHS’ data practices further pervert SOCMINT’s viability. The protocols for the sharing of SOCMINT data should comport with policy and law, and mitigate the potential for misinterpretation by secondary, downstream users. If the critics’ fears prove reasonable, their data sharing concerns would be persuasive objections to SOCMINT.

Patel et al.’s allegation, “DHS programs generally have low standards for sharing highly personal information, such as that found on social media” is questionable. USCIS SOCMINT only involves open-source information that exists in the public domain. There is no reasonable expectation of privacy based on the third-party doctrine, which establishes that when “an individual invests a third party with information, and voluntarily agrees to share information with a recipient, the individual loses any reasonable expectation of privacy in that information.” Therefore, the characterization of what exists in the public fora as “highly personal information” is a contradiction. Nevertheless, USCIS sharing protocols are stringent. For example, USCIS may only share publicly available information from social media websites:

- with federal, state, tribal, local, international, or foreign law enforcement and intelligence agencies, in response to an RFI [Request for Information] in support of criminal and administrative investigations and background checks involving immigrant benefit fraud, criminal activity, public safety, and national security concerns.

Sharing across LEA partners is considered essential to protecting the nation. As Wells notes though, law enforcement practitioners adhere to stricter standards than private

---

sector companies. USCIS takes open-source social media information and actually imposes a “higher” standard for sharing than the originating user. DHS secures the social media content behind the DHS firewall and only shares it with trusted LEA partners for official security matters. In contrast, the originating users indiscriminately release what is posted to anyone with an internet connection. Patel et al.’s claim regarding DHS’ low standards for sharing highly personal information does not pass scrutiny.

Patel et al.’s contention, “[s]ocial media information collected for one purpose is used by DHS in a range of other contexts, increasing the likelihood of misinterpretation” is inaccurate. Documentation on USCIS’ use and safeguards of social media data contradicts the authors’ assertions about misinterpretation. FDNS uses collected social media for only one context—official matters relating to security, as explained earlier. The retained FDNS-DS information “may be used to demonstrate an assessment was conducted so that additional resources do not have [to] be used for a second review.” As a safeguard, “FDNS reconciles data to ensure that the data transferred from FDNS-DS to other systems is transferred accurately and completely to mitigate risk that the data may be taken out of context.” FDNS does not use social media data in the multi-context manner the authors’ allege. Based on the actual single-purpose FDNS use of social media data and the deployed safeguards, Patel et al.’s misinterpretation argument is erroneous.

3. **Data Hacking Risk**

The critics raise the issue that data collected by a SOCMINT program is at risk of hacking. They believe collecting data during SOCMINT operations creates an additional threat to manage, keeping the data secure. The protocols for managing data derived from SOCMINT should address any potential for harm from misappropriation. If the fears

---

397 Wells, “Taking Stock of Subjective Narratives,” 60.
400 U.S. Citizenship and Immigration Services Office of Privacy, 6.
about hacking SOCMINT data are rational, this assertion helps justify the critics’ concerns about data.

The argument, “[g]iven incidents like the breach of the Office of Personnel Management, travelers to the U.S. would have significant reason to be concerned” made by Inserra is irrelevant.\textsuperscript{402} The author bases this argument on the idea, “Social media passwords would be a target for hacktivists, criminals, and nation-state actors.”\textsuperscript{403} Current USCIS policy and practice negates the concern that underpins this argument. Despite an official’s discussion of acquiring users’ social media account passwords, USCIS does not have or seek users’ passwords.\textsuperscript{404} USCIS only collects and uses publicly available information on social media websites.\textsuperscript{405} Travelers to the United States have no basis for concern that their passwords will be hacked while under USCIS control because the agency does not know or store users’ passwords. Inserra’s claim regarding the potential for hacking of users’ passwords is moot because USCIS does not know or possess applicants/petitioners’ social media account passwords.

