FIU Law Review

Volume 13
Number 3 *A Summit on the Future of Legal Education and Entry to the Profession*

Article 9

Spring 2019

Full Transparency: A Case Against The Collection of Internet Information in Trump-Era American Immigration

Thomas P. Campbell
J.D. candidate, 2019, Florida International University (FIU) College of Law

Online ISSN: 2643-7759

Recommended Citation
Thomas P. Campbell, *Full Transparency: A Case Against The Collection of Internet Information in Trump-Era American Immigration*, 13 FIU L. Rev. 513 (2019).
DOI: https://dx.doi.org/10.25148/lawrev.13.3.9

FULL TRANSPARENCY: A CASE AGAINST THE COLLECTION OF INTERNET INFORMATION IN TRUMP-ERA AMERICAN IMMIGRATION

Thomas P. Campbell*

ABSTRACT

The Department of Homeland Security recently posted a Notice in the Federal Register informing of an update to the immigrant tracking database known as the "Alien Files." The Notice stated that the A-Files database will now store: "social media handles, aliases, associated identifiable information, and [internet] search results." On October 28, 2017, the policy change outlined in the Notice went into effect. This Comment critically analyzes the new DHS policy, while considering the various legal, social, and practical concerns associated with this policy. This is a case against the DHS's collection and storage of immigrant social media information.

I. Introduction 514
II. Background 517
A. Social Media Use and Privacy 517
B. The Language in the Notice 519
C. Legal Authorities Protecting Citizen Data from Government Intrusion 521
1. Amendment IV to the United States Constitution 521
2. The Privacy Act of 1974 and E-Government Act of 2002 522
3. The Electronic Communications Privacy Act of 1986 524
4. International Privacy Safeguards 525
III. Analysis 527
A. Mass Collection of Data Does Not Adequately Detect Crime 527
B. Controversial Constitutionality 530
C. Violation of International Law 532
D. Modern Issues with Social Media and Identity 535

---

*J.D. candidate, 2019, Florida International University (FIU) College of Law; B.S. Legal Studies, 2016, Nova Southeastern University. I wish to thank my family for their constant love and support. Special thanks to Professor Juan Carlos Gómez, Director of the Carlos A. Costa Immigration and Human Rights Clinic, for your insight and inspiration throughout the writing process. I am indebted to my colleague Alexandra Mullenax, for your invaluable critiques, edits, and encouragement. Thank you to the *FIU Law Review* Editorial Board and Staff for working so tirelessly on my Comment and this entire issue. I am especially grateful to Alexa Duarte, Articles Editor; Annasofia Roig, Executive Managing Editor; Adrian Karborani, Editor-in-Chief; and everyone else who devoted time to my Comment. I dedicate this article to my late grandmother, Kelly T. Silky (10/22/36–2/3/19).

E. Relevant User-Submitted Comments.....537
IV. Conclusion.....539

I. INTRODUCTION

On September 18, 2017, the Department of Homeland Security ("DHS") posted a notice in the Federal Register (the "Notice") explaining a change in the Alien Files ("A-Files") system.[1] The Notice states that, effective October 18, 2017, a new A-Files system will collect, monitor, and store the social media activity of individuals who are subject to the Immigration and Nationality Act ("INA").[2] This policy would cover lawful permanent residents ("LPRs"), Naturalized United States Citizens, individuals petitioning for INA benefits, legal guardians of the disabled, and any other persons subject to the vast provisions of the INA.[3] The DHS intends to store "social media handles, aliases, associated identifiable information, and search results" in its updated A-Files system.[4]

On October 18, 2017, the customary 30-day comment period officially ended, and the policy specified in the Notice went into effect.[5] During the comment period, 2,994 public comments were submitted.[6] The vast majority of these comments were submitted by individuals offering scathing critiques of the new DHS policy.[7] These comments varied in tone, some offered by esteemed law professors, others offered by worried (and often enraged) private citizens.[8] Some of the more compelling comments will be highlighted here.

Criticisms were not limited to this axiomatic "comment section." United States Representative Ted Lieu spoke out against the new policy and

---

1 *See* Privacy Act of 1974; System of Records, 82 Fed. Reg. 43,556 (proposed Sept. 18, 2017) [hereinafter DHS Notice].

2 *Id.* at 43,556–57.

3 *Id.* at 43,559.

4 *Id.* at 43,557, 43,560.

5 *Id.* at 43,556.

6 *See DHS/USCIS-001 Alien File, Index, and National File Tracking System of Records*, REGULATIONS.GOV, https://www.regulations.gov/docketBrowser?rpp=50&so=DESC&sb=postedDate&po=0&dct=PS&D=DHS-2017-0038 (last visited Oct. 12, 2018).

7 *See id.*

8 *Compare Comment Submitted by Catherine Martinez, Members of the Yale Law School Community*, REGULATIONS.GOV (Oct. 19, 2017), https://www.regulations.gov/document?D=DHS-2017-0038-2986 [hereinafter *Comment by Catherine Martinez*], *with* Megan Hughes, *Comment Submitted by Megan Hughes*, REGULATIONS.GOV (Oct. 20, 2017), https://www.regulations.gov/document?D=DHS-2017-0038-2994.

addressed a letter to then-acting United States Secretary of Homeland Security, Elaine Duke.[9] Representative Lieu began by explaining that he is a naturalized citizen who has lived in the United States for over four decades.[10] Representative Lieu worriedly stated that he was "deeply concerned" that the proposed rule would apply to United States citizens such as himself.[11] He even demanded that the DHS provide further details and clarifications, as related to some of the more ambiguous provisions in the Notice.[12] To date, these clarifications have not been provided.

Critics and skeptics do have a legitimate reason to be worried. At the moment, the United States is one of the largest consumers of social media in the world.[13] Social media usage in the United States is at an all-time high.[14] According to Statista, 81% of the United States population currently utilizes social media.[15] Unsurprisingly, this number is even higher among young Americans.[16] Statista estimates that 86% of young adults (ages 18–29) utilize social media.[17] Because social media is so heavily relied upon in the United States, the new DHS policy can impact a myriad citizens and noncitizens alike.

In wake of the recent outcry, a spokesperson at the DHS has explained to multiple news outlets that the Notice is not new policy.[18] Joanne Talbot, the DHS spokesperson, explained that the Notice is actually "an effort [by the DHS] to be more transparent."[19] In an email to ARStechnica.com, Talbot further explained that the Notice is only an amendment to a 2012 DHS policy

---

9 Cyrus Farivar, *Congressman Demands to Know if DHS Will Collect His Social Media History, Too*, ARSTECHNICA (Sept. 30, 2017, 9:00 AM), https://arstechnica.com/tech-policy/2017/09/congressman-demands-to-know-if-dhs-will-collect-his-social-media-history-too/; Ted. W. Lieu, *Letter to the Honorable Elaine Duke* 1, 1 (2017), https://assets.documentcloud.org/documents/4063724/Letter-to-DHS-Social-Media.pdf.

10 *Id.*

11 *Id.*

12 *Id.*

13 *Social Media Usage in the United States - Statistics & Facts*, STATISTA, https://www.statista.com/topics/3196/social-media-usage-in-the-united-states/ (last visited Apr. 17, 2018).

