Combating Fake News with Digital Identity Verification

Wajeeha Ahmad, Ryan Berg, Sharon Kim

1 Executive Summary

The Internet has become a fundamental source of information exchange in the 21st century. In particular, online social media platforms are becoming increasingly important tools for communication and political discourse in the United States and abroad. This medium presents a novel, unprecedented way for people to become more informed and civically involved, but simultaneously opens democratic societies up to potential interference by foreign, malevolent actors who manipulate the information that social media users consume and use to make decisions. As an example of social media influencing the opinions and actions of U.S. residents, foreign Russian actors were able to organize a protest and a simultaneous counter-protest in Houston, Texas during the 2016 U.S. presidential election campaign using Facebook groups operated by a Kremlin-linked troll farm from Saint Petersburg.[1] Other instances of foreign influences include individuals abroad selling American political advertisements for monetary gain, social bots being used to give the false impression of grassroots public support, and in general, the rapid spread of false, sensational media. Given the ubiquitous role that online platforms play in shaping socio-political discourse and outcomes, we propose a government-supported approach for combating the spread of fake news online by verifying the identities of U.S. residents on social media platforms.

Social media behemoths such as Facebook, Twitter, and Google have made commendable efforts to tackle fake news on their platforms, but have failed to address the full scope of the issue. By way of time-consuming user-reporting and fact-checking procedures, they manage to reduce only the monetary incentives of propagating fake news. Moreover, technical means of identifying fake news have only been partially effective at distinguishing bot-administered accounts from human-administered ones. Company-sponsored post takedowns and account bans also have the potential to undermine online freedom of expression. Additionally, social media companies also do not have sufficient market incentives to reliably verify the identities of their users. Therefore, the methods currently under consideration by private industry are insufficient to counter fake news proliferation by foreign actors, especially those with political incentives to misinform and deceive U.S. residents as a means of election tampering.

We believe that the responsibility of authenticating an individual's identity and U.S. residential status is a primary duty of the government. However, the U.S.'s existing *de facto* "identification" scheme, the Social Security Number (SSN) system, is ignorant of the growing socio-political aspect of digital identity and is therefore inadequate for use on online social media platforms. We therefore recommend the creation of a new, government-issued, cryptographically-secure digital identity system for use by private companies to validate the identities of U.S. residents using their

[1] CNN, Tim Lister and Clare Sebastian. "Stoking Islamophobia and Secession in Texas -- from an Office in Russia." CNN. Accessed November 28, 2017. http://www.cnn.com/2017/10/05/politics/heart-of-texas-russia-event/index.html.

services. This would allow social media users to distinguish between social media posts made by U.S. residents who have a real stake in discussing socio-political affairs pertaining to their country and fake news posts made by foreign actors intending to bias the opinions of U.S. residents. In this paper, we do not attempt to address the question of adoption, either by users or by private companies. Instead, we address the policy questions of whether a digital identity verification system provided by the government can provide a secure and effective means of verifying the U.S. residential status of social media users.

We see four key problems that need to be addressed when creating such a system. First, such a system should be compatible with freedom of expression; in particular, it should not mitigate anonymous speech, which is critical for marginalized groups and maintaining the diversity of opinions online. Our system addresses this by being an opt-in tool for private companies to utilize, and not a mandatory solution to the digital attribution problem. Platforms that choose to opt out of the proposed digital identity verification system, then, are a result of user desire for those systems, which is how the Internet currently operates. Second, the system should be secure and encrypted. For this purpose, we discuss how the Estonian government has set precedents for a digital identity system designed to both minimize data breaches and ensure privacy to the greatest extent possible. Third, an identity system implemented nationwide should be efficient and scalable, not unlike India's Aadhaar program, in which over one billion Indians are enrolled. Fourth, the identity system should protect the privacy of U.S. residents and minimize the potential for government abuse. To this end, we recommend that implementation of this system should not extend to authenticating users for other accounts. Given the backlash against the creation of a U.S. national ID system by prominent experts in technology and privacy after the REAL ID Act of 2005 was proposed by Congress, we advocate for a narrowly-tailored government-backed digital identity verification system as opposed to a universal national identity system that cuts across various government functions. Users should not be required to trust that the keys they are issued accomplish purposes beyond verifying their identity for social media platforms.

In Section 2, we scope the problem of how a lack of digital identity authentication online has led us to the current issues of fake news proliferation, and examine why current measures by private industry illustrate the need for a government-backed solution. Section 3 delves into the identity context of our topic by highlighting past government identification schemes in the U.S. and abroad, particularly with reference to incorporating digital identification systems as implemented by India and Estonia. In Section 4, we analyze various policy concerns facing a digital identity verification system. This includes advocating for maintaining the values of free expression and anonymous speech on online social media platforms in the context of the legal history of anonymous political speech in the United States and the relatively recent "real name" policy controversy faced by social media companies. Additionally, we analyze the implications of such a system on user privacy and trust in government-backed solutions. Section 5 details our proposed government-issued digital identity verification scheme, which can be applied on social media platforms by private industry to enable users to securely identify whether or not news posts originate from foreign actors or U.S.-based sources. Section 6 concludes.

Table of Contents

2 Background on current issues of fake social media accounts

2.1 Effects of fake news on political discourse and outcomes in the United States

The rising popularity of online social media platforms as primary channels of communication and information exchange has had various implications for socio-political discourse in the United States. According to the Pew Research Centre, nearly two-thirds of U.S. adults get at least some of their news from social media curated by their friends and contacts.[2] Additionally, tens of millions of Americans use Facebook as their main source of information today. However, the very same platforms used for the open exchange of information and democratic discourse have made societies more vulnerable to external influence in national affairs as malevolent foreign actors exploit the power of social media platforms to manipulate the flow of information and generate false accounts regarding domestic affairs concerning U.S. residents.

For the purposes of our paper, we define *fake news* as false or misleading information that is presented with the intent to deceive or misinform information consumers as well as garner attention. We refer to the *user* of a social media platform as someone who consumes information via their online news feeds on popular social networking websites such as Facebook, Twitter, or Google Plus, among others. In this paper, we attempt to address technical and policy proposals for combating the spread of fake news propagated by foreign actors to bias American socio-political discourse. We focus on fake news spread via the social media accounts of foreign actors as well as bots operated by foreign actors posing as individuals residing in the United States.

While fake news has existed since the dawn of the printing press, it has more recently acquired unprecedented sophistication in reaching large audiences and misleading news consumers by gaming the algorithms of social media and search engines. For instance, when more people than usual click on a given news story on a platform like Facebook, the company's software algorithms instantaneously spread and promote that story to many other users in the network, enabling articles to quickly "go viral" and making it harder to catch false news before it becomes ubiquitous. Although little is publicly known about the algorithms employed by Facebook, Google, Twitter, and other information gatekeepers, they tend to promote viral or provocative articles that generate clicks, regardless of the veracity of their content. Moreover, according to a report by Freedom House, while the number of governments attempting to control online discussions has risen each year since 2009, the practice has presently become significantly more widespread and technically sophisticated, with bots, propaganda producers, and fake news outlets exploiting social media and search algorithms to ensure high visibility and seamless integration with trusted content.[3]

---

[2] Gottfried, Jeffrey, and Elisa Shearer. "News Use Across Social Media Platforms 2016." *Pew Research Center's Journalism Project* (blog), May 26, 2016. http://www.journalism.org/2016/05/26/news-use-across-social-media-platforms-2016/.

[3] "Freedom on the Net 2017: Manipulating Social Media to Undermine Democracy," October 27, 2017. https://freedomhouse.org/report/freedom-net/freedom-net-2017.

According to the U.S. *National Strategy for Trusted Identities in Cyberspace (April 2011),* among the shortcomings in cyberspace is the online authentication of people and devices. The President's Cyberspace Policy Review during the Obama administration established trusted identities as a cornerstone of improved cybersecurity.[4] In this paper, we focus on what the U.S. government can do to minimize the impact of fake news from foreign actors and bots in the cyberspace without undermining the democratic values of free speech, transparency and open expression. This involves addressing the central issue of making it easier for social media users to differentiate between authentic U.S. residents and fake accounts posing as U.S. residents in order to allow social media users to uphold fake news spread by malevolent foreign actors to greater scrutiny.

2.1.1 Consequences of fake profiles run by foreign actors in manipulating American political discourse

The 2016 U.S. presidential election presents a good case study of foreign actors seeking to influence American political discourse through spreading fake news. Lawyers from Facebook, Google and Twitter have testified before the U.S. Senate Judiciary Committee amid mounting political pressure to fully investigate Russian efforts to influence the 2016 U.S. presidential campaign.[5] This revealed that Russian agents intending to sow discord among American citizens disseminated inflammatory posts that reached 126 million users on Facebook, published more than 131,000 messages on Twitter and uploaded over 1,000 videos to Google's YouTube service, according to copies of prepared remarks from the companies.[6] As an example, Facebook disclosed that the Internet Research Agency, a shadowy Russian company linked to the Kremlin, had posted roughly 80,000 pieces of divisive content that was shown to about 29 million people between January 2015 and August 2017. Those posts were then liked, shared and followed by others, spreading the messages to tens of millions more people. These Russia-linked posts were referred to as "deeply disturbing" and "an insidious attempt to drive people apart" by Facebook's own general counsel, who also noted the posts focused on race, religion, gun rights, and gay and transgender issues - issued of considerable importance to U.S. socio-political discourse.[7] Twitter also discovered more than 2,700 accounts on its service that were linked to the Internet Research Agency between September and November of 2016. Those accounts posted roughly 131,000 tweets over that period. Outside of the activity of the Internet Research Agency, Twitter identified more than 36,000 automated accounts that posted 1.4 million election-related tweets linked to Russia over a three-month period. The tweets received approximately 288 million views.

According to a declassified version of a U.S. Intelligence Community Assessment released on January 6, 2017, Russian efforts to influence the 2016 U.S. presidential election "demonstrated a

[4] "National Security Strategy " The White House May 2010, p27, 17 Dec 2010, http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf
[5] Veronica Rocha and Brian Ries, "Facebook, Twitter and Google testify at Russia hearing: Live updates", CNN Politics, October 31, 2017.
[6] Isaac, Mike, and Daisuke Wakabayashi. "Russian Influence Reached 126 Million Through Facebook Alone." *The New York Times*, October 30, 2017, sec. Technology. https://www.nytimes.com/2017/10/30/technology/facebook-google-russia.html.
[7] Id.

significant escalation in directness, level of activity, and scope of effort compared to previous operations" to undermine the U.S.-led liberal democratic order.[8] These efforts included a combination of covert cyber operations and overt efforts by Russian Government agencies, state-funded media, third-party intermediaries, and paid social media users or "trolls."[9] These social media trolls were used to denigrate Secretary Clinton by amplifying stories on her scandals and the role of WikiLeaks in the election campaign.[10] The activities of professional trolls at the Internet Research Agency in Saint Petersburg were likely financed by a close Putin ally with ties to Russian intelligence.[11] The intelligence report also revealed with high confidence that efforts ordered by Russian President Vladimir Putin to influence the 2016 U.S. presidential election were directly aimed at undermining public faith in the U.S. democratic process, denigrating Secretary Clinton, and harming her electability and potential presidency. Moreover, the intelligence community believes that the use covert social media operations to undermine the integrity of U.S. elections and democratic processes will continue since such means can accomplish Russian goals relatively easily without significant damage to Russian interests.[12]

Other foreign actors were also involved. For instance, there exists evidence that a number of fake profiles on Facebook that posted political ads to influence public opinion during the 2016 U.S. Presidential elections were created by teenagers interested in the idea of using ad revenue as a convenient means of making money in Macedonia, where prospects of securing a real job with a good salary are abysmally low.[13] Even though these Macedonians had no political stake in the U.S. elections, social media platforms made it exceptionally simple for them to finance their posts, which helped deliver momentous consequences.

2.1.2 Consequences of using foreign-administered bots to spread fake news online

Political bots are automated software programs that operate on social media, written to mimic real people in order to manipulate public opinion. The idea behind political botnets is one of numbers: if one account makes a splash with a message, then 1000 bot-driven accounts make a flood, amplifying political messages. Armies of bots pretending to be human, sometimes referred to as "sock-puppet accounts," computationally and automatically extend the ability of the deploying party to spread messages on sites like Twitter. Bots can be used to feign grassroots support for a policy, individual, or party when little such support exists — a phenomenon known as "astroturfing".

[8] Intelligence Community Assessment, "Assessing Russian Activities and Intentions in Recent U.S. Elections", ICA 2017-01D, Office of the Director of National Intelligence, January 6, 2017.
[9] Id., p. 2.
[10] Id., p. 4.
[11] Id., p. 4.
[12] Id., p. 5.
[13] Wired, "Meet the Macedonian Teens Who Mastered Fake News and Corrupted the U.S. Election.", by Samanth Subramanian, February, 2017.