\textbf{B. CONSTITUTIONAL CONCERNS}

The critics’ allegations that SOCMINT is incompatible with constitutional protections—privacy, free speech, and against discrimination—are unconvincing. USCIS’ SOCMINT does not have the alleged adverse effects. The nature of the data involved, USCIS’ existing non-SOCMINT data collection activities, principles of consent, USCIS training, policy, and safeguards, and USCIS’ rationale for target selection disprove the critics’ allegations. USCIS’ SOCMINT initiative is not in tension with the Constitution.

\textsuperscript{402} Inserra, “The U.S. Should Tread Carefully on Social Media Vetting.”

\textsuperscript{403} Inserra.


1. **Privacy**

The critics contend that SOCMINT is unacceptably intrusive. They frame this intrusion as an unavoidable consequence of SOCMINT. A responsible SOCMINT initiative must not unduly burden privacy expectations. The veracity of the intrusiveness claim would bolster the critics’ constitutional incompatibility argument.

Patel et al.’s argument that collecting data, especially social media data, “intrudes on people’s privacy by allowing [the] government to know the details of their personal lives” is unpersuasive. The nature of the social media data collected, privacy rules, and the information collected from non-social media data collection efforts undermine this argument. First, USCIS SOCMINT only involves open-source information in the public domain, which, as noted previously, has no reasonable expectation of privacy based on the third-party doctrine. Second, USCIS may only access publicly available information, which respects users’ social media privacy settings. Third, USCIS’ application processes, unrelated to SOCMINT data collection, already include, but are not limited to, collection of the following types of data, some of which are very personal in nature:

- legal name, aliases, date of birth, place of birth, gender, address, phone number, and e-mail address;
- immigration history (applicant, spouse, and parents);
- marital history (applicant and spouse);
- details about victimization (human trafficking and criminal);

---

• details about political persecution basis (beliefs, religion, sexual orientation, etc.);

• mental competence;

• employment, education, and travel history;

• details on others (current and former spouses, children, and parents);

• ethnicity and race;

• physical details (fingerprints, height, weight, eye, and hair);

• memberships (organizations, associations, funds, foundations, parties, clubs, societies, etc.);

• prior immigration encounters;

• criminal history on acts and violations (applicant, spouse, and parents);

• intended future criminal acts (illegal gambling, prostitution, bootlegging, child porn, etc.);

• security-related intentions (sabotage, exporting sensitive info, overthrowing government, adverse foreign policy consequences, etc.);

• military training;

• communist, Nazi party, and terrorist organization affiliations;

• public assistance benefits received;

• polygamy;

• medical conditions, diseases, and disabilities;

• taxes, assets, debts, and banking statements;

• divorce decrees;
• civics knowledge and English aptitude;
• moral character;
• extent of alcohol consumption;
• child support obligations;
• honesty in immigration and public assistance benefit matters;
• constitutional support;
• willingness to take oath of allegiance and take up arms;
• photographs; etc.  

In addition to the aforementioned items that are unrelated to SOCMINT data collection, FDNS officers may use commercial databases and public records, site visits, and administrative subpoenas to find further information. Commercial databases and public records are rich sources of personal information. Residential site visits provide details of immigrants’ personal lives, e.g., observation of photographs on living room walls, contents of bedroom closets and drawers, and bathroom vanities, etc. Subpoenas are an effective means for gathering details of immigrants’ personal lives.