14 *See id.*

15 *Id.*

16 *Id.*

17 *Id.*

18 *See* Fariviar, *supra* note 9; Joel Rose, *Federal Plan To Keep Files Of Immigrant Social Media Activity Causes Alarm*, NPR (Sept. 30, 2017, 5:00 AM), https://www.npr.org/2017/09/30/554557044/federal-plan-to-keep-files-of-immigrant-social-media-activity-causes-alarm.

19 Rose, *supra* note 18.

titled *Privacy Policy for Operational Use of Social Media*.[20] Talbot also explained that "[t]he Federal Register Notice states that previously captured information from any social media checks that took place up to naturalization will remain in the naturalized citizens [sic] Alien File, otherwise known as the A File. By law, USCIS will not continue to check the social media accounts of naturalized citizens."[21] This clarification may reflect alleged internal protocol, but it seemingly contradicts the explicit language within the Notice.

As the DHS spokesperson's comments emphasized, the language in the Notice is extremely important to the overall comprehension of the new policy. Unfortunately, the language in the Notice is convoluted and difficult to follow.[22] The most concise summary of the new policy to be implemented can be found in the Notice section titled "*I. Background*."[23] This section neatly explains that the "DHS is updating the DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records to include the following substantive changes."[24] The Notice then lists 12 changes.[25] Provision (5) of the list explains that the DHS will now "expand the categories of records to include country of nationality; country of residence; the USCIS Online Account Number; social media handles, aliases, associated identifiable information, and search results."[26] It is this new policy that has sparked the public outcry.

The DHS should promptly halt the collection of immigrant social media information. This Comment addresses the new DHS policy as follows. Part II below sets the stage, introducing the background information necessary to comprehend the issue. Part III begins the analysis, delving deeper into the many issues associated with the new DHS policy. Part IV concludes, settling the case against the Federal collection of immigrant social media information.

---

20 Farviar, *supra* note 9; *see generally* DEP'T OF HOMELAND SEC., PRIVACY POLICY FOR OPERATIONAL USE OF SOCIAL MEDIA 1 (2012), https://www.dhs.gov/sites/default/files/publications/Directive_110-01_Privacy_Policy_for_Operational_Use_of_Social_Media_0.pdf.

21 Farviar, *supra* note 9.

22 *See* DHS Notice, *supra* note 1.

23 *Id.* at 43,557.

24 *Id.*

25 *Id.* at 44,357–58.

26 *Id.* at 43,557.

II. BACKGROUND

A. Social Media Use and Privacy

As the internet grows, communication on the web has become extremely common. Essentially all of our communication takes place via the internet. Unsurprisingly, social media has become the bedrock of American culture.[27] In 2016, researchers determined that nearly 80% of online Americans use Facebook, with another 24% utilizing Twitter.[28] With so many social media users, exactly how private are these modern modes of communication?

United States courts have found that information posted to social media is not as private as a user may assume.[29] In *People v. Harris*, the New York Criminal Court recently explained that Twitter posts are not considered private information.[30] The court reiterated that any information released to a third-party should not be construed as private communication.[31] The court reasoned:

> If you post a tweet, just like if you scream it out the window, there is no reasonable expectation of privacy. There is no proprietary interest in your tweets, which you have now gifted to the world. This is not the same as a private email, a private direct message, a private chat, or any of the other readily available ways to have a private conversation via the Internet that now exist.[32]

The court also explained that any posts or revelations to a third-party social media provider, such as "Twitter, Facebook, Instagram, Pinterest, or the next hot social media application," would not be considered private.[33] This jurisprudential concept is known as the third-party doctrine.

This third-party doctrine was originally set forth by the United States Supreme Court in *Smith v. Maryland*, back in 1979.[34] In this seminal case, an accused burglar was making threatening telephone calls to the victim of his

---

27 *See generally* SHANNON GREENWOOD, ANDREW PERRIN & MAEVE DUGGAN, PEW RESEARCH CTR., SOCIAL MEDIA UPDATE 2016: FACEBOOK USAGE AND ENGAGEMENT IS ON THE RISE, WHILE ADOPTION OF OTHER PLATFORMS HOLDS STEADY 1 (2016), http://assets.pewresearch.org/wp-content/uploads/sites/14/2016/11/10132827/PI_2016.11.11_Social-Media-Update_FINAL.pdf.

28 *Id.* at 3.

29 *See, e.g.*, People v. Harris, 36 Misc. 3d 868, 949 (N.Y. Crim. Ct. 2012).

30 *Id.* at 872.

31 *Id.* at 872–73.

32 *Id.* at 874.

33 *Id.* at 873.

34 Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

prior crime.[35] At police request, the telephone company installed what was known as a "pen register" to track and record all dialed phone numbers coming from the suspect's home phone.[36] The police did not obtain a warrant for the pen register.[37] The suspect argued that the police had violated his Fourth Amendment right to be free from unreasonable search and seizure.[38] The question—whether the installation of the pen register constituted an illegal search—hinged upon whether the suspect had a "'legitimate expectation of privacy' regarding the numbers he dialed on his phone."[39]

Surprisingly, the Supreme Court held that there was no "legitimate expectation of privacy" attached to dialed telephone numbers.[40] The Court explained that when people dial telephone numbers, the telephone company is receiving and potentially making permanent record of these numbers.[41] "This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[42] The Court further explained that the "petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment . . . [i]n so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed."[43] Thus, the third-party doctrine was born. The ever important Fourth Amendment protection—the right to be free from unreasonable search and seizure—officially wilted.

The Supreme Court has never officially applied the third-party doctrine to internet-based communication.[44] Still, legal experts have developed various theories pertaining to the application of the third-party doctrine to online communication. One such application is known as "waiver theory."[45] Waiver theory explains that "a [social media] user consents to revealing . . . information to the ISP and thus seemingly forfeits any protection over the transmission. The user made a voluntary choice to sign an agreement before opening an account, acknowledging that Facebook will hold the user's communications."[46] It thus follows that no Fourth Amendment protection

---

35 *Id.* at 737.

36 *Id.* at 737–38.

37 *Id.* at 737.

38 *Id.* at 738–39.

39 *Id.* at 742.

40 *Id.*

41 *Id.*

42 *Id.* at 743–44.

43 *Id.* at 744.

44 Monu Bedi, *Facebook and Interpersonal Privacy: Why the Third Party Doctrine Should Not Apply*, 54 B.C. L. REV. 1, 3 (2013).

45 *Id.* at 15–17.

46 *Id.* at 16–17.

would be afforded, because internet-based communications are not afforded an objective expectation of privacy.[47]

Ultimately, the third-party doctrine leaves a vast amount of information exposed and unprotected by the Fourth Amendment. For example, information associated with credit card transactions, phone records, and cell phone locations would probably not be protected.[48] The United States government has been given significant leeway to collect and store information transmitted via the internet. Both citizens and noncitizens alike could be subject to significant data collection due to internet use, without any legitimate constitutional redress. Almost 40 years ago, long before the existence of the internet and social media, the Supreme Court made a decision that time has proven unreasonable. Now that internet is so indispensable to every aspect of modern life, governmental oversight bodies can easily justify the collection of social media data as being in tune with the Supreme Court jurisprudence in *Smith v. Maryland*.[49]

B. The Language in the Notice

As previously mentioned, the Notice is lengthy, confusing, and riddled with bullet points. It is important, however, to examine the Notice language thoroughly. If the information contained in the Notice is truly an "effort [by the DHS] to be [more] transparent,"[50] this language is of the utmost importance.