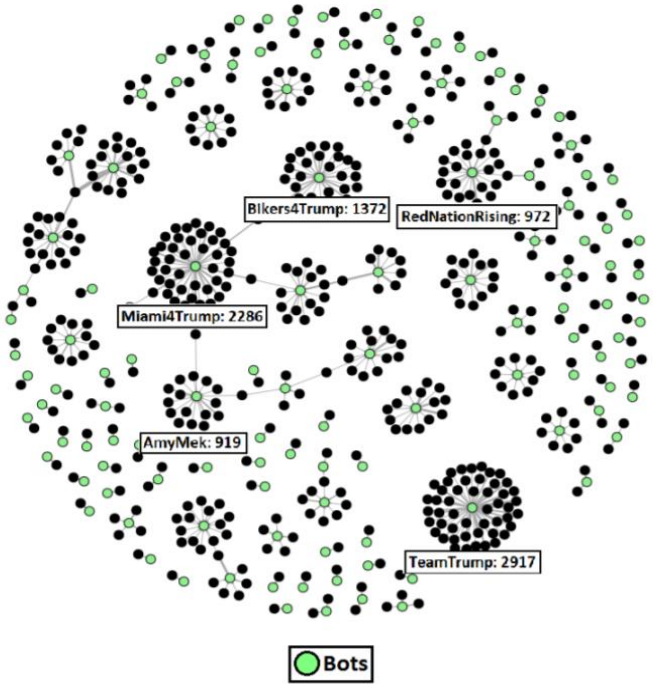
Political campaigns, candidates, and supporters have made use of bots in attempts to manipulate public opinion in the United States for almost a decade.[14] A recent study provided ethnographic evidence that bots affect information flows in two key ways: firstly, by "manufacturing consensus," or giving the illusion of significant online popularity in order to build real political support, and secondly, by democratizing propaganda through enabling nearly anyone to amplify online interactions for partisan ends (Woolley and Guilbeault, 2017). While we do not object to the existence of bots, we take serious objection with the use of bots posing as humans to deceive users and propagate fake news.

During the 2016 election, bots were used numerous times to drive up traffic around a particular event or idea. Figure 1 illustrates the impact of bot accounts by showing how human and bot accounts on Twitter interacted during the 2016 U.S. presidential election. In this network, the average number of times that a given person retweeted a bot was five. The results of this analysis confirm that bots reached positions of measurable influence during the 2016 U.S. election.[15] Research from several other sources also suggests that political bot usage was at an all-time high during key moments of this particular election (Bessi & Ferrara, 2016; Howard et al., 2016; Ferrara et al., 2016). Bots are also used in a transnational industry of artificial "likes" and followers. For example, a review of President Donald Trump's Twitter followers by *Newsweek* in May determined that only 51 percent of his 30 million followers were real.[16] While Twitter has attempted to foil attempts to use bots to create fake "trends" (lists of most-discussed topics or hashtags), it was found that suspected Russian bots sometimes managed to do just that, for example, in one case causing the hashtag #HillaryDown to be listed as a trend.

Additionally, Mønsted et al. (2017) demonstrate that networks of Twitter-bots can be used to seed the spread of norms and misinformation, which spread in a complex, contagious fashion. Such methods establish the potential for bots to influence political discussion online. For instance, at the height of Pizzagate, the conspiracy that linked the Clinton campaign to an alleged human trafficking and child abuse ring, automated shell accounts rampantly spread memes putting Clinton campaign Chair John Podesta and the candidate herself at the centre of the fabricated controversy. A disproportionate number of the accounts generating traffic on Pizzagate appeared to originate from foreign locations in Cyprus, the Czech Republic, and Vietnam (Albright, 2016b). According to the Washington Post, "[A]s the bots joined ordinary Twitter users in pushing out Pizzagate-related rumors, the notion spread like wildfire" (Fisher et al., 2017).

[14] Samuel C. Woolley & Douglas Guilbeault, "Computational Propaganda in the United States of America: Manufacturing Consensus Online." Samuel Woolley and Philip N. Howard, Eds. Working Paper 2017, Oxford, UK: Project on Computational Propaganda. http://comprop.oii.ox.ac.uk/. 28 pp.
[15] Id., p. 22.
[16] PM, Ryan Bort On 5/30/17 at 4:43. "Almost Half of Trump's Twitter Followers Appear to Be Fake." Newsweek, May 30, 2017. http://www.newsweek.com/donald-trump-twitter-followers-fake-617873.

The aforementioned examples make the extent of our vulnerability to foreign manipulation via social media platforms exceptionally clear. The use of fake accounts and bots in spreading misinformation has dire implications for U.S. values of free, fair and credible elections without the influence of any foreign actors. The technical and policy issues of authenticating our digital identities online must be managed with an incredible sense of urgency to ensure that such issues can be minimized for future elections.



Note: In this figure, the bots are coloured green and the humans are coloured black. A connection is drawn between a human and a bot only if the human retweeted that bot. The boldness of an edge is weighted by the number of times that the human user retweeted the bot. The bots with the highest number of humans retweeting them are labelled, with the number of connections beside their name. We removed all bots that were retweeted by only one human, along with all their connections, for the purposes of visualization. This is why thousands of connections are not displayed for the bots with the highest indegree.

Figure 1: A Directed Network of Humans Retweeting Bots (only including connections where a human user retweeted a bot in a network of 15,904 humans and 695 bots). Source: Woolley & Guilbeault, 2017.

2.1.3 Users cannot distinguish between fake and real accounts

One of the main issues in countering the spread of fake news is that users of social media platforms are unable to detect whether or not the profile posting information regarding U.S. politics can be traced back to a foreign account. This is because illegitimate news content appears on social media platforms alongside articles from legitimate outlets or profiles, with no obvious distinction between the two. Even skilled investigators often cannot deduce with certainty if a particular Facebook post or Twitter bot came from Russian intelligence employees, paid “trolls” in Eastern Europe or hackers from Russia’s vast criminal underground.

Similar to fake profiles run by humans, research abounds showing that people are inherently and incurably poor at detecting bots online (Edwards et al., 2014; Guilbeault, 2016). While bot accounts on Twitter characteristically tweet frequently, retweet one another, and disseminate links to external content more often than human-operated accounts, studies have demonstrated the difficulty of detecting bots through any single criterion. Malicious bots, which have made up the majority of bot activity since 2013, are said to be unidentifiable by design.[17]

2.2 Current considerations by private industry

So far, social media companies have been implicitly trusted to self-regulate their platforms against hate speech and inappropriate behaviour. The recent uptake in the spread of fake news has made platforms reconsider whether their efforts have been sufficient. In response, social media platforms have introduced additional steps to increase transparency and security to show their commitment to fighting foreign interference in elections and protecting legitimate online political discussions.[18]

2.2.1 User reporting

Platforms have considered the use of user reports to mark false or inaccurate information. For instance, Facebook announced that it will make it easier for users to report fake news when they see it, which they can do by clicking the upper right hand corner of a post.[19] If enough people report a story as fake, Facebook will pass it to third-party fact-checking organizations that are part of the nonprofit Poynter Institute's International Fact-Checking Network (see Section 2.2.2). Twitter is also considering a feature that would let users flag tweets that are false or inaccurate, in an attempt to combat the spread of disinformation on the platform.[20] It is not yet clear what Twitter would do with the information it gathers from such reports. One reason why efforts in the area have progressed slowly, and why it is still uncertain as to whether the feature will be fully rolled-out at all, is because of concerns that the new reporting feature could be used to "game the system".[21] Other reporting tools have ended up being abused in a similar manner, with individual users finding their accounts suspended after organized campaigns resulted in hundreds of reports of "abusive" behaviour in a short space of time. Additionally, social media companies can be accused of being politically biased for removing certain tweets after users report them or tag them as 'false'.

---

[17] Id., p. 9.
[18] "What is our action plan against foreign interference?", Facebook Help Center, Accessed November 22, 2017. https://www.facebook.com/help/1991443604424859.
[19] Rogers, James. "Facebook Announces Strategy to Tackle Fake News." Text.Article. Fox News, December 15, 2016. http://www.foxnews.com/tech/2016/12/15/facebook-announces-strategy-to-tackle-fake-news.html.
[20] Hern, Alex. "Twitter May Introduce Feature to Let Users Flag 'Fake News.'" *The Guardian*, June 30, 2017, sec. Technology. http://www.theguardian.com/technology/2017/jun/30/twitter-could-introduce-feature-to-let-users-flag-fake-news.
[21] Elizabeth Dwoskin, "Twitter is looking for ways to let users flag fake news, offensive content", The Washington Post, June 29, 2017. https://www.washingtonpost.com/news/the-switch/wp/2017/06/29/twitter-is-looking-for-ways-to-let-users-flag-fake-news/?utm_term=.1647efa48302

2.2.2 Fact checking

Some social media platforms have turned to machine-augmented fact-checking to combat the spread of fake news. For instance, Google launched a tool for its search and news results that will help people determine whether information is real by placing a "Fact Check" tag in its *News* results, in which it showcases results from fact-checking organizations like Politifact and Snopes.[22] However, despite the wide rollout, not every search will be paired with an indication that it has been fact-checked, and some of the sites Google is turning to for verification might disagree on the accuracy of the claim in question. It is unclear how Google will decide what to show in those cases.

Additionally, Facebook added its own warning label to stories that contain questionable information, tagging stories that appear in its News Feed as "disputed" along with a link to a third-party fact-checking site that explains why.[23] While users will still be able to share these stories, they will receive a warning that the story has been disputed, and stories that have been disputed may also appear lower in the News Feed. To implement this, the company is working with five fact-checking and news organizations (ABC News, The Associated Press, FactCheck.org, Politifact and Snopes), and this group is likely to expand. Facebook is also in the process of updating its policy to block ads from Pages that repeatedly share stories marked as false by third-party fact-checking organizations.[24] Nevertheless, it may take several days for a fact-checking website to get around to verifying a story while fake news can spread almost spontaneously as illustrated by recent examples such as Pizzagate. Several company representatives also fear that notifying users of fake accounts and bot threats will deter people from using their services, given the growing ubiquity of these threats and the nuisance such alerts would cause.

While these efforts can be seen as encouraging first steps by companies, fact checking and flagging stories as disputed have their limitations in terms of tackling fake news. According to some social media experts, people will continue to share posts they believe is from someone they 'trust'. Moreover, disputing a story can be debatable since what one source deems to be fake news may not be fake according to another source. Most importantly, it takes some time before a fact-checking organization determines that a particular story is a hoax and before a social media channel can take any action to counter its spread, by which time the fake story will have already garnered massive attention among users who believe it to be true.

2.2.3 Automated detection of fake accounts and bots

Some companies are turning to technical advances to increase protections against manually created fake accounts and using new analytical techniques, including machine learning, to uncover and disrupt fake accounts. Facebook has made recent improvements to recognize inauthentic accounts

[22] April Glaser, "Google is rolling out a fact-check feature in its search and news results: The search giant is trying to battle the spread of fake news", Recode, April 8, 2017.
[23] "News Feed FYI: Addressing Hoaxes and Fake News | Facebook Newsroom." Accessed November 24, 2017. https://newsroom.fb.com/news/2016/12/news-feed-fyi-addressing-hoaxes-and-fake-news/.
[24] "Blocking Ads from Pages That Repeatedly Share False News | Facebook Newsroom." Accessed November 23, 2017. https://newsroom.fb.com/news/2017/08/blocking-ads-from-pages-that-repeatedly-share-false-news/.

more easily by identifying patterns of activity without assessing account contents themselves. This allows its systems to detect repeated posting of the same content or aberrations in the volume of content creation. These improvements enabled Facebook to take action against over 30,000 accounts posting such content in France.[25]

Google's Eric Schmidt has been quoted to favor means of 'engineering' Russian propaganda out of the feed.[26] He believes that patterns of fake news can be detected, and then taken down or deprioritized. Schmidt also believes that the problem of fake news can be ascribed to "basically RT and Sputnik" and that systems can be engineered to prevent these two channels from attaining influence. Such automated means of detection are appealing for web companies, who typically resist the practice of hiring human editors, which they believe would make them vulnerable to criticisms of partisan bias and stray from their core business of building software. However, Facebook, Google and other sites have struggled to find automated solutions to clamp down on fake news, because there is not always a clear line between true and false news online.[27] Identifying the 'truth' has been complicated for platforms, who do not want to become the arbiters of what is and is not true.

Computer scientists have attempted to train AI algorithms to detect anomalies that distinguish bot accounts from those operated by humans.[28] But adding to the complication of automated detection is the fact that the public discussion of false amplifiers is not solely driven by easily detectable automated social bots. The real problem is that people with a high number of followers will continue to share fake posts on social media. Facebook has observed that most false amplification in the context of information operations is not driven by automated processes, but by coordinated people who are dedicated to operating inauthentic accounts. Moreover, Facebook revealed in its Information Operations report that they "observed many actions by fake account operators that could only be performed by people with language skills and a basic knowledge of the political situation in the target countries, suggesting a higher level of coordination and forethought".[29] This shows that even if algorithms are taught to detect bots and fake accounts, the problem cannot be mitigated by purely technical means in the future. We believe that as long as there exists the desire to deceive, fake accounts posting misinformation will continue to emerge in increasingly sophisticated ways.

---

[25] Jen Weedon, William Nuland and Alex Stamos, "Information Operations and Facebook", Facebook Security, April 27, 2017 Version 1.0. https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf

[26] Ling, Justin. "Google Chief Says Google News Will 'Engineer' Russian Propaganda Out of the Feed." Motherboard, November 20, 2017. https://motherboard.vice.com/en_us/article/pa39vv/eric-schmidt-says-google-news-will-delist-rt-sputnik-russia-fake-news.