USCIS application instructions disclose the background and security checks requirement to which an individual must submit.411 For example, the applicant’s declaration section on a typical form states:

I authorize release of any information from any and all of my records that USCIS may need to determine my eligibility for the immigration benefit that I seek…I furthermore authorize the release of information contained in this application, in supporting documents, and in my USCIS record, to other entities and persons where necessary for the administration and enforcement of U.S. immigration law.412

The applicant’s authorizations of release to USCIS and by USCIS function as consent. Arguably, social media content falls within the broad meaning of “any information from any and all of my records that USCIS may need.”413

Patel et al., ACLU, and EPIC’s contention that vetting programs “sweep up information about American friends, family members, and business associates, either deliberately or as a consequence of their broad scope” and impact millions of people living in the United States, including U.S. citizens, is misleading.414 As noted, USCIS policy delineates that IOs may only access publicly available information, which respects users’ social media privacy settings.415 Therefore, any “sweep up” occurs based on the platform consent of the user, which makes raising this objection outlandish. According to Apple’s Chief Executive Officer Tim Cook, “When an online service is free, you’re not the customer—you’re the product.”416 Facebook ranks as one of the most valuable


413 U.S. Citizenship and Immigration Services, 15.


businesses in the world. The answer is from consenting users. Facebook monetizes users by selling ads based on what it knows about its users. In addition, users’ data is available to third parties. The social media business model is based on the exploitation and commercialization of personal data. Gilbert contends, “Facebook is ‘free,’ but you pay with your personal information.” He explains, “In exchange for accessing the social network, messaging, and the many other free services Facebook offers, users give up their personal information.”

Morrisey argues, “This is how Cambridge Analytica leveraged 272,000 app users into an entrée to access the personal data of 50 million of their friends.” He questions, “But should anyone really be surprised that Facebook allowed access to the personal data of 50 million people to outside firms?” For Morrisey, the answer is no because “[a]fter all, Facebook has been selling such access to advertisers for many years—and no one forces users to provide the data in the first place.” Morrisey warns, “If you don’t want to be the product, don’t sign up in the first place, or short of that, don’t load a bunch of personal data in the expectations that it will be kept private.” USCIS only collects and uses publicly available information on social media websites—data that the users

418 Morrisey.
419 Morrisey.
420 Morrisey.
421 Morrisey.
423 Gilbert.
424 Morrisey, “You’re Not Facebook’s Customer.”
425 Morrisey.
426 Morrisey.
427 Morrisey.
consented to allowing USCIS and anyone else to access. Consequently, Patel et al., ACLU, and EPIC’s argument objecting to vetting programs and the privacy of this data does not withstand scrutiny.

2. Free Speech

The critics theorize that SOCMINT will have adverse implications on free speech. They foresee SOCMINT creating far-reaching, undesirable effects beyond the subjects of inquiry. A viable SOCMINT capability should be structured to create public confidence that freedom of speech is not endangered. Unless mitigated, this contention supports the critics’ concerns about SOCMINT chilling speech.

EPIC, ACLU, and Patel et al.'s contention that SOCMINT will chill free speech because foreign visitors, immigrants, and their family members and friends will self-censor online is misleading. Collectively, the critics have presented a mischaracterization of the SOCMINT initiative that USCIS has deployed. Had their allegations in the previous chapters and sections concerning problems, safety, efficacy, and data been true, then arguably, people might have reason to consider self-censoring when posting on social media. However, as discussed earlier, these claims are false. In addition, USCIS honors First Amendment freedoms. The former USCIS director was emphatic with his directive that:

> Employees will limit collection of information related to First Amendment protected activities that have taken place in the United States or related to activities undertaken by U.S. Citizens abroad to information that is reasonably related to adjudicative, investigative, or incident responses matters.

---


In support of this mandate, officers conducting social media checks are required to “[c]omplete the USCIS Privacy Requirements for Operational Use of Social Media training program and acknowledge they have read and understand the Component Rules of Behavior, on an annual basis.” Officers must also “Complete all training for the operational use of social media offered by FDNS and acknowledge that they have read and understand the Rules of Behavior for that operational use of social media.” In addition, officers must conduct social media research pursuant to the Social Media Operational Use Template approved by the DHS Office of Privacy. Nevertheless, the critics raise an important issue. As with any human-based system, efforts at the front end may not guarantee employee conduct during execution. Policies, procedures, and training are not 100 percent effective, despite best intentions. However, separate investigation, adjudication, and appeal personnel provide multiple, layered opportunities for oversight and course correction, if necessary. USCIS has established policy, procedures, and training in an effort to respect the exercise of freedom of speech consistent with the Constitution and thereby mitigate the risk of SOCMINT chilling free speech.