The Notice begins by stating that the outdated, partially paper-based A-Files system is set to be clarified and updated.[51] The Notice introduces these changes in the "*Supplementary Information*" section.[52] This section states that each immigrant alien has an A-File, which corresponds with their Alien Number.[53] The Notice then explains that the United States Citizenship and Immigration Services ("USCIS") is the custodian of the A-Files system.[54] This filing system is jointly contributed to by the USCIS, United States Immigration and Customs Enforcement ("ICE"), and United States Customs and Border Protection ("CBP").[55]

---

47 *Id.*

48 *See* Note, *Data Mining, Dog Sniffs, and the Fourth Amendment*, 128 HARV. L. REV. 691, 691–92 (2014).

49 *See generally* Smith v. Maryland, 442 U.S. 735 (1979).

50 Rose, *supra* note 18.

51 DHS Notice, *supra* note 1, at 43,557.

52 *See id.* at 43,556.

53 *Id.*

54 *Id.* at 43,557.

55 *Id.*

The next section, titled "*I. Background*," reiterates and further expounds upon the policy that is to change.[56] As previously mentioned, this section sets a list of substantive changes to the current A-Files system, including the "expan[sion] [of] categories of records to include . . . social media handles, aliases, associated identifiable information, and search results."[57] This section also clarifies the legality of the proposed data collection scheme.[58] It explains that because the A-Files system is a "system of records," it is governed by the Privacy Act of 1974.[59] A system of records is defined as "any records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual."[60] The Privacy Act defines the term "individual" as someone "encompass[ing] U.S. citizen[ship] and lawful permanent residents."[61]

In a later section titled "*Purpose(s) of the System*," the DHS explains and attempts to justify its newly proposed policy.[62] The purpose of this new program is to create an official record of an "individual's immigration applications, petitions, and requests, as well as enforcement transactions as he or she passes through the U.S. immigration process."[63] Earlier in the Notice, the DHS explained that the USCIS, in conjunction with the DHS, is responsible for processing "applications and petitions submitted for citizenship, asylum, and other benefits."[64] Thus, according to the Notice, this new A-Files system is meant to streamline the process and prevent fraudulent applications from being granted.[65]

Another important section in the Notice is aptly titled "*Categories of Individuals Covered by the System*."[66] Individuals covered by the system include LPRs, naturalized United States citizens, individuals petitioning for benefits on behalf of another, individuals acting as a guardian on behalf of a disabled individual, individuals who receive benefits, and individuals who are subject to enforcement provisions.[67] The system also covers: anyone who is subject to the INA and is under investigation for national security purposes;

---

56 *Id.* at 43,557–59.

57 *Id.* at 43,557.

58 *See id.*

59 *See id.*

60 *Id.* at 43,559.

61 *Id.* at 43,559.

62 *See id.* at 43,558.

63 *Id.*

64 *Id.* at 43,557.

65 *Id.* at 43,557–59.

66 *Id.* at 43,558.

67 *Id.*

anyone who was investigated in the past; anyone who is suspected of having violated any non-INA immigration provision; and anyone with information related to certain INA violations.[68] Essentially, anyone who has come in contact with the United States immigration system is subject to the new policy.[69]

Despite the overwhelming amount of information in the Notice, it also contains some shockingly underdeveloped provisions. Specifically, it contains no limiting language or oversight provisions. Astonishingly, the Notice states that the information collected in the A-Files system "may be shared with [the] appropriate Federal, State, local, tribal, territorial, foreign, or international government agencies."[70] With so much leeway being afforded to the DHS, the lack of restraint associated with this new governmental policy is extremely evident and troublesome.

C. Legal Authorities Protecting Citizen Data from Government Intrusion

It is clear that the United States government has granted itself a lot of freedom to monitor. Still, there are some privacy protections in place designed to protect against government overreach. Unfortunately, these protections are mostly inadequate, and do not stop the United States government from monitoring immigrants. Relevant United States domestic legislation and international privacy protections are examined below.

1. Amendment IV to the United States Constitution

In the United States, one of the most sacred and revered protections against unwarranted governmental intrusion is embedded in the Constitution.[71] The Fourth Amendment to the United States Constitution reads as follows:

> The right of the people to be secure in their persons, houses, papers, and effects, *against unreasonable searches and seizures*, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[72]

---

68 *Id.*

69 *See id.*

70 *Id.* at 43,558.

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

72 *Id.* (emphasis added).

The Fourth Amendment features very specific language written centuries ago—long before the existence of Facebook or Twitter. The question thus becomes, will this language protect the social media information of immigrants in today's modern society?

Courts have wrestled with this question and reached puzzling conclusions. In *United States v. Meza-Rodriguez*, the Seventh Circuit examined the Fourth Amendment's usage of the words "the people," in an attempt to determine if noncitizens are afforded Fourth Amendment protections.[73] The court applied the *Verdugo-Urquidez* Supreme Court rationale and concluded that, for Fourth Amendment protections to apply, an alien must show "'substantial connections' with [the United States]."[74] Further, the Supreme Court in *Plyler v. Doe* simply stated that, "an alien is surely a 'person' in any ordinary sense of that term."[75] When surveillance occurs within the United States, the assumption is that the associated "person" is entitled to Fourth Amendment protections, whereas outside the United States the reverse is the case.[76] Even immigrant aliens within the United States would seemingly be granted Fourth Amendment protections as "persons."[77]

However, as explained above, the Supreme Court in *Smith v. Maryland* set forth the third-party doctrine, essentially whittling away Fourth Amendment protections as applied to data collected via a third-party.[78] The Court explained that despite some subjective expectations,third-party facilitated communications are private, andthere isno objectively reasonable expectation of privacy.[79] Until the Supreme Court is presented with a chance to rescind the third-party doctrine, the Fourth Amendment will not protect internet-based communications.[80]

2. The Privacy Act of 1974 and E-Government Act of 2002

In a subsequent email sent to ARStechnica.com, DHS spokesperson Joanne Talbot attached a declassified presentation titled "DHS Social Media

---

73 *See* 798 F.3d 664, 670–71 (7th Cir. 2015).

74 *Id.* at 670 (citing United States v. Verdugo-Urquidez, 494 U.S. 259, 271 (1990)).

75 457 U.S. 202, 210 (1982).

76 *See* Francesca Bignami & Giorgio Resta, *Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance* (2018), GWU LAW SCHOOL PUBLIC LAW & LEGAL THEORY RESEARCH PAPER SERIES No. 2017-67 (forthcoming Sept. 2017).

77 *See Plyler*, 457 U.S. at 210.

78 *See* 442 U.S. 735, 743–44 (1979).

79 *See id.* at 740.

80 *See id.* at 743–44.