[27] Dwoskin, Elizabeth, Caitlin Dewey, and Craig Timberg. "Why Facebook and Google Are Struggling to Purge Fake News." *Washington Post*, November 15, 2016, sec. Business. https://www.washingtonpost.com/business/economy/why-facebook-and-google-are-struggling-to-purge-fake-news/2016/11/15/85022897-f765-422e-9f53-c720d1f20071_story.html.

[28] Ferrara, Emilio, Onur Varol, Clayton Davis, Filippo Menczer, and Alessandro Flammini. "The Rise of Social Bots." *Communications of the ACM* 59, no. 7 (June 24, 2016): 96–104. https://doi.org/10.1145/2818717.

[29] Id.

2.2.4 Increasing Ad Transparency

Several fake news writers have exploited social media platforms to generate ad revenue. One prolific, Facebook-focused fake-news writer named Paul Horner disclosed to the Washington Post that he makes approximately $10,000 a month from AdSense.[30] Moreover, among the growing group of Macedonian teenagers who take advantage of American gullibility to make easy money from fake news, the most successful can make about $5,000 a month.[31]

Although Facebook has stated that it is not in a position to make definitive attribution to the actors sponsoring fake news ads on its platform, the company has recently opened the door to reporting and disclosing the origins of the political advertising on its platform.[32] To do so, the platform is building a tool that will allow users to click a link and see the ads a Page is running, even ones not targeted to them directly. Anyone purchasing U.S. election ads will also now be required to confirm who they are.[33] Additionally, in a Facebook post shared on November 22, 2017, Sheryl Sandberg, Facebook COO, announced, "Today we're sharing that we're building a tool to let people see which, if any, of the Internet Research Agency Facebook Pages or Instagram accounts they may have liked or followed between January 2015 and August 2017." According to Facebook, this tool will be available by the end of the year as "part of our ongoing effort to protect our platforms and the people who use them from bad actors who try to undermine our democracy".[34]

Fake news writers like Horner warn that although such an ad policy might initially be devastating for their revenue, he and others like him who have been engaged in the business of fake news for a long time[35] would be able to adapt to the changes. Moreover, while the new ad policy is a positive step, such tools would fall short of demands by U.S. lawmakers that Facebook individually notify users about Russian propaganda posts or ads they were exposed to. However, platforms like Facebook are not required by U.S. law to report posts made on its platform by foreign actors regarding U.S. elections or any other topic.[36] Therefore, while increasing the transparency of ads

---

[30] "Analysis | This Is How Facebook's Fake-News Writers Make Money." Washington Post. Accessed November 22, 2017. https://www.washingtonpost.com/news/the-intersect/wp/2016/11/18/this-is-how-the-internets-fake-news-writers-make-money/.

[31] Alexander, Craig Silverman Lawrence. "How Teens In The Balkans Are Duping Trump Supporters With Fake News." BuzzFeed. Accessed November 23, 2017. https://www.buzzfeed.com/craigsilverman/how-macedonia-became-a-global-hub-for-pro-trump-misinfo.

[32] Romm, Tony. "Facebook Told the U.S. Government That It's Open to New, Limited Political Ad Disclosure Rules." Recode, November 13, 2017. https://www.recode.net/2017/11/13/16646688/facebook-political-ads-fec-disclosure-rules-russia-election.

[33] "Blocking Ads from Pages That Repeatedly Share False News | Facebook Newsroom." Accessed November 23, 2017. https://newsroom.fb.com/news/2017/08/blocking-ads-from-pages-that-repeatedly-share-false-news/.

[34] Id.

[35] "This Is Not an Interview with Banksy." Washington Post. Accessed November 25, 2017. .

[36] The Federal Election Campaign Act requires candidate committees, party committees and PACs to file periodic reports with the Federal Election Commission (FEC) disclosing the money they spend, including funds used to buy online ads. In 2006, the FEC updated its regulations to clarify that the law applies to paid advertisements that outside groups place on another person's website. In that same 2006 rulemaking, the FEC determined that content posted online for free, such as blogs, is off limits from regulation. Consequently,

could be helpful, such efforts cannot counter the spread of fake news by foreign actors who do not choose to engage in advertising or 'boosting' their posts with additional money.

2.2.5 Takedowns and bans

Facebook has been investing in operations and hiring 10,000 people including ad reviewers, engineers and security experts and combining their skills with automated means to identify and remove content violations and fake accounts.[37] In October 2017, Twitter decided to ban "advertising from all accounts owned by *Russia Today* (RT) and *Sputnik*, two Russian state-owned media outlets.[38] However, the problem is less straightforward than simply finding Russian or other foreign-linked posts and taking down content; such takedowns of fake posts has implications for free and anonymous speech on social media. The Electronic Frontier Foundation has argued that Twitter's ban on all ads and posts from a particular entity constitutes an over-broad prior restraint on speech.[39] Such a ban also defies the content-neutral aspect of social media platforms, sets a new dangerous precedent for curtailing free speech and impacts the reader's free expression right to receive information.

Twitter's ban even goes beyond U.S. electoral rules, which do not support a total ban on paid promotions even if the promoter violated the laws governing foreign nationals' participation in U.S. elections.[40] Under the Federal Election Commission rules, foreigners can fund ads if they are not "election influencing" i.e. that they do not mention candidates, political offices, political parties, incumbent federal officeholders or any past or future election. However, U.S. law "does not restrain foreign nationals from speaking out about issues or spending money to advocate their views about issues." Therefore, we contend that there are better and more nuanced ways to fight improper interference in U.S. elections than Facebook's takedowns and Twitter's overbroad ban on particular foreign entities, which restricts freedom of expression.

2.2.6 Examining the need for our proposal

From the above discussion, we conclude that given the difficulty of manually taking down fake content as well as spotting fake news and propaganda using just automated computer programs,

---

posting political content on social media platforms such as Twitter and Facebook as opposed to paying to run ads on those sites falls under activities that do not need to be reported to the FEC.
See Gold, Matea. "Did Facebook Ads Traced to a Russian Company Violate U.S. Election Law?" *Washington Post*, September 7, 2017, sec. Post Politics. https://www.washingtonpost.com/news/post-politics/wp/2017/09/07/did-facebook-ads-traced-to-a-russian-company-violate-u-s-election-law/.

[37] "An Update On Information Operations On Facebook | Facebook Newsroom." Accessed November 23, 2017. https://newsroom.fb.com/news/2017/09/information-operations-update/.

[38] "Announcement: RT and Sputnik Advertising." Accessed November 4, 2017. https://blog.twitter.com/official/en_us/topics/company/2017/Announcement-RT-and-Sputnik-Advertising.html.

[39] Opsahl, Kurt. "Twitter's Ban on Russia Today Ads Is Dangerous to Free Expression." Electronic Frontier Foundation, October 27, 2017. https://www.eff.org/deeplinks/2017/10/twitters-ban-russia-today-ads-dangerous-free-expression.

[40] "Foreign Nationals." FEC.gov. Accessed November 5, 2017. https://www.fec.gov/updates/foreign-nationals/.

there is a dire need for a better verification system for digital identity on social media platforms. We argue that fact-checking and user reports themselves are insufficient measures to curb the spread of fake news by foreign actors. This is because fact-checking and deleting fake posts in response to user complaints takes considerably more time than the time taken for fake news to spread and impact user options and actions. Given the time and the resources involved in fact-checking, it does not serve the purpose of helping people make more informed decisions regarding the veracity of a post when they encounter fake news from foreign agents or bots. Additionally, user report features, takedowns and bans can be significantly abused to shut down unwanted voices and censor legitimate free speech.

For relatively faster methods such as automated detection of fake posts or profiles, fake bot accounts are difficult to counter from a technical standpoint[41] and it is only a matter of time before fake news writers develop greater sophistication to avoid detection. So while companies are starting to use technical tools and teams of analysts to detect fake accounts, the scale of the sites (328 million users on Twitter and nearly two billion on Facebook) means they often remove fake accounts only in response to complaints. Additionally, as Table 1 illustrates, efforts to increase ad transparency can only tackle fake accounts associated with monetary incentives while automated AI-powered methods are mostly aimed at detecting fake bot accounts using anomalous features of bot activity.

	Fake human-administered accounts	*Fake bot-administered accounts*
Monetary incentives	Ad transparency	Some automated detection and ad transparency
Political incentives	**Not sufficiently countered**	Some automated detection

Table 1: Measures for countering fake news by private industry based on type of fake account and incentives of the account holder. User reporting, fact-checking, takedowns and bans are general, often time-consuming methods of countering fake news that apply to all of the above four sections, but are insufficient means with negative consequences.

Critics argue that one of the possible reasons for the lack of greater action taken to combat the spread of fake news on behalf of companies is that it puts their bottom line at risk. Since shareholders judge the companies partly based on a crucial data point, "monthly active users", companies are reluctant to police their sites too aggressively for fear of reducing that number. Although they are yet to comprehensively disclose the numbers, social media companies have also profited from the spread of fake Russian propaganda meant to bias American users. Already, Facebook has uncovered $100,000 in fake ad spending tied to Russian operatives during the 2016

[41] "In the Battle against Fake News, the Bots May Be Winning." World Economic Forum. Accessed November 25, 2017. https://www.weforum.org/agenda/2017/11/fake-news-bots-are-winning/.

U.S. Presidential Election,[42] and Twitter said it has been paid nearly $2 million from RT, the Russian state-funded media, alone since 2011.[43] While Google has more of an incentive to make information reliable because its business is based on providing accurate information to those looking for it, Facebook "is about attention, not so much intention."[44] Therefore, social media platforms have some business incentive to let viral stories, whether legitimate or hoax, continue to stay on the platform. According to David Carroll,[45] an associate professor of media design at the New School and an expert in advertising tech, companies such as Google and Facebook use a business model that has changed little over the years, whereby each company could "lose revenue if it shuts down a huge number of fake sites".

In the larger picture, not all hoaxers are motivated by money. Cutting off the revenue of those who make fake news to earn a living will not stop people from sharing stories that are untrue because political incentives for misinformation will still exist even if monetary incentives are removed as mentioned in the Intelligence Community Assessment report of January 6, 2017. Therefore, the methods currently under consideration by private industry are insufficient to counter the negative impact of fake news proliferation by foreign actors, especially those with political incentives to misinform and deceive U.S. residents as a means of election tampering. This illustrates the need for a solution that can enable users to easily distinguish between social media posts made by U.S. residents who have a real stake in discussing socio-political affairs pertaining to their country and fake news posts made by foreign actors intending to bias the opinions of U.S. residents.

While a successful solution would effectively counter the spread of fake news by foreign actors with political incentives to misinform U.S. residents, it must also remain consistent with the U.S. legal tradition and protect the democratic values of free speech, freedom of association and the right to anonymous political speech on the Internet. Any such solution must also not compromise the privacy of social media users or give the U.S. government any more personal information about users than it already has to avoid potential abuses of power. It is also important that any form of digital identity solution is secure and does not make its users more vulnerable to identity theft. Finally, we believe that it is essential not to restrict sources of information on social media platforms through measures involving takedowns and bans or by enabling certain authorities – whether private entities or governments – to assume the role of an arbiter of the truth; instead, a success solution for mitigating fake news must add greater nuance to information consumed by social media users by furthering their digital literacy and promoting their ability to make informed decisions.

---

[42] "Facebook Uncovers $100G in Fake Ad Spending Tied to Russian Operatives during 2016 Election | Fox News." Accessed November 24, 2017. http://www.foxnews.com/tech/2017/09/06/ facebook-uncovers-100g-in-fake-ad-spending-tied-to-russian-operatives-during-2016-election.html.

[43] "Twitter Bans Russia Today And Sputnik From Advertising On Its Platform." *WeRSM - We Are Social Media* (blog), October 30, 2017. http://wersm.com/twitter-bans-russia-today-and-sputnik-from-advertising-on-its-platform/.

[44] Id.

[45] "David Carroll - Associate Professor." Accessed November 23, 2017. https://www.newschool.edu/parsons/faculty/David-Carroll/.

3 Comparative analysis of national digital identity systems

We advocate for a narrowly-tailored digital identity verification system, as opposed to a universal national identity system that cuts across other services and government functions. Our reasoning for scoping the system in this manner is threefold: 1) the privacy and security implications of extending the U.S. Social Security Number (SSN) system to a digital identity system, 2) backlash against the REAL ID Act of 2005, and 3) the American public's distrust of the government to handle personal data.

Several countries have already implemented their own versions of digital identity systems. We discuss the fully-implemented and functional digital identity schemes of India and Estonia, instituted in 2009 and 2014, respectively. We examine the precedents they set forth in terms of design implementation and security measures that need to be established for such an endeavor to be possible in the U.S., taking into consideration the differing historical contexts and policy concerns of each country. From our analysis, we identify two common points of vulnerability in existing digital identity systems that are important to consider for a future analog in the U.S. The first is on the user-end: assigning a single, global identifier to an individual for their authentication and verification across multiple platforms (i.e., for email, bank, and health services), poses a serious security concern if this identifier were to be obtained by an intruder. The second is on the back-end: compiling personal records in a central, national repository is an obvious target for malevolent actors. India and Estonia's identity schemes offer insights into the possible solutions and pitfalls of a system structured in this manner.