3. Discrimination

SOCMINT, in the eyes of the opposition, exacerbates exiting concerns over discrimination. The opponents equate SOCMINT to efforts akin to the Muslim travel ban. An ethical SOCMINT capability should identify and address potential threats on their merits and not discriminate based on religion or ethnicity. If incontrovertible, the opposition’s argument about discrimination creates a compelling justification for scrapping SOCMINT.

Handeyside and Cagle’s contention that DHS’ social media screening “lacks protections against discrimination and profiling” and has a risk of abuse is debatable. The authors base their claim on limited information from redacted USCIS SOCMINT

\[431\] Rodriguez, 1442.
\[432\] Rodriguez, 1442.
\[433\] Rodriguez, 1442.
documentation on research and development findings. Handeyside and Cagle opine that “internal reviews obtained through FOIA from U.S. Citizenship and Immigration Services show that its social media screening efforts lacked protections against discrimination and profiling.” In support of this allegation, Handeyside and Cagle cite Sternstein. According to Sternstein, “Civil rights groups who reviewed the USCIS [FOIA] documents say that their wording suggests the social media program is targeting foreigners from predominantly Muslim nations.”

The absence of policy discussions concerning “discrimination and profiling” in a research and development report does not prove, however, that the appropriate protections do not exist. The protections are a matter more appropriately memorialized in policy documents and standard operating procedures, not research and development findings involving a social media tool assessment. The authors thus offer unconvincing evidence to support their claim about the risk of abuse.

Patel et al.’s question on whether SOCMINT “disproportionately targets Muslims and those from Muslim-majority countries” is shortsighted. The populations chosen for SOCMINT research and development testing are not dispositive on what populations will be screened when a fully deployed operational capability is launched. Government, like industry, routinely tests new initiatives on subsets of populations. USCIS made it clear that its efforts were not disproportionately focused. For example, internal reports indicate, “USCIS also intends to pilot the expansion of the use of social media to other cases/benefit request types.” USCIS made good on that promise.

---

435 Handeyside and Cagle, 3.
DHS began social media research and development projects in 2015. The *Proposed Refugee Admissions for Fiscal Year 2017* report details the number of admissions of refugees by country for fiscal year 2015. Analysis of “TABLE III Refugee Arrivals By Country of Origin Fiscal Year 2015” indicates that 91.4 percent of arriving refugees come from a mere 10 of the 59 countries that involve refugee admission: Burma, Iraq, Somalia, Democratic Republic of Congo, Bhutan, Iran, former Soviet Union, Syria, Eritrea, and Sudan. Five of these countries are alleged “Muslim-ban” countries: Iraq, Somalia, Iran, Syria, and Sudan. The Department of State estimates that 50 percent of the Eritrea population is Sunni Muslim. Therefore, a majority of the top 10 refugee countries are Muslim. Creating a new initiative requires a starting point. Arguably, it makes sense to research and develop a SOCMINT capability that is sensitive to the cultural, linguistic, etc., nuances of a group that represents the majority of the total refugee population that needs to be vetted. However, USCIS did not focus its SOCMINT efforts exclusively on refugees.

In 2016, DHS conducted a number of research and development projects to review “social media information across a number of high priority application populations, including refugees and [emphasis added] Visa Waiver Program travelers.” The 38 Visa Waiver Program countries are not generally considered Muslim countries. USCIS commenced its SOCMINT testing with a population choice based on refugee statistics and then expanded it to a population that includes 38 non-

---


442 Department of State, Department of Homeland Security, and Department of Health and Human Services, 62–64.


Muslim countries, which dispels any myths concerning the disproportionate targeting of Muslims.