Update."[81] Talbot explained that "[t]he attached presentation will help you understand how [the] DHS uses its already-in place social media policy."[82] The presentation, dated December 5, 2016, was released internally by the DHS privacy office.[83] On the slide titled "*Legal Authorities*," one bullet states that there are "[n]o explicitly worded authorities regarding social media."[84] However, the last bullet on this slide states that "[s]tatutes such as the E-Government Act of 2002 and the Privacy Act of 1974 create privacy protection for individuals whose information is being used and stored by the government."[85]

The Notice also refers directly to the Privacy Act of 1974.[86] This Act was passed after the Watergate scandal, at a time when Congress was concerned about illegal surveillance and computer-stored information.[87] The Privacy Act controls the collection of data stored in a "system of records" by the government.[88] The Act has four main policy objectives:

> 1. To restrict disclosure of personally identifiable records maintained by agencies.
>
> 2. To grant individuals increased rights of access to agency records maintained on them.
>
> 3. To grant individuals the right to seek amendment of agency records maintained on themselves upon a showing that the records are not accurate, relevant, timely, or complete.
>
> 4. To establish a code of 'fair information practices' which require agencies to comply with statutory norms for collection, maintenance, and dissemination of records.[89]

---

81 Fariviar, *supra* note 9.

82 *Id.*

83 *See id.*

84 DEP'T OF HOMELAND SEC., DHS SOCIAL MEDIA UPDATE 1, 4 (2016), https://assets.documentcloud.org/documents/4065386/DPIAC-Social-Media.pdf.

85 *Id.*

86 *See* DHS Notice, *supra* note 1.

87 *Privacy Act of 1974, 5 U.S.C. § 552a*, JUSTICE INFORMATION SHARING, https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1279 (last updated Aug. 16, 2013).

88 *About the Privacy Act*, FED. TRADE COMMISSION, https://www.ftc.gov/about-ftc/foia/about-privacy-act (last visited Apr. 16, 2018).

89 *Privacy Act of 1974*, *supra* note 87.

The Privacy Act also requires that the public be informed via a System of Records Notice ("SORN") published in the Federal Register.[90]

Following the Privacy Act of 1974, Congress passed the E-Government Act of 2002, attempting to cope with the rapidly changing dynamics of the internet.[91] This Act mandates that all federal agencies must create Privacy Impact Assessments ("PIAs") when implementing new "technology that collects, maintains, or disseminates personally identifiable information . . . , or for a new aggregation of information that is collected, maintained, or disseminated using information technology."[92] Assumedly, the Notice complies with this E-Government Act.

3. The Electronic Communications Privacy Act of 1986

In 1986, the United States government passed the Electronic Communications Privacy Act ("ECPA").[93] The passage of this Act was another attempt by Congress to prevent "unauthorized government surveillance of electronic communications."[94] This Act only shielded the popular electronic communication of that era.[95] More specifically, the Act made it illegal for the government to wiretap, interfere with stored electronic communications, and required a warrant for the deployment of a pen register.[96]

Because the ECPA is full of outdated language, it is difficult to extend its protections to modern internet-based communications. Still, the ECPA states that the government must obtain a search warrant (supported by probable cause) to access any stored communications less than 180 days old.[97] However, due to the obsolescence of the ECPA, protections seemingly extend only to stored, unread emails.[98] As Professor Mondu Bedi

---

90 *Id.* Note that the DHS Notice is a SORN, which is why the Notice was posted in the Federal Register.

91 E-Government Act of 2002, Pub L. No. 347, 116 Stat. 2899 (2002); *see also E-Government Act of 2002*, JUSTICE INFORMATION SHARING, https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1287 (last updated Sept. 19, 2013).

92 *Id.*

93 Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–22 (2018); s*ee also* Bedi, *supra* note 44, at 31.

94 Bedi*, supra* note 44, at 31–32.

95 *Id.* at 32.

96 *Id.*

97 *See* 18 U.S.C. § 2703 (2018).

98 Bedi, *supra* note 44, at 33–34.

summarizes, "most . . . [social media] communications will not receive SCA[99] protection."[100]

4. International Privacy Safeguards

Aside from these various, mostly faltering domestic privacy protections, some international protections exist. Unfortunately, these protections are more conceptual than practical. Since its inception, the United Nations has attempted to protect the human right to privacy.[101] In 1948, the UN General Assembly unanimously adopted the Universal Declaration of Human Rights ("UDHR").[102] The right to privacy thus became recognized as a universal and fundamental right.[103] Article 12 of the UDHR states: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to protection of the law against such interference or attacks."[104]

Because the UDHR was a resolution and not a binding instrument, the UN took steps to memorialize the declaration.[105] This lead to the passage of the International Covenant on Civil and Political Rights ("ICCPR").[106] The ICCPR is an "early" United Nations treaty, guaranteeing several civil and political rights.[107] The ICCPR was adopted in 1966.[108] 26 years later in 1992, the United States formally ratified the convention.[109] However, despite the ratification, the United States attached numerous reservations, understandings, and declarations ("RUDs").[110] Article 17, which is most relevant to the discussion here, was not reserved against by the United States.[111]

---

99 The Stored Communications Act, 18 U.S.C. §§ 2701–13 (2018). Note that Stored Communications Act is a provision (Title II) of the Electronic Communications Privacy Act.

100 Bedi, *supra* note 44, at 33.

101 Lauren H. Rakower, Note, *Blurred Line: Zooming in on Google Street View and the Global Right to Privacy*, 37 BROOK. J. INT'L L. 317, 320 (2011).

102 Universal Declaration of Human Rights, G.A. Res. 217 (III) A U.N. Doc. A/RES/217 (III) (Dec. 10, 1948).

103 *See id.*

104 *Id.* at art. 12.

105 Rakower, *supra* note 101, at 321.

106 Bignami & Resta, *supra* note 76, at 3.

107 Kristina Ash, *U.S. Reservations to the International Covenant on Civil and Political Rights: Credibility Maximization and Global Influence*, 3 NW. J. INT'L HUM. RTS. 1, ¶ 3 (2005).

108 *Id.* at n.7.

109 *Id.* at ¶ 3.

110 *Id.*

111 *Id.*

In 2015, Human Rights Council Resolution 28/16 "directly or indirectly confirmed that Article 17 of the ICCPR is implicated by the gathering and processing of personal data."[112] Article 17 of the ICCPR explicitly states that "(1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. (2) Everyone has the right to protection of the law against such interference or attacks."[113] Article 2(1) recognizes the relevant scope of the Covenant, stating:

> Each State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.[114]

It thus follows that communication taking place within a nation's borders, or communication involving a state citizen, would satisfy this scope requirement, triggering Article 17.[115]

ICCPR Article 2 also relates to potential extraterritorial communications, but not according to the United States.[116] The United States takes an extremely narrow view regarding the scope of the ICCPR.[117] It is the United States' position that the Covenant does not reach extraterritorial-based communications.[118] "According to the United States, the ICCPR's safeguards apply only to persons who are both within the state's territory and subject to the state's jurisdiction."[119] This narrow interpretation allows and justifies various United States surveillance programs of foreign individuals.[120]

---

112 Bignami & Resta, *supra* note 76, at 3.

113 International Covenant on Civil and Political Rights art. 2, Dec. 16, 1966, S. Treaty Doc. No. 95-20, 999 U.N.T.S. 171.

114 *Id.* at art. 2, para. 1.