3.1 Identity in the United States

3.1.1 Overview of the U.S. Social Security Number system

Before the 1930s, support for the elderly was not considered a federal concern in the United States, but a local and family one. However, widespread suffering caused by the Great Depression ushered in proposals for a national old-age insurance system, along with many other financial and economic reforms. Opponents of the proposed retirement insurance system considered such legislation as governmental invasion of the private sphere. Nonetheless, with increasing economic pressures from the Great Depression, the Social Security Act was signed into law in one fell swoop as a part of the New Deal by President Franklin D. Roosevelt in 1935.[46]

Since its inception in 1936,[47] the Social Security Number (SSN) system has become the U.S.'s *de facto* national ID system. Upon creation, its sole purpose was to track the earnings histories of U.S. workers so the Social Security Administration could calculate their Social Security benefit entitlement and levels. Although this is still the primary purpose of the SSN, it has since been

[46] "Social Security Act (1935)." 100 Milestone Documents, https://www.ourdocuments.gov/doc.php?flash=true&doc=68.
[47] Yurieff, Kaya. "Why Are We Still Using Social Security Numbers as ID?" CNN Money, 2017, http://money.cnn.com/2017/09/13/technology/social-security-number-identification/index.html.

adopted for a number of identification purposes by private industry and government agencies. This is mostly due to the fact that the SSN provides a unique number that identifies each individual, which can be an efficient, albeit irresponsible, way for institutions to keep track of their employees. Coupled with a wide lack of understanding of the narrow purpose and intent of the SSN, it was in this poorly-wielded manner that the SSN became America's *de facto* national identity system.[48]

Importantly, the SSN was never designed to be secure for SSN holders.[49] This fact has become increasingly obvious in light of recent data breaches of major companies and agencies, including Equifax,[50] Yahoo,[51] Target,[52] and the U.S. Office of Personnel Management.[53] With just the Equifax data breach alone, hackers had access to SSNs of nearly one-third of the American population. According to a study by Statista.com, data breaches have become significantly larger in number and impact, starting from 157 million data breaches in 2005 to 1 billion in 2016.[54] Moreover, researchers at Carnegie Mellon were able to devise an algorithm capable of predicting an SSN correctly 44% of the time for an individual in the U.S. overall and as much as 90% of the time for an individual in a given state, using data from the Social Security Administration's publicly available SSN Death Master file.[55]

The Social Security Number system itself and the circumstances surrounding it are teeming with security insufficiencies and incompatibilities. Given the incidents and findings above, we conclude that the SSN system is inadequate for our proposal, in which we aim for a robustly secure ID system using encryption techniques. We therefore dismiss the opportunity to build off of the outmoded and narrowly-purposed Social Security Number system, the U.S.'s existing ID system, and instead consider more modern implementations of identity schemes by other countries. We consider the SSN relevant to our proposal only to the extent that there exists a system in the U.S. that is indeed capable of accounting for every U.S. resident without duplicates. The SSN system itself, in terms of its design and implementation, is not suitable for extension to a digital identity verification system (see 3.2.1 for more details).

---

[48] Puckett, Carolyn. The Story of the Social Security Number. Social Security Office of Retirement and Disability Policy, https://www.ssa.gov/policy/docs/ssb/v69n2/v69n2p55.html.
[49] Rotenberg, Marc. EPIC Testimony on the Use and Misuse of the Social Security Number. EPIC, 11 May 2000, https://epic.org/privacy/ssn/testimony_0500.html.
[50] Wolff, Josephine. The Equifax Hack Means It's Time to Stop Pretending Social Security Numbers Are Secure IDs. 2017, https://qz.com/1093213/why-do-we-still-use-social-security-numbers-to-prove-our-identities/.
[51] Larsen, Serena. "Every Single Yahoo Account Was Hacked - 3 Billion in All." CNN Tech, 2017, http://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html.
[52] McCoy, Kevin. "Target to Pay $18.5M for 2013 Data Breach That Affected 41 Million Consumers." U.S.A Today, 5–23 2017, https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/.
[53] Cybersecurity Resource Center: What Happened. U.S. Office of Personnel Management, https://www.opm.gov/cybersecurity/cybersecurity-incidents/.
[54] Identity Theft Resource Center; CyberScout. Annual Number of Data Breaches and Exposed Records in the United States from 2005 to 2016 (in Millions). Statista, 2017, https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/.
[55] Timmer, John. "New Algorithm Guesses SSNs Using Date and Place of Birth." Ars Technica, 2009, https://arstechnica.com/science/2009/07/social-insecurity-numbers-open-to-hacking/.

3.1.2 The policy debate following the REAL ID Act of 2005

In March 2007, the U.S. Department of Homeland Security (DHS) announced that it would establish "minimum standards for State-issued driver's licenses and identification cards that Federal agencies would accept for official purposes after May 11, 2008, in accordance with the REAL ID Act of 2005".[56] The DHS draft regulations would have created a *de facto* national identification system by requiring changes to the design of licenses and identification cards, and expanding schedules and procedures for retention and distribution of identification documents and personal data, among other changes. It would also make REAL ID cards necessary for "accessing Federal facilities, boarding commercial aircraft, and entering nuclear power plants."[57]

As it was being considered, a group of experts in privacy and technology reached the conclusion that REAL ID was fundamentally flawed, unworkable and must be repealed.[58] This was because the Act created an illegal de facto national identification system filled with threats to privacy, security and civil liberties, which could not be resolved regardless of the implementation plan. Twelve U.S. senators also stated that REAL ID "places an unrealistic and unfunded burden on state governments and erodes Americans' civil liberties and privacy rights".[59]

Although the use of the SSN system has expanded considerably as explained in Section 3.1.1, it is not a universal identifier and efforts to make it one have been consistently rejected as has the idea of a national identification system by members of national leadership and civil liberties committees.[60] In 1973, the Health, Education and Welfare Secretary's Advisory Committee on Automated Personal Data Systems rejected the creation of a national identifier and advocated for significant safeguards to protect personal information.[61] In 1977, the Carter Administration reiterated that the SSN would not become an identifier. In 1981, Attorney General William French Smith stated that the Reagan Administration was "explicitly opposed to the creation of a national

---

[56] Dep't of Homeland Sec., Notice of Proposed Rulemaking: Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes, Fed. Reg. 10,819, Mar. 9, 2007. http://a257.g.akamaitech.net/7/257/2422/01jan20071800/edocket.access.gpo.gov/2007/07-1009.htm.

[57] See REAL ID Draft Regulations at *supra* note 1.

[58] Department of Homeland Security, Docket No. DHS 2006-0030, "Notice of Proposed Rulemaking: Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes", Comments of Electronic Privacy Information Center (EPIC) AND [Experts in Privacy and Technology]. https://epic.org/privacy/id_cards/epic_realid_comments.pdf

[59] Press Release, S. Comm. on Homeland Sec. & Governmental Affairs, Twelve Senators Urge Frist To Keep Real ID Act Off Supplemental Appropriations Bill Sweeping Proposal Needs Deliberate Consideration, Apr. 12, 2005. http://www.senate.gov/%7Egov_affairs/index.cfm?FuseAction=PressReleases.Detail&Affiliation=R&PressRelease_id=953&Month=4&Year=2005.

[60] Marc Rotenberg, Exec. Dir., EPIC, Testimony and Statement for the Record at a Hearing on Social Security Number High Risk Issues Before the Subcomm. on Social Sec., H. Comm on Ways & Means, 109th Cong., March 16, 2006. http://www.epic.org/privacy/ssn/mar_16test.pdf

[61] The committee said, "We recommend against the adoption of any nationwide, standard, personal identification format, with or without the SSN, that would enhance the likelihood of arbitrary or uncontrolled linkage of records about people, particularly between government or government-supported automated personal data systems. What is needed is a halt to the drift toward [a standard universal identifier] and prompt action to establish safeguards providing legal sanctions against abuses of automated personal data systems". See Dep't of Health, Educ. & Welfare, Sec'y's Advisory Comm. on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens, July 1973, http://www.epic.org/privacy/hew1973report/.

identity card."[62] The U.S. Congress also made it clear in the enabling legislation of the DHS that the agency could not create a national ID system.[63] In September 2004, the incumbent DHS Secretary Tom Ridge reiterated, "[t]he legislation that created the Department of Homeland Security was very specific on the question of a national ID card. They said there will be no national ID card."[64]

Under REAL ID, the government would have easy access to an incredible amount of personal data stored in one national database. In a significant expansion of the personal data previously reviewed or stored by State motor vehicle agencies, the Act compelled States to begin maintaining paper copies or digital images of important identity documents, such as birth certificates or naturalized citizenship papers, for seven to 10 years. This would make identification documents originally kept in numerous places – the Social Security system, the immigration system, local courthouses – accessible to at least tens of thousands of government employees nationwide. Such a broad expansion of data collection and retention could create significant threats to privacy and security. For instance, a centralized system used across the nation would put hundreds of millions of people at risk for identity theft. Moreover, the Act allowed the DHS to contemplate expanding the REAL ID card into everyday transactions in a way that would make it easy for insurance firms, credit card companies, even video stores, to demand a REAL ID driver's license or ID card to receive services. This would expand the uses of the REAL ID system so that the card becomes a national identifier – one card for each person throughout the country. According to security expert Bruce Schneier, EPIC and others, it decreases security to have one ID card for many purposes since a substantial amount of harm could be caused when the card is compromised.[65] Using a national ID card was likened to using one key to open your house, your car, your safe deposit box, your office, and more.[66]

We draw two main lessons from the policy debate ensuing the REAL ID Act of 2005. Firstly, given the security and privacy concerns of mandating a national ID system, we advocate against the creation of any centralized digital identification system such as the one realized under REAL ID. Any newly-created digital identity system must be narrowly tailored to a single purpose; in our case, it would only allow for the verification of U.S. residential status on social media platforms that choose to incorporate the system. Moreover, any official and unofficial purposes of such a digital verification system must not be increased beyond its specific original use, federal agencies should not have universal access to such a system and third-party collection or storage of data from the digital verification system must not be allowed. This is important because there must be no restrictions on the ability of U.S. residents to share their ideas freely on social media platforms,

[62] Robert B. Cullen, Administration Announcing Plan, Associated Press, July 30, 1981.
[63] Pub. L. No. 107-296, 116 Stat. 2135 (2002).
[64] Tom Ridge, Sec'y, Dep't of Homeland Sec., Address at the Center for Transatlantic Relations at Johns Hopkins University: "Transatlantic Homeland Security Conference" (Sept. 13, 2004), available at http://www.dhs.gov/xnews/speeches/speech_0206.shtm.
[65] Melissa Ngo, Dir., EPIC Identification & Surveillance Project, Prepared Testimony and Statement for the Record at a Hearing on "Maryland Senate Joint Resolution 5" Before the Judicial Proceedings Comm. of the Maryland Senate (Feb. 15, 2007) ["EPIC Testimony at Maryland Senate"], available at http://www.epic.org/privacy/id_cards/ngo_test_021507.pdf.
[66] Melissa Ngo, Dir., Identification & Surveillance Project, EPIC, Prepared Testimony and Statement for the Record at a Meeting on "REAL ID Rulemaking" Before the Data Privacy & Integrity Advisory Comm., Dep't of Homeland Sec. Apr. 14, 2007. http://www.epic.org/privacy/id_cards/ngo_test_032107.pdf.

without fear of reprisal. Since the right to have conversations unmonitored by the government is essential to democracy, statutory and technical limitations must be set to prohibit the linkage of personal data on social media platforms to official or unofficial government records. This can be achieved by limiting the role of the government to only generating and replacing lost pairs of private and public keys for U.S. residents[67] while leaving the implementation details of introducing the digital identity verification system on various platforms to private social media companies.

Secondly, the group of experts in privacy and technology and the Electronic Privacy Information Center (EPIC) also recommended that if REAL ID implementation does go forward, the protections of the Privacy Act of 1974 must be fully enforced for all uses. The Privacy Act of 1974 was intended "to promote accountability, responsibility, legislative oversight, and open government with respect to the use of computer technology in the personal information systems and data banks of the Federal Government".[68] It was also intended to guard the privacy interests of citizens and lawful permanent residents against government intrusion. Congress found that "the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies," and recognized that "the right to privacy is a personal and fundamental right protected by the Constitution of the United States."[69] According to the Office of Management and Budget guidelines, the Privacy Act "stipulates that systems of records operated under contract or, in some instances, State or local governments operating under Federal mandate 'by or on behalf of the agency . . . to accomplish an agency function' are subject to . . . the Act."[70] Therefore, any government-backed digital identity system must fully apply Privacy Act requirements of notice, access, correction, and judicially enforceable redress. To prevent any unauthorized access by third parties, any personal data in a digital identity system should be encrypted, and the user should be able to control who receives or accesses their data at any time.