C. CONCLUSION

The critics’ data management issues argument is unconvincing. Data retention benefits both the agency and those seeking immigration benefits. DHS has instituted strict data sharing protocols, and has implemented safeguards to mitigate the critics’ misinterpretation concerns. The retention of social media data presents no more hacking risk than other government data holdings. Consent, the nature of the social media data collected, privacy rules, and other non-social media data collected by DHS persuade against the critics’ privacy contentions. SOCMINT is not in conflict with constitutional protections. The DHS’ deployment of SOCMINT across a broad group of vetting populations forecloses accusations about discrimination against certain groups. DHS has policy, procedures, and training in place to honor freedom of speech. However, humans are not infallible. Therefore, USCIS must maintain strong, layered oversight mechanisms to mitigate the critics’ legitimate concerns about chilling speech. In sum, the merits of the critics’ claims about data and constitutional concerns fail to convince. The next chapter presents recommendations and conclusions based on the propositions for SOCMINT and the analysis of objections and rebuttals contained in this chapter and in the preceding two chapters.
VI. CONCLUSIONS AND RECOMMENDATIONS

Homegrown violent extremism abetted by the reach and power of contemporary social media has completely changed national security today.

—Bruce Hoffman, author,
Inside Terrorism

Balancing the security needs of the U.S. with the efforts to welcome immigrants must be a coordinated effort. The weight of this charge does not rest solely on the shoulders of the immigration services of the country, it requires input and cooperation from several agencies and departments within the government as well as the support of Congress and the American People.

—Julie Farnam, author,
U.S. Immigration Laws under the Threat of Terrorism

Terrorists use the internet to disseminate propaganda, solicit new members, communicate, gather intelligence, seek money, and inspire and plan attacks. Their use provides an opportunity for DHS to leverage SOCMINT to secure the homeland. This thesis explored the necessity and efficacy of open-source SOCMINT in identifying potential fraud, public safety, and/or national security concerns from immigrants seeking immigration benefits from USCIS. This thesis examined qualitative data of the issue rhetoric—the debate and discussion—between the critics and supporters of implementing SOCMINT. In addition, quantitative data from the PIRUS dataset provided insight into the viability of using SOCMINT to identify threats among immigration benefit seekers.

A. SUMMARY

USCIS “administers the nation’s lawful immigration system, safeguarding its integrity and promise by efficiently and fairly adjudicating requests for immigration benefits while protecting Americans, securing the homeland, and honoring our

446 Coats, Worldwide Threat Assessment of the U.S. Intelligence Community, 6.
USCIS began conducting SOCMINT research and development projects to test the automation of “bulk screening of social media information” supplemented with human analyst “review across a number of high-priority populations.” The OIG investigated and reported on DHS’ efforts as if they were pilots versus research and development projects. Based in part on the OIG findings and FOIA-released documents, the skeptics of SOCMINT argue against its use. The skeptics contend that the number of social media platforms, posts, and foreign languages used, context ambiguities, constitutional implications, data management issues, and targets’ evasion efforts make the DHS open-source SOCMINT capability unviable.

1. **Propositions for SOCMINT**

As discussed in Chapter II, the PIRUS dataset reveals that approximately 10 percent of individuals who have radicalized have had contact with the lawful immigration system. The internet and social media played a significant role for the majority of those who radicalized. The internet played a role in terrorist plots for radicalized immigrants who use social media. For example, almost 87 percent used the internet for logistics or communication in preparation of a violent plot. One-third of these subjects were doers versus talkers in that they acted on carrying out their terrorist plots. Over 61 percent of the subjects used social media at least daily in a manner that related to radicalization and/