115 Bignami & Resta, *supra* note 76, at 4.

116 *Id.*

117 *Id.*

118 *Id.*

119 *Id.*

120 *Id.*

III. ANALYSIS

A. Mass Collection of Data Does Not Adequately Detect Crime

The DHS cites to several justifications for the new DHS policy.[121] Its most touted justification is that this new policy will support increased national security—likely a result of a recent terroristic trigger.[122] According to Alex Nowrasteh, an immigration expert at the Cato Institute Center for Global Liberty and Prosperity, the recent focus on immigrant social media information may stem from one of the San Bernardino shooter's later-discovered social media pages.[123] Nowrasteh explained that this policy shift "is another example of the government changing security protocols based on a previous incident that will impose an enormous cost and that is of dubious value for the future."[124] Still, research has shown that social media collection does not adequately deter crime.[125]

The idea of incorporating online social media into immigration analysis is not new.[126] The DHS has revealed recent policy from 2012, which permits the collection of immigrant social media information.[127] According to documents obtained by thedailybeast.com, the United States Citizenship and Immigration Services ("USCIS"), a component of the DHS, began projects to analyze the "publicly available social media of small groups of would-be immigrants."[128] Documents further reveal that in 2016, USCIS created an entire Social Media Branch dedicated to monitoring social media data belonging to immigrants from "high risk populations."[129] In 2017, the Trump administration approved a policy requiring social media username and profile information for anyone applying for a United States visa.[130]

---

121 *See* DHS Notice, *supra* note 1, at 43,559.

122 *See id.*

123 Adolfo Flores, *People Are Worried About DHS Plans to Gather Social Media Info*, BUZZFEED (Sept. 25, 2017, 7:28 PM), https://www.buzzfeed.com/adolfoflores/people-are-worried-about-dhs-plans-to-gather-social-media?utm_term=.qrQ93bM1A#.rmwOxJK3R.

124 *Id.*

125 *Id.*

126 Aliya Sternstein, *Obama Team Did Some 'Extreme Vetting' of Muslims Before Trump, New Documents Show*, DAILYBEAST (Jan. 2, 2018, 5:00 AM), https://www.thedailybeast.com/obama-team-did-some-extreme-vetting-of-muslims-before-trump-new-documents-show?ref=home.

127 *Id.*; *see also* Fariviar, *supra* note 9; *Privacy Policy for Operational Use of Social Media*, *supra* note 9.

128 Sternstein, *supra* note 126.

129 *Id.*

130 Melissa Quinn, *State Department Starts Vetting Visa Applicants' Social Media Profiles: Report*, WASH. EXAMINER (June 6, 2017, 8:16 AM), http://www.washingtonexaminer.com/state-department-starts-vetting-visa-applicants-social-media-profiles-report/article/2625047.

The evolution of immigrant social media vetting has reached its zenith. However, the data does not show that data collection has effectively prevented any national security threats or denied admissions to any dangerous peoples.[131] According to a report released by the Office of the Inspector General, the DHS's social media monitoring programs do not contain the requisite criteria for determining effectiveness.[132] The report is appropriately titled, "*DHS' Pilots for Social Media Screening Need Increased Rigor to Ensure Scalability and Long-term Success*," and recommends that the DHS implement a plan to include measurable quality standards in their collection programs.[133] The DHS concurred with the findings, and set forth a four-prong approach to meet the report's recommendations.[134] Thereafter, the DHS dismissed the issue, claiming that the problem was rectified.[135]

Additionally, social media collection programs have not been shown to prevent any dangerous immigrants from entering the United States.[136] Immigration analyst Alex Nowrasteh argues that "[s]ocial media has been used by immigration courts for years but there is very little evidence that it's helped with visa vetting."[137] Shockingly, his claims are substantiated by internal White House documents.[138] These briefing documents, provided to then president-elect Donald Trump and his transition team, stated that the collection and analysis of refugee social media did not yield any successful results.[139] Excerpts of the White House documents explain that the first three "Refugee Pilots" were able to link applicants to their respective social media accounts.[140] However, the information gleamed from these accounts "did not produce clear links to national security concerns even for applicants who were found to pose a potential national security threat."[141] According to the

---

131 *See* Flores, *supra* note 123.

132 OFF. OF INSPECTOR GEN., DHS' PILOTS FOR SOCIAL MEDIA SCREENING NEED INCREASED RIGOR TO ENSURE SCALABILITY AND LONG-TERM SUCCESS (REDACTED) 1 (2017), https://www.oig.dhs.gov/sites/default/files/assets/2017/OIG-17-40-Feb17.pdf.

133 *Id.*

134 *Id.*

135 *Id.*

136 Flores, *supra* note 123; *see also* Zach Whittaker, *NSA is so overwhelmed with data, it's no longer effective, says whistleblowe*r, ZDNET (Apr. 27, 2016, 7:00 PM), http://www.zdnet.com/article/nsa-whistleblower-overwhelmed-with-data-ineffective/ (explaining that NSA mass surveillance programs are overwhelmed and ineffective. According to former NSA official William Binney, "[t]he US government's mass surveillance programs have become so engorged with data that they are no longer effective, losing vital intelligence in the fray.").

137 Flores, *supra* note 123.

138 *Id.*

139 *Id.*

140 *Id.*

141 *Id.*

information in the documents obtained by thedailybeast.com, "[a]s of November 2016, USCIS had not denied anyone entry or legal status 'solely or primarily because of information uncovered through social media vetting.'"[142]

The language in the Notice, as applied to these findings, should highlight the inadequacies of this new DHS policy. First, the federal government has conducted programs implementing similar policy, yielding no positive result.[143] Because social media has become such an integral part of modern communication, storing "social media handles, aliases, associated identifiable information, and search results,"[144] will not effectively pinpoint valuable information. Recent history has shown this. There is simply too much information. The language in the Notice is not precise enough to meet its objective.

The Notice attempts to justify mass data collection by explaining that "USCIS . . . supports national security by preventing individuals from fraudulently obtaining immigration benefits and by denying applications from individuals who pose national security or public safety threats."[145] The United States has historically used national security as a reason to impede upon and minimize several human rights—especially the right to privacy.[146] The protection of human rights is extremely important. Professor William Burke-White argues that there seems to be an "observed correlation between systematic human rights violations and interstate aggression."[147] Thus, using security-centric language to justify the degradation of American rights may actually be a telling factor indicating a propensity for extraterritorial violence.[148]

It follows that the policy in question, the collection and storage of immigrant social media information in the DHS A-Files system, will not adequately prevent dangerous individuals from entering the United States because the past use of similar programs has been largely unsuccessful. The language in the Notice is also too lax and provides the DHS with unconstrained oversight powers. The DHS should stop the collection of immigrant "social media handles, aliases, associated identifiable information, and search results."[149] At the very least, the Notice language and

---

142 Sternstein, *supra* note 126.

143 Flores, *supra* note 123.

144 DHS Notice, *supra* note 1, at 43,557.

145 *Id.*

146 William W. Burke-White, *Human Rights and National Security: The Strategic Correlation*, 17 HARV. HUM. RTS. J. 249, 249 (2004).

147 *Id.* at 265.

148 *See id.*

149 DHS Notice, *supra* note 1, at 43,557.

corresponding DHS policy would need to be made more specific, in order to successfully deter dangerous individuals from entering the United States.