3.1.3 American distrust of the U.S. government with digitized personal data

The Snowden disclosures of May 2013 had an immensely chilling effect on the future of America's personal data security in the hands of government and major privately-held companies that citizens entrust with their data. Broadly speaking, the U.S. government's most treacherous acts were twofold: secret court orders mandating overbroad collection of Americans' personal data, and secondly, even more covert, NSA-backed efforts to crack encrypted communications, thereby undermining Internet security.[71]

For months preceding the Snowden revelations, secret court orders issued by the Foreign Intelligence Surveillance Court had been requiring Verizon and other major cell-phone service providers to give the NSA the phone numbers, duration, time, routing information and other details

[67] See Section 5 for details on enrollment, storage and handling of lost private keys.
[68] S. Rep. No. 93-1183 at 1 (1974).
[69] Pub. L. No. 93-579 (1974).
[70] Pub. L. No. 109-13, 119 Stat. 231 (2005).
[71] Franceschi-Bicchierai, Lorenzo. "The 10 Biggest Revelations From Edward Snowden's Leaks." Mashable, 2014, http://mashable.com/2014/06/05/edward-snowden-revelations/#of26IC1w0PqV.

for any calls made within the U.S. or between the U.S. and other countries.[72] Although these court orders were kept secret from the public, they were known to private sector companies involved.

Despite this collusion, the U.S. continued to glean further data from private sector companies without their consent or knowledge through the NSA-backed programs XKEYSCORE and MUSCULAR. Using direct fiber optic (Ethernet) connections to the backbone of the Internet, the NSA collected and processed America's Internet searches, emails, documents, usernames and passwords, and other private communications under XKEYSCORE.[73] Through MUSCULAR, the NSA secretly broke into the main communications links that connect Yahoo and Google data centers around the world, which incited rage among the tech circles. With MUSCULAR, the NSA had uniquely positioned itself to collect data from hundreds of millions of user accounts at will, many of them belonging to Americans.[74]

In a January 2014 speech on reviewing signals intelligence, former President Obama attempted to assuage national concerns about the privacy and security of personal data. Although the President aimed to provide greater transparency to the government's surveillance activities and strengthen the protections of the privacy of U.S. citizens, it is unclear if the government did indeed succeed in regaining trust from the American public. While the government is still able to glean information from Americans in the name of national security through its surveillance activities, the American public is still the victim of such scrutiny. Although reforms to FISA Section 702, the national security letters, and Section 215 of the Patriot Act have been instituted to safeguard citizens' digital privacy,[75] little can be done to prevent our personal data from being collected and processed altogether, given that private sector companies still have broad and basically unlimited access to Americans' personal data.

3.2 India's Aadhaar program

In 2009, India rolled out its own digital identity program called Aadhaar under the Unique Identification Authority of India (UIDAI). Aadhaar is the world's most comprehensive and pervasive national identity program, with over 1 billion members are enrolled.[76] To obtain an Aadhaar ID, a citizen must submit both demographic and biometric data and is assigned a unique, 12-digit

[72] Verizon Forced to Hand over Telephone Data – Full Court Ruling. https://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order.
[73] Marquis-Boire, Morgan, et al. "XKEYSCORE: NSA's Google for the World's Private Communications." The Intercept, 2015, https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications/.
[74] Gellman, Barton, and Ashkan Soltani. "NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say." The Washington Post, 2013, https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html?utm_term=.66e291ef25d7.
[75] Obama, Barack. Remarks by the President on Review of Signals Intelligence. https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.
[76] State/UT Wise Ranking Based on Aadhaar Saturation as on 30th Sept, 2017. Unique Identification Authority of India, 30 Sept. 2017, p. 3, https://uidai.gov.in/images/StateWiseAge_AadhaarSat_24082017.pdf.

number.[77] The whole country's demographic and biometric data is stored in the Central Identities Data Repository (CIDR), which is maintained and operated solely by UIDAI. Today, Aadhaar has become the ubiquitous method for authentication and verification processes for Indian citizens, who receive a wide array of services including but not limited to pension schemes, employee provident funds, electoral roll verification, opening bank accounts, digital payments, and filing tax returns. As of May 2017, over fifty central government schemes are linked to Aadhaar.[78]

3.2.1 Biometric data as a method of uniquely identifying individuals

One of the main precedents that Aadhaar has set forth is the integration of biometric data to uniquely identify its citizens. Many other countries such as Estonia, Australia,[79] Singapore,[80] and Norway[81] have followed suit with their national digital identity systems, which endeavor to collect a number of different kinds of biometric data, such as headshots, fingerprints, and iris scans. In the following section, however, we dismiss the biometric portion of the Aadhaar implementation as a possible consideration for our proposal, due to the differences in privacy as a fundamental right between the two countries, and the existing Social Security Number (SSN) system's ability to narrowly account for all residents and workers in the U.S.

Until 24 August 2017, the right to privacy in India was not upheld as a fundamental right under the Indian Constitution. In *Justice K. S. Puttaswamy* v. *Union Of India*, a landmark decision overturning two precedential cases dismissing privacy as a fundamental right of citizens, the Supreme Court of India newly framed privacy as a "primordial" right that must be understood in the context of an interconnected world.[82] In the U.S., however, privacy has been a fundamental right since the birth of the nation. Additionally, the U.S. has heavy data protection laws that would put government collection of biometric data under close and unforgiving scrutiny. Because of this societal difference between the two countries, it is unlikely that biometrics can be a viable component of a digital identity scheme in the U.S. Today, with privacy safeguards newly in place, the biometrically-driven Aadhaar program faces an uphill battle in the courtrooms of India with heavy opposition from privacy advocates.[83]

What is more, the the origins of biometric data integration into Aadhaar trace back to India's first problematic and poorly designed National Population Register. By 2008, the country was suffering

[77] Aadhaar Enrolment. Unique Identification Authority of India, 2016, https://uidai.gov.in/enrolment-update/aadhaar-enrolment.html.
[78] Deepalakshmi, K. "The Long List of Aadhaar-Linked Schemes." The Hindu, 2017, http://www.thehindu.com/news/national/the-long-list-of-aadhaar-linked-schemes/article17641068.ece.
[79] Lee, Justin. "Australian Government to Launch Digital Pass Verification Service in Early 2018." Biometric Update, 2017, http://www.biometricupdate.com/201703/australian-government-to-launch-digital-pass-verification-service-in-early-2018.
[80] Lee, Justin. "Singapore's New Digital Identity System to Include Biometrics." Biometric Update, 2017, http://www.biometricupdate.com/201703/singapores-new-digital-identity-system-to-include-biometrics.
[81] "Norway's BankID Identity Scheme to Pilot App." Planet Biometrics, 2016, http://www.planetbiometrics.com/article-details/i/4645/desc/norways-bankid-identity-scheme-to-pilot-biometric-app
[82] Justice K. S. Puttaswamy v. Union Of India 8–24 2017, https://indiankanoon.org/doc/91938676/
[83] Srivas, Anuj. "Legal Tussle Over Mandatory-Voluntary Nature of Aadhaar Kicks Off Next Week." The Wire, 2016, https://thewire.in/68957/mandatory-voluntary-aadhaar-supreme-court/.

from excessive welfare spending due to leaky welfare delivery mechanisms, citizens who would register their name multiple times to receive extra social security benefits, and the rise of tax evasion. At the time, technology entrepreneurs and officials at the Unique Identification Authority of India (UIDAI) determined that the most efficient and effective method of weeding out duplicate identities from their register to was to digitize and "de-duplicate" the system by taking and storing biometrics of citizens.[84] However, the U.S. does not suffer from a similar fraudulent duplication problem internally. Although the Social Security Number (SSN) system cannot be considered an identity system analogous to Aadhaar, the U.S. has in fact managed to narrowly account for every domestic worker and resident without duplicates with the SSN system.

3.2.2 Contemporary pervasiveness of Aadhaar

Without a ruling on the constitutionality of Aadhaar, the Indian Supreme Court has continued to implicitly condone its use as a valid form of identification for an increasingly wide array of public services. Although Aadhaar was established in January 2009, the Indian government recently extended the use of Aadhaar for all types of pension schemes and employee provident funds under the Mahatma Gandhi National Rural Employment Guarantee Act (NREGA No. 42) on 15 October 2015. This is in addition to Aadhaar already being a valid form of proof of identity, electoral roll verification, opening bank accounts, digital payments, and filing tax returns.[85] Meanwhile, the Indian Supreme Court and federal government have responded to privacy violation allegations on the grounds that registering for Aadhaar is purely voluntary, despite enrollment being effectively unavoidable in India's modern landscape.

Although our proposed digital identity system is also voluntary and opt-in, we argue that the reason Aadhaar became essentially pervasive is because the Indian government used it to provide access to essential government services. Conversely, our proposed digital identity verification system is not used for access to any essential services or even any social media platforms i.e. it is not tied to any form of log-in system. The completely voluntary nature of our proposal rules out the privacy concerns tied to pervasive use as is the case for the Aadhaar identity system. In fact, pervasiveness in our case means that more and more users are encouraged to verify their U.S. residential status on social media accounts, which would increase the effectiveness of combating fake news perpetrated by foreign actors. The network effects of use associated with our digital identity verification system add to its effectiveness in combating fake news from foreign actors and bots.

Additionally, we rely on the unlikelihood of the U.S. to institute a national identity system that is equally as ubiquitous as Aadhaar. This is because of the country's long history of fierce opposition to central, national identity systems by civil liberties groups,[86] members of national leadership,[87]

---

[84] Aadhaar Shows India's Governance Is Susceptible to Poorly Tested Ideas Pushed by Powerful People. 2016, https://scroll.in/article/825103/aadhaar-shows-indias-governance-is-susceptible-to-poorly-tested-ideas-pushed-by-powerful-people.

[85] Deepalakshmi, K. "The Long List of Aadhaar-Linked Schemes." The Hindu, 2017, http://www.thehindu.com/news/national/the-long-list-of-aadhaar-linked-schemes/article17641068.ece.

[86] The committee said, "We recommend against the adoption of any nationwide, standard, personal identification format, with or without the SSN, that would enhance the likelihood of arbitrary or uncontrolled linkage of records about people, particularly between government or government-supported automated

and Congress,[88] and the fact that the REAL ID Act of 2005 was effectively repealed and replaced with more narrow legislation in 2007. Moreover, a study by the Pew Research Center showed that American public trust in the government with their personal data went down after the Snowden disclosures.[89] Therefore, given the vast differences in the legislative history and socio-political climate between India and the United States, we recommend against the adoption of a universal digital identification system like Aadhaar for providing access to various government services in the U.S.

3.2.3 Aadhaar ID number as a single, global identifier and corresponding security concerns

Concerns about the ubiquity of Aadhaar are echoed among security expert communities. Upon enrollment into Aadhaar, a user receives a single, 12-digit number they can use to authenticate and access a variety of government services across multiple domains including, bank accounts, social security benefits, and health records. Agrawal et al. point out a major security risk associated with this implementation: what if a user's 12-digit number ends up in the wrong hands? How many different services does the malevolent actor have access to as a result of this simple mishap?[90]

Analogous to this issue is the problem of password management by individual users: if a single user uses the same password for many different domains, an intruder can easily gain access to the user's email, bank account, and health records, provided that only one of the user's passwords is known. To circumvent this problem, the UIDAI advises that third-party services using Aadhaar authentication maintain an internal, unidirectional mapping between their domain-specific identifiers and the global Aadhaar numbers in their back-end systems. We propose an alternative solution in section 3.3.1, however, that utilizes a Public Key Infrastructure (PKI) for user authentication.

3.2.4 How Aadhaar informs our proposal

In addition to being impressive in scale and pervasiveness, Aadhaar sets important precedents for other countries endeavoring to implement a digital identity system of their own. However, it is derived from a different historical and societal context than that of the U.S. Although Western democracies such as Australia and Norway have also integrated biometrics into their national digital identity systems much as Aadhaar does, a biometrically-driven identity program cannot be easily assimilated into the American political or societal climate.

---

personal data systems. What is needed is a halt to the drift toward [a standard universal identifier] and prompt action to establish safeguards providing legal sanctions against abuses of automated personal data systems". See Dep't of Health, Educ. & Welfare, Sec'y's Advisory Comm. on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens, July 1973, http://www.epic.org/privacy/hew1973report/.

[87] Robert B. Cullen, Administration Announcing Plan, Associated Press, July 30, 1981.

[88] Pub. L. No. 107-296, 116 Stat. 2135 (2002).

[89] Gao, George. What Americans Think about NSA Surveillance, National Security and Privacy. Pew Research Center, 5–29 2017, http://www.pewresearch.org/fact-tank/2015/05/29/what-americans-think-about-nsa-surveillance-national-security-and-privacy/.

[90] Agrawal, Shweta, et al. Privacy and Security of Aadhaar: A Computer Science Perspective. Computer Science and Engineering, IIT Delhi, p. 15, http://www.cse.iitm.ac.in/~shwetaag/papers/aadhaar.pdf.

However, the Aadhaar system does provide insights into how a potential design implementation in the U.S. could be improved. As opposed to a ubiquitous national identity scheme that encompasses access to a wide range of services, we narrowly scope our digital identity program to provide an authentication and verification mechanism that aims to reduce foreign influences on our domestic electoral processes through online social media platforms. In doing so, we sidestep criticisms from privacy advocates who argue that instituting a central, national identity scheme has a chilling effect on privacy and civil liberties. As an additional privacy safeguard, we maintain the voluntary, opt-in condition of our proposed identity scheme.