447 U.S. Citizenship and Immigration Services, “About Us.”
448 Department of Homeland Security, “Written Testimony of I&A Under Secretary Francis Taylor.”
449 Roth, *DHS’ Pilots for Social Media Screening*, 4.
or plot mobilization. Almost 10 percent directly communicated with members of an extremist group on social media to facilitate a domestic attack. Only 70 percent used operational security measures to hide or conceal preparation for the plot. These figures indicate an opportunity and need to use SOCMINT to identify fraud, public safety, and/or national security threats among immigration benefit seekers. The figures support Nissen’s argument that terrorists have weaponized social media.\textsuperscript{451} State, local, federal, and international LEAs are using social media, in turn, to identify potential terrorists. While critics have questioned the efficacy of using open-source SOCMINT to stop terrorism, the LEA proponents of SOCMINT have achieved successful results for years.

2. **SOCMINT Problematic Effort and Necessity Concerns**

Despite the evidence that deploying a SOCMINT capability will likely play a vital role in USCIS’ obligation to secure the homeland, the critics put forth a series of objections to SOCMINT. A broader, balanced analysis of the OIG report and FOIA-released documents, however, undermines the allegation that efforts to deploy a SOCMINT capability to date have been fraught with problems. Nevertheless, the critics raise insightful concerns about the value of evaluating efforts and policy and procedure. USCIS’ deployed operational capability must continue to heed those concerns. Insights from the 9/11 Commission and other experts, a more fulsome reading of the OIG and FOIA-released documents, and the PIRUS dataset undermine the argument that the nation is safe enough without SOCMINT.

3. **SOCMINT Efficacy Concerns**

The critics also identify an assortment of issues that call into question the efficacy of SOCMINT including yield, scope, scale, language, context, encryption, and identity resolution challenges. A broader, balanced analysis of the OIG report and FOIA-released documents, though, refutes the claims about yield in identifying threats. Security experts’ opinions, LEAs’ use of and their successes with SOCMINT, and the PIRUS research provide evidence that SOCMINT can improve the nation’s security. The critics’

\textsuperscript{451} Nissen, \textit{TheWeaponizationOfSocialMedia}, 10.
automation argument about scope and scale is unpersuasive because USCIS is not relying on automated SOCMINT for the process of reviewing posts. Safeguards are in place to mitigate language and context misinterpretation and any potential derivative adverse outcomes. Nevertheless, the critics’ interpretation concerns demand USCIS’ continued vigilance because any human-based system is fallible. The PIRUS dataset contradicts the critics’ encryption claim for both internet users and social media users. The critics’ claim about identity resolution is therefore questionable.

4. **SOCMINT Data and Constitutional Concerns**

Those opposing the SOCMINT initiative insist that it creates a variety of ancillary problems related to data management: data retention, sharing, and security. Social media data retention has multiple benefits for immigrants and the agency, and safeguards exist to mitigate the risk of misinterpretation at a later time. The critics’ arguments about misinterpretation from data sharing are unpersuasive because there is no reasonable expectation of privacy in open-source social media data. Nonetheless, USCIS imposes strict sharing protocols, which are actually a “higher” standard for sharing than the originating user. The argument regarding the potential for hacking of users’ passwords is inapt because USCIS does not collect social media account passwords.

The critics also argue that the SOCMINT capability is incompatible with constitutional protections. The nature of the social media data collected, privacy rules, and the information collected from non-social media data collection efforts undermine the argument about SOCMINT privacy intrusiveness. USCIS has implemented policy, procedures, and training in an effort to respect the exercise of freedom of speech consistent with the Constitution. USCIS’ efforts thereby mitigate against the risk of SOCMINT chilling free speech. USCIS nonetheless must maintain strong, layered oversight mechanisms to mitigate the critics’ legitimate concerns about chilling speech. USCIS’ SOCMINT vetting activity involving refugees and a population that includes 38 non-Muslim countries counters myths concerning the disproportionate targeting of Muslims.
B. LIMITATIONS