B. Controversial Constitutionality

In theory, the third-party doctrine allows the DHS to collect social media information without a warrant and without any Fourth Amendment considerations.[150] However, this doctrine is controversial and antiquated.[151] The DHS explained in the Notice that it is collecting and storing immigrant "social media handles, aliases, associated identifiable information, and search results."[152] The citizenship status of the immigrants (or nonimmigrants) would not matter.[153] The third-party doctrine totally removes internet-based data collection from Fourth Amendment scrutiny.[154]

The third-party doctrine stemmed from the 1979 Supreme Court "pen register" case, *Smith v. Maryland*.[155] The Court held that an individual could not have a reasonable expectation of privacy when information was transmitted via a third-party.[156] This case, which was decided almost 40 years ago, has changed Fourth Amendment jurisprudence in the United States. Now, no Fourth Amendment protections are afforded to any internet-based or electronic communication.[157] Even though many internet users do believe that their communications are confidential or that their search results are hidden, the Court has ruled that this expectation is not "reasonable."[158] Unsurprisingly, the third-party doctrine is highly controversial and often contemplated by legal scholars.[159]

There has been some modern pushback to this third-party doctrine. Recently, the Department of Justice ("DOJ") requested that Apple assist the Federal Bureau of Investigations ("FBI") in accessing the password/encryption protected iPhone of one of the San Bernardino

---

150 *See* 442 U.S. 735, 743–44 (1979).

151 Matthew D. Lawless, *The Third Party Doctrine Redux: Internet Search Records and the Case for a "Crazy Quilt" of Fourth Amendment Protection*, 11 UCLA J.L. & TECH. 2, 8 (2007).

152 *See* DHS Notice, *supra* note 1, at 43,557.

153 *See* Bedi, *supra* note 44, at 3–4, 8, 47.

154 *See id.*

155 442 U.S. 735, 742 (1979).

156 *Id.* at 743–44.

157 Lawless, *supra* note 151, at 8.

158 *Smith*, 442 U.S. at 743–44.

159 *See* Bedi, *supra* note 44, at 1; Lawless, *supra* note 151, at 2–5; Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 562–64 (2009).

shooters.[160] Apple refused to comply.[161] Ultimately, the FBI employed the help of an anonymous hacker to gain access to the contents of the encrypted iPhone.[162] Even though the Fourth Amendment was not directly implicated, this situation brought the importance of data privacy to the limelight. As Apple CEO Tim Cook explained, circumventing iPhone encryption at the government's request would create a dangerous precedent—even more dangerous than the third-party doctrine.[163]

Many scholars recognize the inherent problems associated with the third-party doctrine. Professor Stephen E. Henderson writes that this controversial doctrine is "fundamentally misguided."[164] Professor Henderson illustrates this by exploring a modern, online book shopping experience.[165] He describes, "today if I want to purchase a book I am likely to do so online, where not only the bookstore, but also my Internet service provider and payment provider will make personal records."[166] He continues, "these records are stored in a digital format that permits, once an architecture has been established, essentially costless searching and distribution . . . [n]othing in the Fourth Amendment prohibits such a bookstore, or any other third party, from conveying information to law enforcement on its own initiative."[167] This example illustrates the consequences and dangers of the third-party doctrine, as applied to a simple, noncriminal online shopping experience.

There are clear lines drawn when it comes to data privacy and Constitutionality. As applied to the DHS Notice, any individual who wishes to visit (or immigrate to) the United States could have search histories, Twitter rants, YouTube binges, and Facebook profile information stored in their Alien File.[168] This encourages anonymous online activity and password protected, encrypted hard drives. The Fourth Amendment has been stretched in favor of the United States government, under the guise of national security. But opposite result is likely—internet savvy individuals subject to the INA

---

160 Clark D. Cunningham, *Apple and the American Revolution: Remembering Why We Have the Fourth Amendment*, 126 YALE L.J. 216, 216 (2016).

161 *Id.* at 216–17.

162 *See* Kristen M. Jacobsen, Note, *Game of Phones, Data Isn't Coming: Modern Mobile Operating System Encryption and Its Chilling Effect on Law Enforcement*, 85 GEO. WASH. L. REV. 566, 569 (2017).

163 *See* Tim Cook, *A Message to Our Customers*, APPLE (Feb. 16, 2016), http://www.apple.com/customer-letter/.

164 Stephen E. Henderson, *The Timely Demise of the Fourth Amendment Third Party Doctrine*, 96 IOWA L. REV. BULL. 39, 40 (2011).

165 *Id.* at 45.

166 *Id.*

167 *Id.*

168 *See* DHS Notice, *supra* note 1, at 43,557.

may attempt to avoid ending up in databases that could decrease their chances of admission to the United States.

Ultimately, the third-party doctrine is an outdated jurisprudential mishap. The only way to rectify this mishap is to bring a case to the Supreme Court to potentially rescind the doctrine. Only then would citizens, and certain noncitizens alike, have their Fourth Amendment privacy protections restored. At this moment, the constant collection and storage of internet-based information by the DHS is technically constitutional. Despite this controversial constitutionality, negative social repercussions are likely to follow if the DHS continues to collect immigrant social media information.

C. Violation of International Law

There are also certain international privacy protections that may shield some information from government surveillance. Article 17 of the International Covenant on Civil and Political Rights ("ICCPR") states that, "No one shall be subjected to arbitrary or unlawful interference with his *privacy*."[169] The United States has signed and ratified the ICCPR, and has not entered any RUDs against Article 17.[170] The DHS's social media collection policy violates this provision of the ICCPR.[171] Despite this violation, international law does not provide a practical pathway to halt the enforcement of the new DHS policy.[172]

Unfortunately, when an aggrieved individual seeks redress under the ICCPR they face limited options.[173] Despite not having a judicial enforcement mechanism, the ICCPR "has instead an oversight and complaints-handling body in the form of the Human Rights Committee" ("UNHRC").[174] The United States has stifled this procedure by not signing the First Optional Protocol to the ICCPR, the document creating the Human Rights Committee.[175] Despite the influence of the UNHRC, their decisions are not binding under international law.[176] Still, the UNHRC has previously challenged the legality of mass surveillance programs, such as the (Edward

169 International Covenant on Civil and Political Rights, *supra* note 113 (emphasis added).

170 *See* Ash, *supra* note 107, at ¶ 3.

171 *See* Lee A. Bygrave, *Data Protection Pursuant to the Right to Privacy in Human Rights Treaties*, 6 INT'L J.L. & INFO. TECH. 247, 249–54 (1998).

172 *Id.* at 249.

173 *Id.*

174 *Id.*

175 *Id.*

176 Bygrave, *supra* note 171.

Snowden-uncovered) NSA surveillance program, as being incompatible with Article 17 of the ICCPR.[177]

In 1988, the Human Rights Committee released a general comment on Article 17 of the ICCPR, titled "*CCPR General Comment No. 16: Article 17 (Right to Privacy) The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*."[178] This comment explains the responsibilities of states to implement the privacy protections required by Article 17 of the ICCPR.[179] For instance, in the very first paragraph the comment states that "[t]he [privacy] obligations imposed by this article require the State to adopt legislative and other measures to give effect to the prohibition against such [governmental] interferences and attacks as well as to the protection of this [privacy] right."[180] The privacy protection laws in the United States are inadequate, as evidenced by the federal DHS policy.