Lastly, with regards to concerns about vulnerabilities associated with a national ID system that assigns a single, global identifier to each individual, we use a PKI to circumvent this issue, which will be discussed in more detail in Section 5.x.x.

3.3 e-Estonia

Unlike the U.S., Estonia has the unique benefit of being a country born into today's technology-oriented landscape. Consequently, e-Estonians are able to interact with 600 different government-, health-, and bank-related services in a streamlined and efficient manner through a digital identity system known as e-Estonia. Because of e-Estonia's user-friendliness and robust security safeguards, Estonia has been deemed as one of the most technologically advanced countries in the world.[91] Notably, Estonia has not had a security breach in over a decade.[92]

3.3.1 Front-end security safeguards

Upon enrolling in e-Estonia, the government issues two PIN codes, one for authentication and the other for identification. The authentication code is used only by the user when services need to ensure the user's authenticity. The identification code is used by services to digitally identify the user within its infrastructure. This implementation quite similar to our proposed digital identity verification system described in Section 5, where we discuss the role of public key infrastructure (PKI). To bolster security safeguards, the e-Estonian ID cards utilize certificates that bind the user's private and public keys to each other. These certificates are regularly updated to keep up with the pace of increasing computing power and evolving cryptographic algorithms.[93]

3.3.2 Back-end security safeguards

To integrate e-Estonia with a variety of services, e-Estonia utilizes X-Road, a decentralized, secure data sharing network and blockchain infrastructure. Members of X-Road can be categorized as either data providers, government registries that contain personal data on citizens, or accessors, agencies and companies in the public and private sectors who need access to the data (See Figure

[91] Hammersley, Ben. "Concerned about Brexit? Why Not Become an E-Resident of Estonia." The Wired UK, 2017, http://www.wired.co.uk/article/estonia-e-resident.
[92] "Estonia Takes the Plunge." The Economist, June 2014, https://www.economist.com/news/international/21605923-national-identity-scheme-goes-global-estonia-takes-plunge.
[93] Leetaru, Kalev. "Estonia's ID Card And The March Of Cryptography." Forbes, 2017, https://www.forbes.com/sites/kalevleetaru/2017/09/11/estonias-id-card-and-the-march-of-cryptography/#7e02a36352f4.

2). X-Road is notable for its decentralized, public, and trustworthy management as well as the policy limitations set on accessors' ability to create copies of personal data.

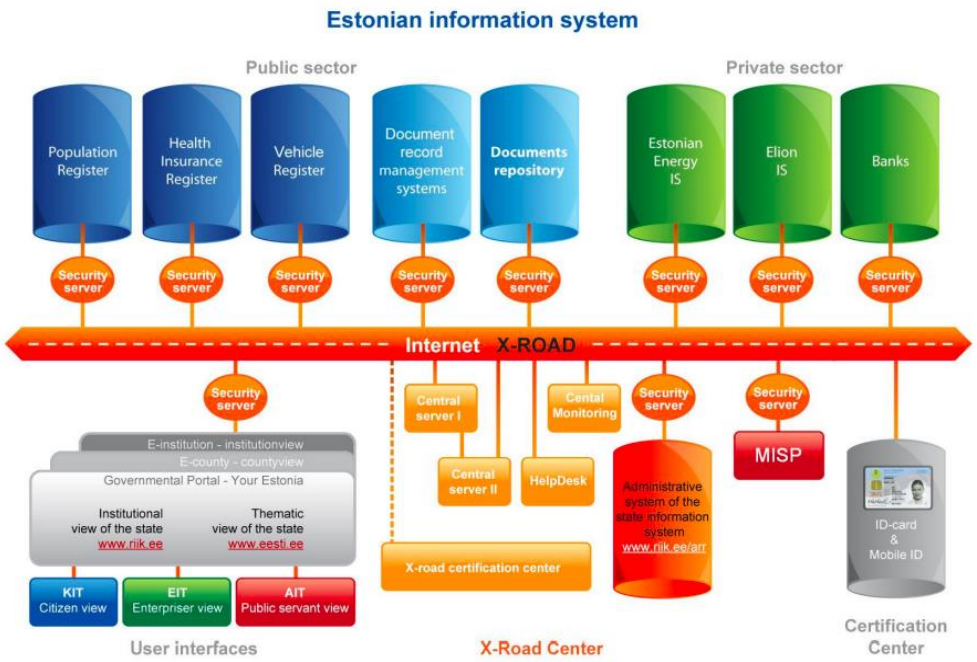


Figure 2. *Architecture of e-Estonia, with X-Road as the secure data-sharing network in the middle.*[94]

X-Road utilizes blockchain technology, which is a public ledger distributed across many computers. In essence, X-Road is a non-repudiation of time-ordered events by a group of distributed servers under the control and viewership of different people. In X-Road, all members, including both data providers and accessors, have their own copy of the ledger. Changes to the ledger are public and broadcast to all participating members. All data exchanges and interactions take place within a brief, predetermined time frame, and are detectable with a unique cryptographic stamp.[95] X-Road's security is strong largely because the identity documents are stored on and authenticated by the distributed ledger, which provides attribution and accountability. Moreover, the public nature of adding new "blocks," or modifications to the ledger, makes it difficult to tamper with past blocks or force a false block to be accepted by the network.

Estonia has also enacted adequate security policies for maintaining X-Road with user trust. Accessors of X-Road are prohibited from maintaining databases that store copies of the personal data they query. Additionally, the RIHA repository promotes transparency in how X-Road operates and who has access to X-Road. It serves the important function of allowing Estonians to see which

[94] Cybernetica AS, "X-Road: e-Government Interoperability Framework", Cybernetica, https://cyber.ee/uploads/2013/03/cyber_xroad_NEW2_A4_web.pdf.
[95] Riigi Infosüsteemi Amet, "How X-Road Works and Participants on X-Road", 2017, https://moodle.ria.ee/mod/book/view.php?id=335&chapterid=150.

officials have viewed their data and file complaints or questions about services or authorities accessing their data, if necessary.[96]

3.3.3 How e-Estonia informs our proposal

e-Estonia is a compelling case study of what a digital identity verification program might look like were it to be instituted on the national scale. The X-Road infrastructure paired with the PKI infrastructure provide adequate protections for both front-and back-end points of security vulnerability as described in the beginning of Section 3.3.

To safeguard against front-end security vulnerabilities, the PKI infrastructure equips each user with two keys, one public, for identification, and the other private, for authentication. This effectively uproots the flawed single, global identifier system in which the same identifier can be used to verify and unlock access to a wide array of services and domains without the consent or knowledge of the user. We use this same implementation in our proposal.

The X-Road infrastructure ensures backend safety. Although the country's personal data is stored in one place, the same concerns do not apply here because of its blockchain infrastructure, which allows decentralized, public, and trustworthy management and maintenance of the data. What is more, accessors of X-Road are prohibited from creating copies of the personal data they access. Although we cannot create a distributed, wide system similar to X-Road for the narrow purpose of safeguarding our digital democracy, we can implement similar policy frameworks that prohibit replication of data stored on databases.

4 Analysis of relevant policy debates

4.1 Maintaining values of free and anonymous speech online

Given the history of anonymous political speech in the United States, we recognize the need to ensure that individuals are able to preserve the ability to have anonymous discourse on social media platforms. This is why our policy proposal only advocates for the voluntary use of the digital identity system for both platforms and individuals users on those platforms. Additionally, we argue that encouraging the verification of U.S. residential status on social media platforms is consistent with U.S. legal doctrine as explained in Section 5.1.1 below. Moreover, for reasons illustrated in Section 5.1.2, our proposal does not compel social media users to use their real or legal names on their public social media profiles if they choose to verify their U.S. residential status on their profiles, thereby enabling anonymous discourse for U.S. residents.

4.1.1 United States legal context

A reasonable counter-argument to our proposal is that it may impede the right of U.S. residents to freedom of speech, anonymous speech, and freedom of association, thereby compromising their

[96] Herlihy, Peter. "'Government as a Data Model' : What I Learned in Estonia." Digital Strategy, GDS Team, GOV.UK, 10–31 2013, https://gds.blog.gov.uk/2013/10/31/government-as-a-data-model-what-i-learned-in-estonia/.

First Amendment rights. While our proposal is only meant to allow U.S. residents to more effectively distinguish between posts made by foreign actors seeking to propagate fake news regarding U.S. affairs and posts made by U.S. residents themselves who have an actual stake in those affairs, it could be argued that asking people to verify that they are U.S. residents on social media platforms could compromise one aspect of their online anonymity.

Free speech proponents frequently rely on McIntyre v. Ohio Elections Commission's[97] rule that the First Amendment protects anonymous political leaflets.[98] Furthermore, Buckley v. American Constitutional Law Foundation[99] extended the protection of anonymous speech by invalidating a law which required that petition circulators wear identification badges. Throughout this line of cases, the U.S. Supreme Court emphasized the important historical role of anonymous literary and political speech and acknowledged the tradition of judicial protection of anonymous political speech.[100]

In McIntyre, the Court held that an Ohio election law's prohibition of the distribution of anonymous campaign literature violated the First Amendment. Mrs. McIntyre distributed leaflets in opposition to a proposed school tax to attendees of a public meeting at a local middle school. These leaflets concluded with the signature "CONCERNED PARENTS AND TAXPAYERS." As a result, the Ohio Elections Commission fined Mrs. McIntyre for violation of the Ohio election law that prohibited distribution of anonymous leaflets. The leaflets did not contain libelous, false, or misleading information; rather, the Commission fined Mrs. McIntyre solely for her violation of the ban on anonymous political leaflets. The Court explained that the choice to remain anonymous might stem from fear of economic or governmental retaliation, concern about social ostracism, or the desire to preserve privacy. The Court reasoned that the contribution of anonymous literary works to the "marketplace of ideas" outweighed any public concern with the speech's source, and thus concluded that the First Amendment protects an author's decision to remain anonymous.

We argue that there is much greater public concern with the source of fake news posts now than there was for speech sources at the time that McIntyre v. Ohio was decided (1995). Additionally, the Internet provides a unique opportunity for speech, including false speech, to reach large audiences, whereby most people can participate in discussions on a wide range of topics unhindered by any editorial content screening and an online speaker has immediate access to a large audience. These qualities increase the potential for harm from false Internet speech, thus, it is important to consider the Internet's unique nature when evaluating the importance of anonymity in the context of fake news postings.

---

[97] 514 U.S. 334 (1995).

[98] See McIntyre v. Ohio Elections Comm'n, 514 U.S. 334,344,347 (1995) (describing challenged speech as speech "intended to influence the electoral process" and "core political speech").

[99] 525 U.S. 182 (1999).

[100] See Mcintyre, 514 U.S. at 342-43 (stating that "even in the field of political rhetoric, where 'the identity of the speaker is an important component of many attempts to persuade,' the most effective advocates have sometimes opted for anonymity" (citing City of Ladue v. Gillco, 512 U.S. 43, 56 (1994)); Talley v. California, 362 U.S. 60, 62, 64 (1960) (noting that "[a]nonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind" and explaining that "persecuted groups ...throughout history have been able to criticize oppressive practices and laws either anonymously or not at all").

Most importantly, there are a number of differences between the situations of McIntyre v. Ohio and today's context of rapid fake news proliferation. A careful examination of both McIntyre's facts and the Court's analysis indicates that it may not be appropriate to uphold the assumption that the case extends to all anonymous Internet speech. The factual and technical distinctions of the case indicate that the Court did not contemplate aspects of speech that include cybersmear or fake news in its assessment of Mrs. McIntyre's speech. Therefore, wholesale application of Mcintyre in the context of fake news would be misapplied.

The first technical difference between Mclntyre and fake news is that the Ohio election law at issue in Mclntyre was a content-based restriction on speech.[101] InMcIntyre, the Court explained that only publications designed to influence voters had to comply with the identity disclosure requirements and accordingly determined that the election law directly regulated the content of speech.[102] The Ohio law required that all political leaflets include identity information, thus forbidding anonymous expression before it took place. Although the McIntyre Court emphasized the value of anonymous speech, it ultimately invalidated the election law because it regulated the content of anonymous, political speech. Thus, citations to McIntyre correctly note the Court's recognition of the value of anonymous speech and that constitutional protection extends to such speech. However, it is an overstatement to declare that McIntyre stands for First Amendment protection of all anonymous speech.

As recognized by the McIntyre Court, anonymity can be abused if used unlawfully.[103] While the Court protected the publishing of truthful or lawful speech, such as Mrs. McIntyre's speech, it did not address fraudulent, libelous, or otherwise unlawful anonymous speech because Mrs. McIntyre's leaflets did not warrant such examination. The Court did not protect nor recognize any value in knowingly false speech.[104] The Court concluded that protecting anonymous political speech is necessary because "anonymous pamphleteering is... an honorable tradition of advocacy and of dissent... [and] a shield from the tyranny of the majority". Intentionally false, unlawful speech does not have a similar redeeming value. Therefore, although the Court emphasized a general respect for the anonymous advocacy of political causes, it did not contemplate anonymous unlawful speech such as social media posts that propagate fake news by foreign actors.