Although the research in this thesis supports the continued deployment of SOCMINT to assist in achieving USCIS’ mission, the study experienced several limitations. The first limitation relates to bias potential. As the author is an FDNS officer, a SMD certified SOCMINT officer, and former member and lead on the SMTF, the potential for bias does exist. This thesis nonetheless attempts to remain analytically neutral and allow the propositions for and against SOCMINT to flourish based on their fact-based merit. A second limitation was the nature of the research and discussion. Much of DHS’ work in this sphere is classified as top secret and takes place in sensitive compartmented information facilities. However, the research and discussion in this thesis relies exclusively on publicly available information. This reliance was unavoidable because comprehensive threat and tradecraft disclosures might provide threat actors a blueprint for evasion. Other limitations were related to policy and technology.

SOCMINT is a dynamic space in terms of how threat and technology affect policy. The research and conclusions of this thesis contemplate the current threat environment and technological capabilities as policy drivers. Technological advances impact wrongdoers’ opportunities to achieve their ends and the homeland security enterprise’s capability to thwart the wrongdoers’ efforts. A contemporary assessment of SOCMINT therefore must embrace these policy drivers.

C. RECOMMENDATIONS

Potentially allowing threats to go undetected ignores USCIS mission mandates. Ignoring reasonable lines of investigative inquiry violates public trust.\(^{452}\) Hypothetically, if it became known that USCIS failed to identify discoverable threats, USCIS would likely face scrutiny from the public and internal stakeholders, such as Congress, the OIG, the GAO, etc. Consequently, there are a number of recommendations that flow from the research and analysis contained in this thesis.

\(^{452}\) Clapper, *Domestic Approach to National Intelligence*, 3.
USCIS should continue to use open-source SOCMINT to identify fraud, public safety, and/or national security threats. Agile leveraging of authorities and technology to meet threat identification needs is critical. It is important to look broadly beyond DHS for expertise and best practices on SOCMINT among law enforcement agency partners’ initiatives, e.g., Social Media the Internet and Law Enforcement conferences, Five Eyes members, and ROSM.453

Wells warns of the adverse effect on the public perceptions of SOCMINT initiatives when the subjective narratives are not addressed.454 Ignoring the opposing narratives and failing to engage the grievances and misconceptions fosters a lack of public clarity.455

DHS should use care in appropriately designating efforts as pilots or research and development projects and ensure a unified understanding, management, and messaging across DHS components. DHS components should resist merely concurring with OIG findings to silence concerns versus defending actions on their merits. Senior DHS leadership should publicly defend ill-informed narratives from critic and media echo chambers that confound fact-based public interpretation of DHS initiatives.

After conducting SOCMINT research and development projects using DARPA and commercial tools, DHS identified technical challenges that may continue to serve as obstacles in deploying the most robust SOCMINT capability. Conversely, the UK pursued a collaborative approach to tool development with TENSOR and DANTE. The UK partnered with different countries, different LEAs, academia, and industry forming consortiums and using advisory boards. The TENSOR and DANTE projects purport to

---

453 Inspectors General of the Intelligence Community, Department of Homeland Security, and Department of Justice, Review of Domestic Sharing of Counterterrorism Information, 8.


455 Wells, 58–63.
have addressed the identical technical and privacy challenges that DHS’ efforts encountered.

Organizationally, a successful SOCMINT capability requires a clear vision, unity of effort, and momentum. Each of these requirements flourishes under an unambiguous articulation and execution of commander’s intent. Centralization, in the form of a COE or hub, of the SOCMINT efforts has desirable benefits. Best practices, lessons learned, and intelligence are easily shared. DHS component members who would comprise the COE could avoid duplicate development and maintenance costs, innovation failures, etc. This avoidance is particularly critical in technology endeavors where change and updates are exponentially recurring. Participants in the UK’s OSINT Hub tout the benefits of yielding state-of-the-art tools, the generation and access to actionable intelligence, coordination, cost avoidance, innovation, among other things—all resulting in better decision making in the fight against terrorism.