Unsurprisingly, the United States views the scope of ICCPR very narrowly. The United States interprets ICCPR protections to extend only to individuals already within the territorial jurisdiction of the United States.[181] This viewpoint justifies surveillance and data collection on foreign immigrants.[182] As legal scholar Francesca Bignami argues, this narrow interpretation is not correct, in light of the language within the ICCPR.[183] Covenant protections cover a person when they are within the "effective control" of a state actor, not just within the territory of the state.[184] Because the Notice states that individuals subject to the INA are to have their data collected and stored, ICCPR protections should be triggered. The ICCPR codifies the universal right to privacy, not just a territorial one.[185]

Since there are no binding international judicial remedies, not much can be done. The only semi-realistic option that foreign states could select is the application of political pressure against the United States. The international community would have to explicitly condemn the actions of the United States and the DHS policy. First and foremost, the UN General Assembly and Human Rights Committee ought to condemn the DHS policy as incompatible

177 Bignami & Resta, *supra* note 76, at 7.

178 U.N. Human Rights Committee, *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, U.N. Doc. HRI/GEN Rev.1 (April 8, 1988).

179 *See id.*

180 *Id.* at para. 1.

181 Bignami & Resta, *supra* note 76, at 4.

182 *Id.* at 7.

183 *Id.* at 5.

184 *Id.*

185 *Id.*

with the provisions in the ICCPR.[186] However, due to the complex international political atmosphere, it is unlikely that any political pressure will be applied at this time.

The European model of understanding the international right to privacy should provide the United States with better guidance to avoid implementing policies that may infringe upon this right. The European Convention of Human Rights ("ECHR") and the European Court of Human Rights ("ECtHR") provide EU states with greater privacy safeguards and remedies, compared to the United States.[187] Specifically, Article 8 of the ECHR titled the "*Right to respect for private and family life*," states that: "(1) Everyone has the right to respect for his private and family life, his home and his correspondence."[188] The second provision of Article 8 explains that:

> (2) There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[189]

Despite this caveat, the ECtHR has ruled that mass surveillance programs must be particularized.[190] The ECtHR has ruled that mass surveillance operations are not compatible with the right to privacy, as encapsulated in the ECHR.[191] The United States should respect the international right to privacy, as a party to the ICCPR, and implement safeguards akin to the understandings in the ECHR.

The DHS social media collection policy (specified in the Notice) violates Article 17 of ICCPR. The United States has failed to properly implement domestic legislation protecting the universally recognized right to privacy. The United States is at odds with the international consensus on this matter, and should promptly end the newly implemented DHS social media

---

186 *Id.* at 6 (citing U.N. Human Rights Committee, *Concluding Observations on the Fourth Periodic Report of the United States of America* 10, U.N. Doc. CCPR/C/USA/CO/4 (Apr. 23, 2014)).

187 *Id.* at 2.

188 Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 11, 1950, 213 U.N.T.S. 221.

189 *Id.*

190 Bignami & Resta, *supra* note 76, at 18 (explaining that in the case "*Szabó and Vissy v. Hungary,* [the ECtHR's] first NSA-style surveillance case, the Court manifested serious concerns over the technological advances that have enabled state authorities to collect enormous masses of personal data and build detailed individual profiles." *Id.* The Court highlighted that for this sort of data collection to be appropriate, the data collection must be "strictly necessary in a democratic society." *Id.* This data collection must also be particularized. *Id.*).

191 *See id.*

collection policy. If the United States refuses to do so, there are no viable international judicial remedies to reconcile this violation—aside from certain political condemnations.

D. Modern Issues with Social Media and Identity

As above-mentioned, global social media use is at an all-time high. Theoretically, in America and abroad, nearly everyone has utilized social media in one form or another. In 2017, Facebook founder Mark Zuckerberg exclaimed that his social media platform now hosts over two billion people.[192] Within this vastness of social media, usership and content problems are issues that are not considered by the new DHS policy and Notice. These problems put immigrants at risk of being unfairly denied entrance to the United States—at no fault of their own.

The first striking issue, that could seriously alter admissions and denials to the United States, is social media-based identity theft. According to reports, in the year 2016, social media identity fraud was up an astonishing 57%.[193] According to the fraud prevention service Cifas, "Facebook, Twitter, and LinkedIn . . . [have] become a 'hunting ground' for identity thieves."[194] When identity thieves have obtained stolen (or even public) information from an individual, they have the tools to create fake social media profiles.[195] The content on these fake profiles could then get swept up and stored in an immigrant's DHS A-File system.

Similarly, a social media profile may also be accessed by an unauthorized third party or "hacker." Any information posted under the guise of the original account owner could be stored and archived in an A-File. According to The University of Phoenix researchers, "[n]early two in three U.S. adults who have social media profiles say they . . . [were] aware that their accounts . . . [had] been hacked."[196] There have been numerous recent

---

192 Mark Zuckerberg, FACEBOOK (June 27, 2017, 1:04 PM), https://www.facebook.com/zuck/posts/10103831654565331.

193 *Identity Fraud Up by 57% as Thieves 'Hunt' on Social Media*, BBC NEWS (Jul. 5, 2016), http://www.bbc.com/news/uk-36701297.

194 *Id.*

195 *See* Scott Bernstein, *The Growing Epidemic of Fake LinkedIn Profiles*, LINKEDIN (Oct. 8, 2015), https://www.linkedin.com/pulse/growing-epidemic-fake-linkedin-profiles-scott-bernstein; *see also Social Media Protection Brand Fraud Report*, PROOFPOINT, https://www.proofpoint.com/sites/default/files/pfpt-en-social-media-protection-brand-fraud-report.pdf (last visited Apr. 16, 2018) (examining the prevalence of fake, branded social media).

196 UOPX News, *Nearly Two-Thirds of U.S. Adults with Social Media Accounts Say They Have Been Hacked*, U. PHOENIX (Apr. 27, 2016), https://www.phoenix.edu/news/releases/2016/04/uopx-social-media-hacking.html.

high-profile hacking incidents.[197] Some hackers can even gain access to entire populations of users, compiling user credentials and auctioning them off to the highest bidder.[198] This exact situation has affected every major social media site, including Facebook, Twitter, Myspace, and LinkedIn.[199] Social media security issues have arisen time and time again. The DHS Notice does not specify any procedure for determining the validity of the collected and stored social media information.[200]

Hackers continue to have a keen interest in accessing social media accounts. Modern hackers often utilize a hacking method known as "spear phishing."[201] Spear phishing occurs when a bot social media account, posing as a real person, sends a malicious link to an unsuspecting social media user.[202] Hackers can blend their bots in with other legitimate accounts, and even assume the identity of a target account's friends or acquaintances.[203]

These attacks have become so prominent and effective that the United States government has taken note of the severity of the situation.[204] According to a *Time* magazine report, "a Russian-led cyberattack tried to spear phish 10,000 Twitter accounts belonging to Defense Department employees, using personal messages targeted at specific users."[205] Once an account is compromised and hackers have acquired personal information and passwords, the hacker can assume the stolen identity, or sell the information to the highest bidder. The DHS Notice does not provide any protections for situations where a social media account is compromised. The DHS Notice presumes that all social media activity is legitimate, and would purportedly sweep up and permanently store all information connected to a target individual.