---

[101] See McIntyre v. Ohio Elections Comm'n, 514 U.S. 334,345 (1995) (calling statute "a direct regulation of the content of speech").

[102] See id. ("Every written document covered by the statute must contain 'the name and residence or business address of the chairman, treasurer, or secretary of the organization issuing the same, or the person who issues, makes, or is responsible therefor.' (citing OHIO REV. CODE ANN. § 3599.09(A) (1988))).

[103] See McIntyre, 514 U.S. at 357 ("The right to remain anonymous maybe abused when it shields fraudulent conduct").

[104] See Gertz v. Robert Welch, Inc., 418 U.S. 323, 340 (1974) (stating that "there is no constitutional value in false statements of fact"); N.Y. Times Co. v. Sullivan, 376 U.S. 254,270 (1964) (stating that neither intentional lie nor careless error materially advances society's interest in "uninhibited, robust, and wide open debate on public issues"); Chaplinsky v. New Hampshire, 315 U.S. 568, 572 (1942) (noting that libelous speech is "of such slight social value as a step to truth that any benefit that may be derived from [the speech] is clearly outweighed by the social interest in order and morality").

A prior Supreme Court decision, Talley v. California,[105] extended the freedom to publish anonymously for the advocacy of political causes. In Talley, the Court recognized the historical importance of unpopular groups' anonymous criticism of oppressive regimes. Furthermore, the Court stated that an author might believe that an idea will be more persuasive if delivered anonymously. The McIntyre court explained that although Talley specifically addressed the anonymous advocacy of an economic boycott, it established a general respect for the anonymous advocacy of political causes. Despite this recognition, the Court explained that anonymous speech could be abused if used to shield fraudulent conduct.

In McIntyre v. Ohio, the Court explained that while identity information is no different than other parts of a document's content that an author may choose to exclude, a state's enforcement interest might justify a more limited identification requirement. Justice Ginsburg's concurrence emphasized that the Court left open the possibility for valid state regulation of anonymous speech.[106] Moreover, Justice Scalia, joined by Chief Justice Rehnquist, dissented from the majority opinion. Justice Scalia disputed the existence of a right to anonymous speech so entrenched in the constitutional system that it could not be compromised to protect the integrity of the election process.[107] He concludes that anonymity facilitates wrongdoing because it eliminates the accountability necessary to protect the election process. By leaving open the door for "a more limited identification requirement," the McIntyre Court suggested that the regulation of unlawful speech might justify such a limitation.[108] Although our proposal does not involve direct regulations of Internet speech, this suggestion indicates that McIntyre does not fully extend to anonymous, unlawful speech such as the Internet postings that spread fake news.

For the aforementioned reasons, we conclude that neither the First Amendment nor McIntyre protects the intentionally false speech propagated by fake news postings.[109] Moreover, McIntyre does justify the use of limited identification requirements given the nature of the issue at stake. Since fake news spread by foreign actors and bots can significantly impact the integrity of U.S. elections as illustrated in Section 2, we contend that encouraging the use of verified digital identities by U.S. residents on social media platforms would be in keeping with the U.S. legal tradition.

---

[105] 362 U.S. 60 (1960).

[106] See id. at 358 (Ginsburg, I., concurring) ("We do not thereby hold that the State may not in other, larger circumstances require the speaker to disclose its interest by disclosing its identity.').

[107] See McIntyre, 514 U.S. at 378 (Scalia, J., dissenting) (stating that "the right to anonymity" is not "such a prominent value in our constitutional system that even protection of the electoral process cannot be purchased at its expense," and noting that prior compelled disclosure cases "did not acknowledge any general right to anonymity" but "recognized a right to an exemption from otherwise valid disclosure requirements" if it was reasonably probable "that the compelled disclosure would result in 'threats, harassment, or reprisals from either Government officials or private parties'").

[108] See Mcintyre, 514 U.S. at 353.

[109] See Gertz v. Robert Welch, 418 U.S. 323, 340 (1973) (stating that "there is no constitutional value in false statements offset"); N.Y. Times Co. v. Sullivan, 376 U.S. 254,270 (1964) (stating that "[n]either the intentional lie nor the careless error materially advances society's interest in uninhibited, robust, and wide open debate on public issues"); Chaplinsky v. New Hampshire, 315 U.S. 568, 572 (1942) (noting that libelous speech is "of such slight social value as a step to truth that any benefit that may be derived from [the speech] is clearly outweighed by the social interest in order and morality").

4.1.2 The real name policy controversy

The expectation of using "real names" online did not exist in the early days of web-based socializing when users would choose handles that represented them, and trust was meant to be earned between users, not on the basis of a platform vetting them. While such an anonymous community can act as a breeding ground for harassment and abuse, it was also a means of protection for many users, who relied on an alternative identity in order to participate in their communities.

Facebook's "real name" policy controversy began in late 2014, when a group of drag queens, performers often more well-known by their stage names than their legal names, were locked out of their Facebook accounts after being anonymously reported for not using "authentic names" on the social media site.[110] The issue escalated as people realized that the real name policy unfairly affected abuse survivors, transgender people and political refugees, many of whom often use pseudonyms online to protect themselves from people who might harm them in the real world.[111] This problem is not confined to the U.S.; political dissidents in Egypt, for example, use pseudonyms to spread their message.

Facebook requires users to register with "authentic names" and provide identification if asked, or face being locked out of their accounts. Facebook has maintained that it requires people to use their real names because it prevents anonymized bullying and stops people from hiding behind pseudonyms to "harass, scam, or engage in criminal behavior."[112] The rules for names allowed on Facebook state that "the name on your profile should be the name that your friends call you in everyday life. This name should also appear on an ID or document from our ID list", and "pretending to be anything or anyone isn't allowed."[113] The list of IDs accepted by Facebook for verification include government issued or verifiable IDs such as a birth certificate, driver's license, passport or a social security card.[114] Facebook's founder Mark Zuckerberg has been clear about his stance on individual identity and privacy in the past. In a 2010 interview, he repeatedly emphasized that we all have "one identity," that "having two identities for yourself is an example of a lack of integrity".[115]

Facebook's policy also allows users to report other users registered under alias names and gives Facebook the ability to suspend any accounts where the identity of a user is found to be

[110] Karyne Levy, "Facebook Is Forcing Drag Queens And Other Performers To Use Their Legal Names", Business Insider, Sep. 11, 2014. http://www.businessinsider.com/facebook-drag-queens-real-names-2014-9.

[111] "Facebook's Real Names Policy Threatens Free Expression." Pacific Standard. Accessed November 4, 2017. https://psmag.com/environment/problem-facebooks-shifting-policy-using-legal-names-91723.

[112] Facebook Newsroom, "Community Support FYI: Improving the Names Process on Facebook", December 15, 2015. https://newsroom.fb.com/news/2015/12/community-support-fyi-improving-the-names-process-on-facebook/

[113] Facebook Help Center, "What names are allowed on Facebook?". Accessed October 21, 2017. https://www.facebook.com/help/112146705538576.

[114] Facebook Help Center, "What types of ID does Facebook accept?". Accessed October 21, 2017. https://www.facebook.com/help/159096464162185?helpref=faq_content.

[115] Zimmer, Michael. "Facebook's Zuckerberg: 'Having Two Identities for Yourself Is an Example of a Lack of Integrity' | MichaelZimmer.org." Accessed November 4, 2017. http://www.michaelzimmer.org/2010/05/14/facebooks-zuckerberg-having-two-identities-for-yourself-is-an-example-of-a-lack-of-integrity/.

"fraudulent." This abuse system has been used to silence a broad range of users, from drag queens to Vietnamese pro-democracy activists.[116] The "real name" debate hit a tipping point when gay rights activists said their Facebook accounts were being deactivated as a result of a coordinated campaign by detractors who reported them under Facebook's naming policies. In response, the Nameless Coalition, a collection of civil society organizations and individuals that oppose the real names policy wrote an open letter to Facebook asking the company to, among other demands, commit to allowing pseudonyms and non-legal names on the site in appropriate circumstances.[117]

Facebook, whose profit motive hinges on real names since data attached to other handles is not nearly as valuable, has defended its "real name" policy, arguing that when people are forced to use their real name on the Internet, it adds weight and authenticity to their statements. Other, smaller, social networks like Twitter and Reddit do not require users to identify themselves with their real names. Google+ also reversed its 'real name policy' in 2014 after three years of tough deliberation.[118] When Google Plus launched three years ago, one of the people who signed up was Iranian activist known widely on the Iranian Internet by the pseudonym "Vahid Online." Since Iran is well known to arrest people for their online activity, Vahid had a good reason not to use his real name.[119] When Google announced that pseudonyms would not be allowed, Vahid's account was deactivated along with many others. An outcry ensued—not just from activists in authoritarian countries who are vulnerable to arrest for their online activity, but from a broader set of people who believe fiercely in everyone's right to define and control one's own online identity.

In response, Google adjusted its policy in January 2012, allowing people to use "established pseudonyms" and nicknames if they could provide evidence both of their real identity as well as proof that they had an online identity with a "meaningful following." This allowed Vahid Online to resurface after going through many virtual hoops to prove who he was to Google staff and why his need for a pseudonym was valid. Now, those requirements have been lifted and "there are no more restrictions on what name you can use."[120]

---

[116] Galperin, Eva, and Wafa Ben Hassine. "Changes to Facebook's 'Real Names' Policy Still Don't Fix the Problem." Electronic Frontier Foundation, December 18, 2015. https://www.eff.org/deeplinks/2015/12/changes-facebooks-real-names-policy-still-dont-fix-problem.

[117] "Open Letter to Facebook About Its Real Names Policy." Electronic Frontier Foundation, October 5, 2015. https://www.eff.org/document/open-letter-facebook-about-its-real-names-policy.

[118] MacKinnon, Rebecca, and Hae-in Lim. "Google Plus Finally Gives Up on Its Ineffective, Dangerous Real-Name Policy." *Slate*, July 17, 2014. http://www.slate.com/blogs/future_tense/2014/07/17/google_plus_finally_ditches_its_ineffective_dangerous_real_name_policy.html.

[119] Arash Karami, "Facebook Activists Sentenced to Prison, Lashes in Iran." Al-Monitor, July 14, 2014. http://www.al-monitor.com/pulse/originals/2014/07/iran-facebook-activists-sentenced-prison-lashes.html.

[120] "When We Launched Google+ over Three Years Ago, We Had a Lot of Restrictions O..." Accessed October 21, 2017. https://plus.google.com/+googleplus/posts/V5XkYQYYJqy. Also, see: MacKinnon, Rebecca, Hae-in Lim, and April Glaser. "Google Plus Finally Gives Up on Its Ineffective, Dangerous Real-Name Policy." *Slate*, July 17, 2014. http://www.slate.com/blogs/future_tense/2014/07/17/google_plus_finally_ditches_its_ineffective_dangerous_real_name_policy.html.

In light of the aftermath of the real name policy debate, we recognize that requiring "legal" names on social media could stifle free expression and the ability to communicate online. Since the use of our digital identity verification system is not as a login system and does not enforce that the government-issued digital identity code match the legal name on an official ID, our proposal allows users to choose how they wish to be identified on social media platforms, and feel safe using their preferred identity when speaking online. This is because verifying one's U.S. residential status is entirely separate from a user's profile name. Once social media users see posts from a verified profile, they can trust that it belongs to a U.S. resident regardless of the profile name it displays. By being separate from a login system, our proposal also ensures that the U.S. government has no access to the social media profiles of users who adopt our proposed digital identity verification system, except if the users chooses their postings to be made public. This removes the risk of exceptional government access to social media profiles, and ensures that users can exercise their rights to freedom of expression and anonymous speech.

4.2 Mitigating concerns regarding privacy and government trust

4.2.1 Privacy concerns of an accessible digital verification system

A verification system which is available for private-sector usage carries with it the potential of exposing private information of residents to the private entities available to access it.

This problem is dependant on the design of such a public verification system. If the system can verify names, birthdates, citizenship status, etc., then all of that information is potentially available to be accessed beyond the scope of acceptable usage. For this reason, it is important that the purpose of such a system be narrowly tailored.

Another potential way to circumvent this problem is to regulate the usage of the information exposed by the digital verification system. There is plenty of precedent for the regulated protection of important consumer information by private institutions, such as is the case with "Protected Health Information" of consumers regulated by the Health Insurance Portability and Accountability Act of 1996.[121]

A final way of addressing privacy concerns is to allow optional participation in the digital verification system. In this way, residents can choose whether they would prefer to withhold this information from any potential risk of abuse, at the expense of being unable to participate in the system.

4.2.2 The dangers of over-utilizing the verification system

While each digital ID includes a private key that does not need to be known by the government for the system to work correctly, it is entirely possible for the government to store each private key on issuance without any knowledge on the part of the user. For this reason, the digital ID system must

[121] Secretary, HHS Office of the, and Office for Civil Rights (OCR). "Summary of the HIPAA Privacy Rule." *HHS.gov*, U.S. Department of Health and Human Services, 26 July 2013, www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

stay scoped to issues that the U.S. government already has authority over, i.e. evaluating an individual's identity, authenticating access to public services, etc. It should not be used as a replacement for privately-held credentials of any sort, like account passwords, key cards, or other places that the government does not already have explicit access to.