- DHS should consider supplementing the open solicitation and commercial tool approach for SOCMINT tool development in favor of a model more aligned with the UK’s DANTE and TENSOR project approaches.456

- DHS should research the viability of creating a centralized COE for DHS’ SOCMINT capability modeled on the UK’s CENTRIC OSINT Hub.457

SOCMINT policies should provide optimal threat detection and actionable intelligence useful to decision makers.458 However, this outcome requires sensibly constructing efforts designed to achieve a balance between security and liberty by


457 Akhgar, “OSINT as an Integral Part of the National Security Apparatus,” 8.

listening to those who have an interest in the outcome.\textsuperscript{459} This stakeholder consideration helps foster enhanced public trust.\textsuperscript{460}

- USCIS should ensure data and constitutional protections are robust. Policies, procedures, and training are in place to prevent problems. However, as with any human-based system, efforts at the front end may not guarantee employee conduct during execution. Policies, procedures, and training are not 100 percent effective, despite best intentions. Consequently, USCIS must also remain equally vigilant in its oversight efforts to protect the principles of our homeland.

D. FUTURE RESEARCH

In light of the results of this study, several recommendations for future research can be proffered. First, this thesis focused on DHS, specifically USCIS, SOCMINT efforts. However, the war on terrorism is truly global and affects many agencies and countries. Partnering and information sharing are key tenets of success in the fight against terrorism. Future studies could explore in detail how other LEAs, foreign and domestic, specifically deploy tradecraft to conduct SOCMINT programs successfully. Such an effort would require a thesis audience restricted to law enforcement personnel, but might enhance USCIS success with SOCMINT.

Second, this study only considered evasion from detection by use of operational security, such as encryption. However, the social media platform operators’ takedowns can also affect detection, e.g., when platforms remove terrorism content and suspend accounts. Future studies could explore how platform operators make those takedown decisions, the takedowns’ effect on LEAs’ monitoring of terrorist networks, the takedowns’ effect on LEAs’ undercover operations, and the potential for private and public sector collaboration to enhance safety.

\textsuperscript{459} National Commission on Terrorist Attacks upon the United States, \textit{The 9/11 Commission Report}, 386.

Third, this study did not take a deep dive into the SOCMINT tool technology. As technology changes, new or improved tool capabilities for enhanced detection may appear. Future studies could assess the emerging state of the art of natural language processing, sentiment analysis, deep neural networks, image classifiers, etc. This research may assist DHS in ensuring it is consistently leveraging the best in class as technology changes.

Fourth, this study considers only USCIS’ research and development efforts for tool development and capability deployment. Other agencies and countries have taken different approaches to SOCMINT tool development and organizational capability deployment. As alluded to in the aforementioned recommendations, future studies could comparatively explore the UK’s TENSOR and DANTE initiatives and OSINT Hub architecture. This research may assist DHS in ensuring it is using optimal SOCMINT tools and operating its SOCMINT capability in an optimal organizational structure.

E. CONCLUSION

Social media has changed the world, in part by presenting new threat and detection opportunities for terrorism. Open-source SOCMINT offers USCIS a contribution in assisting with its homeland security mission. Despite the poor assessment narratives flourishing in the critics’ echo chamber, SOCMINT could be a successful and effective means to identity threats among immigration benefit seekers as long as USCIS adheres to its dual-obligation to use SOCMINT to secure the homeland while being mindful of the aforementioned data and constitutional concerns. The benefits of SOCMINT, overall, outweigh the potential for harm.
APPENDIX. PROFILES OF INDIVIDUAL RADICALIZATION IN THE UNITED STATES

Figure 11. Profiles of individual radicalization in the United States, Keshif data visualization tool\textsuperscript{471}

\textsuperscript{471} Adapted from National Consortium for the Study of Terrorism and Responses to Terrorism (START), “Profiles of Individual Radicalization in the United States (PIRUS).”
LIST OF REFERENCES


123


INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California