There may also be issues with specific social media platforms, as applied to the DHS Notice. Again, the Notice specifies that "social media handles, aliases, associated identifiable information, and search results" are to be collected and stored. [206] Despite this seemingly broad language, each

---

197 *See* Selena Larson, *The Hacks That Left Us Exposed in 2017*, CNN BUS. (Dec. 20, 2017, 9:11 AM), https://money.cnn.com/2017/12/18/technology/biggest-cyberattacks-of-the-year/index.html.

198 *Hackers are Targeting You on Social Media*, ZEROFOX (June 16, 2016), https://www.zerofox.com/blog/mark-zuckerberg-hack/.

199 *See id.*

200 *See* DHS Notice, *supra* note 1, at 43,556.

201 Sheera Frenkel, *Hackers Hide Cyberattacks in Social Media Posts*, N.Y. TIMES (May 28, 2017), https://www.nytimes.com/2017/05/28/technology/hackers-hide-cyberattacks-in-social-media-posts.html.

202 *Id.*

203 *Id.*

204 *Id.*

205 *Id.*

206 *See* DHS Notice, *supra* note 1, at 43,557.

social media platform has unique characteristics. For instance, Twitter features a unique ability for a user to "retweet" content that was originally posted by a different user.[207] Many Twitter users have even gone as far as adding a disclaimer to their profile, exclaiming that "RTs [retweets] do not equal endorsements."[208] Will retweeted information be added to an A-File? Will a tweet that is "liked" or "favorited" by the user negatively impact someone looking to travel to the United States? Unsurprisingly, the DHS Notice does not answer any of these questions.

The DHS Notice does not consider many unique issues associated with social media. Thus, this new DHS policy could unfairly affect people who are not as technologically savvy as others. The policy, as understood by the language in the Notice, is simply not particularized enough. Therefore, the DHS should halt this policy, and consider the problems associated with modern social media usage.

E. Relevant User-Submitted Comments

As is customary with all notices posted in the Federal Register, interested individuals have the ability to submit comments on the proposed new policy. The Notice comment period began on September 18, 2017 and ended on October 18, 2017.[209] During this time, almost 3,000 comments were submitted. Most of these submitted comments present compelling arguments against the implementation of the DHS data collection policy. Several of these comments will be highlighted herein.

Andrew Sellars, the director of the Boston University/Massachusetts Institute Technology ("MIT") and Cyberlaw Clinic, submitted a comment on behalf of students and faculty at MIT.[210] Sellars summarizes the comment by stating that:

> The Commenters are all students and scholars of Internet communications and related technologies, and write specifically to inform DHS of the critical shortsightedness of this planned expansion, to explain why a sound academic would never propose such a system of information collection, and to emphasize why such collection inherently

---

207 *See* Anne Johnson, *The Ethics of Retweeting and Whether it Amounts to Endorsement*, NPR (July 31, 2014, 5:30 PM), https://www.npr.org/sections/ombudsman/2014/07/31/336921115/the-ethics-of-retweeting-and-whether-it-amounts-to-endorsement.

208 *See id.*

209 *See* DHS Notice, *supra* note 1.

210 *Comment Submitted by Andrew Sellers*, REGULATIONS.GOV (Oct. 18, 2017), https://www.regulations.gov/document?D=DHS-2017-0038-2960 [hereinafter *Comment by Andrew Sellers*].

> violates the Fair Information Practice Principles that this agency has adopted.[211]

First, Sellars argues that the Notice is not clear enough, making it impossible to determine what kind of information would be collected and stored.[212] Sellars also points out that the only person who is unable to access the A-Files database is the subject themselves.[213] Sellars contends that this is incompatible with the Privacy Act of 1974.[214]

Sellars's second main argument is that a broad collection scheme is too unprincipled to actually catch any dangerous content.[215] Sellars explains that the "[t]he ease of development of social media means that there is a plethora of fake and misleading accounts online, which can easily portray an individual as something they are not."[216] Sellars explains that he is worried that "[s]uch a system will . . . experience a sea of false negatives and false positives."[217] Many of Sellars's positions support the arguments proffered herein.

Another compelling comment was submitted by Catherine Martinez and 111 other members of the Yale Law School community.[218] This comment is critical of the proposed DHS rule, "urg[ing] DHS to rescind the rule."[219] The comment first argues that the proposed DHS rule violates the First Amendment to the United States Constitution.[220] The commenters argue that because the policy indirectly limits access and use of internet speech, the First Amendment is violated.[221] "[T]he Proposed Rule threatens to chill individuals' ability to exercise their rights to freedom of speech and association on social media."[222]

Later in their impressive comment, the Yale commenters argue that the proposed DHS policy violates the Fifth and Fourteenth Amendments.[223] They argue that because the proposed policy is to collect the social media information of naturalized citizens, it is impermissibly classifying citizens

---

211 *Id.* at 1.

212 *Id.* at 1–2.

213 *Id.* at 2.

214 *Id.*

215 *Comment by Andrew Sellers*, *supra* note 210, at 3–4.

216 *Id.* at 4.

217 *Id.*

218 *See Comment by Catherine Martinez*, *supra* note 8.

219 *Id.* at 1.

220 *Id.* at 3.

221 *Id.*

222 *Id.* at 5.

223 *Id.* at 10.

"on the basis of national origin."[224] "By allowing the DHS to collect this information about naturalized citizens while excluding natural-born citizens, this policy conditions its application to citizens on the basis of national origin, and therefore is inherently suspect."[225] They then argue that this discrimination is not supported by the necessary compelling governmental interest, and that the policy is not narrowly tailored to achieve that interest.[226] Thus, according to these Yale commenters, the policy violates the Equal Protection guarantees of the Fifth and Fourteenth Amendments to the United States Constitution.[227]

The above comments are just a few of the unique and convincing arguments presented by concerned individuals. The clear majority of the comments submitted express extreme distrust and condemnation towards the DHS policy outline in the Notice. Many of these complex, creative, and compelling comments have attacked the policy in every way imaginable. The DHS policy is clearly problematic, prompting an enormous public outcry. The resistance against the DHS policy is clear, and the DHS should halt the now-implemented policy until these concerns are addressed.

IV. CONCLUSION

The DHS Notice is an example of the powerful internet data oversight powers the United States government has reserved for itself. The internet has evolved to such a point that outdated legislation does not adequately protect the American people from constant surveillance. Supreme Court jurisprudence is also being used to assist the government in its spying operations.[228] The United States government is in no hurry to provide its people with more adequate protections—especially at a time when hypervigilant safety-based paternalism is at its peak. Instead, the government is targeting vulnerable immigrant populations, ramping up its data-collection operations while carefully broadcasting the policy to the world. Under existing domestic law, this collection is perfectly legal.

We are now at a crossroad. The current legal situation—surrounding the governmental collection of internet-based information—is remarkably lax. Even though the DHS policy is proposed to track immigrant internet data, citizen data does not feature any increased protections. Most people have never heard of the third-party doctrine, and are simply unaware that their

224 *Id.*

225 *Id.*

226 *Id.* at 10–11.

227 *Id.* at 11.

228 *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

online activity is ripe for governmental surveillance. To rectify this legal inadequacy, increased data protections must be created and implemented by the American legislature or judiciary. Nevertheless, for reasons mentioned herein, the United States government should discontinue the collection and storage of immigrant social media information.