Although the government needs to generate private keys for all U.S. residents, there is no need for a centralized database for private keys. The private key only needs to be transmitted to the user, after which the user is the only entity in possession of their private key. Any user who loses their private key can ask the government to generate another set of private and public keys for them, which would revoke the old public key associated with the lost private key in order to mitigate the risk of the lost private key being misused by a malicious actor to verify the account of a foreign actor or bot as a "verified" U.S. resident account.

Using digital ID as a form of authentication for any other system would open up that system to potential abuses of government access, which would be a concerning advancement of government power. Failure to make this consideration will potentially impede adoption by anyone who does not trust the government absolutely -- a potentially large number of individuals. If the scope of usage is narrowly tailored, however, then the issue of government trust is only as concerning for users as it is before the adoption of the proposed digital identity system.

5 Our Policy Proposal: A Digital Identity Verification System

5.1 An extensible digital identity for all U.S. residents

To combat the issues presented in the preceding sections, we propose that the United States adopt a robust digital identity verification system to allow for a cryptographically verifiable and secure way to authenticate the identity of U.S. residents on social media platforms using a government-issued digital identification number.

In the same way that the U.S. government currently issues ID cards for most physical, in-person forms of identification, the government could be including in these IDs on-card devices and keys for cryptographic digital identification, similar to the chips present on most modern credit and debit cards, or alternatively just issue a new card or device which has the relevant key.[122] Key to our proposal is the idea that such uses of digital identification are useful to private Internet companies, which is possible if the government hosts a ledger containing public keys for the private keys stored on the ID card or device. These public keys would allow anyone to verify that a given message signed or encrypted with an issued private key is coming from a certain device, but would not allow anyone to create such a message that could impersonate the key-bearer.[123]

---

[122] Groenfeldt, Tom. "More Secure Credit Cards With Chips Coming To The U.S." *Forbes*, Forbes Magazine, 3 July 2014. www.forbes.com/sites/tomgroenfeldt/2014/06/23/more-secure-credit-cards-with-chips-coming-to-the-u-s/#df4e92454906.

[123] "An Introduction to Public Key Cryptography and PGP." *Surveillance Self-Defense*, Electronic Frontier Foundation, 22 May 2017
ssd.eff.org/en/module/introduction-public-key-cryptography-and-pgp

For a newly created digital identity verification system that uses encryption, only the public key of a user would be available to those looking for it, in the same manner that GNU, PGP and bitcoin users make their public keys available without incurring additional privacy or security risks.[124] The private key would thus never need to be transferred to any entity besides the user. Unlike in the case of REAL ID, which tied previously existing identifiers in on database, a new digital identity verification system would involve creating a new set of public and private keys that is not tied to any other personal data of the user and would therefore not compromise the privacy of other existing personal data.

To use the digital identity verification system, a social media company would generate a unique token to be given to the user. The user would take their issued private key, encrypt the token, and then return the encrypted token along with the ID number of their public key. The social media company would take the encrypted token and the ID number, look up the public key associated with that ID number in a ledger of active keys maintained by the government, and then attempt to use that public key to decrypt the token. If the social media can get back the original token using the public key, it means that the token was correctly encrypted with that private key, and as such the person that they are communicating with must be in possession of that private key. Careful choice of tokens will ensure protection against replay attacks and other similar attacks. Thus, our proposal allows private social media companies to easily implement their own identity verification solutions off of a government-backed digital identity verification system by verifying the subset of their users comprising of U.S. residents.

5.2 Features of our proposed digital verification system

5.2.1 The importance of an opt-in system for service providers

While a digital ID system is valuable, it is critical that the use of such a system in private contexts is opt-in by the Internet service provider, rather than mandatory. As explained previously, the authors of this paper fully recognize the value of anonymous speech online, and mandating that service providers accept digital verification of identity will eliminate all social media platforms where verified and unverified accounts are currently on equal footing.

Additionally, an action to mandate integration of a government tech solution would represent a significant change in the relationship between the government and Internet enterprise; one which would stifle the freedom of social media companies to work according to the needs and preferences of their user-base and the market.

5.2.2 Ledger of public keys with privacy protections

The system requires a ledger of active public keys to be available to the social media companies for use. A public ledger of public keys can potentially be a privacy risk, depending on the information

[124] R.C. Merkle, "Protocols for public key cryptosystems," In *Proc. 1980 Symposium on Security and Privacy,,* IEEE Computer Society,, April 1980

linked to the key. If that information is name or SSN, then the full list of the names and SSNs of all U.S. residents could be available to anyone. There are two ways to resolve this issue.

First, the digital ID system could have some means of opting out. This allows for all information to be retained privately, but it forces users to choose between that and utilizing a digital ID. This option, on its own, is not an effective privacy protection as the user should not need to choose between credibility on platforms utilizing the digital ID system and privacy of their personal information.

The other option is that each key could be tied to an ID number and nothing more, such that the ID number is completely unrelated to the person possessing the key. This prevents platforms from verifying information such as legal name, but it does verify residency and retains all privacy of the individual in question. We recommend that both these options be utilized, but especially believe the latter to be an effective solution to this problem, as the ID number is not linkable to any particular individual.

5.2.3 Handling lost keys

In the event of lost keys, which is an inevitability in a system of this scale, there needs to be a process for key revocation, to prevent identity theft and fraudulent verification. This is useful in the case where someone's private key either gets lost, or it gets duplicated by a malicious party.

Luckily, such a key revocation is easily compatible with the public key registry described previously. In the event of a key loss event, the holder of the key simply reports their key stolen to the government, along with a manual verification of their identity to prove that they were the key holder. The government then replaces their private key with a new one, and replaces the public key in the registry with the new public key that matches their new private key. Thus, any attempt to utilize the old, lost private key will fall short as there will be no matching public key available on the registry, and so any verification transaction will be invalid. Meanwhile, the original owner can now take their new private key and proceed to do verification transactions immediately.

5.3 Possible uses

5.3.1 Verification marks

Many social media companies currently implement some form of an "identification" mark, where there is a qualifying icon used to express confidence in some aspect of an account. Twitter[125] and Facebook[126] both currently use a verification icon scheme, where well-known users or businesses can contact the platforms directly to prove their identity and receive a check mark next to their account's name, signifying that their account actually represents the person or business that they claim to.

[125] "About verified accounts", Twitter. https://support.twitter.com/articles/119135
[126] "What is a verified Page or profile?" *Facebook Help Center*, Facebook, www.facebook.com/help/196050490547892

More recently, Facebook started introducing "constituent marks,"[127] which are small icons visible on comments made on politicians profiles or pages signifying that the user making that comment lived in the legislative district for the politician in question. Such a mark, Facebook claims, allows politicians to engage specifically with the people that they are tasked with serving. There is no verification for a user claiming that they live in a politician's district, however, and so this feature is open to potential abuse.

One potential use for our proposed system is for the use of a "U.S. resident" mark, which would accompany the actions of any account that has been verified with a valid digital ID. Such marks would signify to other users whether a user has actual stakes in political speech regarding the U.S. This could also extend to pages, groups, and other types of content distributors in social media, which would deservedly ruin the credibility of pages and groups which claim to be U.S. bodies, but are actually operated by foreign admins. Any multinational organizations would need to have a U.S.-administered online presence (although not exclusively) in order to utilize the mark, a fair and non-stifling restriction.

Such verification mark systems carry heavy credibility implications for users that have the mark. Twitter's marks have been used effectively to combat impersonating accounts and misleading news, and as such do a lot of work towards improving the quality of communications for accounts that are verified.[128] Given that there is an impact on the highest levels, expanding the system to more users without compromising quality would have an even bigger impact in discrediting fake accounts.

Twitter's verification marks have received repeated criticism for being too narrow to the point of being seen as endorsement from the platform for various high-profile figures with views that are not generally accepted by the public, and this is inherent to a verification system that is too difficult to operate at scale.[129] A system grounded in digital ID, which is secure as well as being easy to automatically verify, would effectively combat this problem.

5.3.2 Combating bots

A monumental task that most social media companies face is the policing of "bots," or fake accounts, which are often controlled by software to post large amounts of content and provide an unfair advantage in speech to the owner of those accounts. Bot accounts are often utilized to "astroturf," which is the act of covering pages or posts with a large number of comments, such that the sentiment the botnet expresses seems to be coming from widespread grassroots support.[130] A typical user will see many different individuals expressing a similar sentiment and perceive it to be

[127] "What is a constituent badge?" *Facebook Help Center*, Facebook, www.facebook.com/help/157047021494292

[128] Castillo, Michelle. "Does being verified on Twitter really matter?" *CNBC*, CNBC, 19 May 2015, www.cnbc.com/2015/05/19/does-being-verified-on-twitter-really-matter.html

[129] Wagner, Kurt. "This is why everyone is upset about Twitter's blue check mark verification policy." *Recode*, Recode, 9 Nov. 2017, www.recode.net/2017/11/9/16629796/twitter-halts-verification-white-supremacist-jason-kessler-policy-blue-check-mark.

[130] Bienkov, Adam. "Astroturfing: what is it and why does it matter? | Adam Bienkov." *The Guardian*, Guardian News and Media, 8 Feb. 2012, www.theguardian.com/commentisfree/2012/feb/08/what-is-astroturfing

common, when in reality it is backing the agenda of whatever entity is in control of the botnet impersonating many individuals.

Such schemes present an obvious risk to free and fair discourse on the Internet, by unfairly favoring the opinions of groups willing and able to manipulate these large technical systems. By providing an identification scheme that correctly maps an account to a single resident, a company can rule out all users who have provided digital ID from their set of potential bot accounts, because it is nearly impossible for an attacker to amass so many IDs easily. It is as simple as providing a restriction on the number of accounts which may be tied to any given ID. For most platforms, this bound would likely be one, but any bound which allows for reasonable use but not automated abuse would curb the prevalence and credibility of bot speech impersonating human speech on social media platforms.

5.4 Laying the groundwork for implementation

5.4.1 The role of the government in providing a digital identity verification system

Since the government is the arbiter of who is and is not a U.S. resident, a system that verifies whether someone is or is not a resident should be developed and maintained by the government. Any third-party verification scheme would likely ultimately rely on government-issued documents regardless. Such systems should only be used for tasks which the government is already entrusted with, such as verifying residential status.

Additionally, there are currently not sufficient market incentives for most Internet companies to develop their own verification systems that scale to the size of the U.S., as demonstrated by the fact that most current verification systems are only available to public figures and businesses. Our proposal would be far more cost-effective, due to relying on the government's authority on identity instead of any technical or personal analysis on the part of the company, and result in increased adoption. We believe that any situation in which the market does not provide sufficient incentives to solve major problems warrants government intervention, as in this case where existing privately-driven solutions to the problems presented are not nearly sufficient.

For the reason of limiting potential abuse by a system that migrates from market to government, such a digital identity system should not be used by social media companies to replace privately-held credentials, but only to add additional factors of authentication, in much the same way that many companies currently ask for a user's phone number and will use that channel of communication to verify that the user authenticating is the holder of that phone.

5.4.2 Rough estimates of implementation cost

Our worst-case analysis of a one-time distribution of these ID cards to 100% of the American population is less than 500 million dollars. This rough approximation is based on India's Aadhaar

estimate of $1.50 to distribute and enroll a single user into the program.[131] It is worth noting that the Aadhaar system is considerably larger and far more technically comprehensive than our proposal (on account of collecting various biometric details for each user), and so this estimate represents a high upper bound. The bulk roll-out cost of $500 million is also assuming that every U.S. citizen opts-in to using this system, which again represents an upper bound on the adoption of the system.

Our proposal would cost $500 million as an extreme upper bound, which is approximately 0.01% of the 2018 U.S. federal budget.[132] This can be further remediated by amortizing the roll-out cost to subsets of the population over the course of several budget cycles, and once all of the keys are distributed, the cost scales only with the rate of population growth and key revocation and reissuance.

5.4.3 Adoption of an unprecedented system

There are no current systems, either in the United States or abroad, that really parallel in use and implementation to this system. For this reason, we believe it is extremely difficult or impossible to provide an accurate estimation of how well-utilized this system will be. More research is required to make any claim regarding the population penetration of such a digital verification system. Luckily, that very same research may likely provide evidence to the public that this system is valuable if utilized. And of course, if the population largely does not choose to use this system, then the cost scales appropriately and financial losses are minimized.

6 Conclusion

Our proposal is a legally compliant, secure means by which users can verify their U.S. residential status on social media platforms that choose to adopt the digital identity verification system. It allows social media users to easily distinguish between posts made by "verified" U.S. residents and fake accounts aiming to stir up controversy and propaganda by impersonating U.S. residents. By providing users with more nuanced information about a particular post, our proposal helps them make more informed choices based on the news content they consume on social media platforms. In furthering digital literacy, this proposal removes any reliance on third parties serving as truth arbiters and companies trying to limit information sources through taking down posts and banning certain profiles. This ensures that there are no compromises to the freedom of speech of social media users or to their right to engage in anonymous political speech.

Our proposal also successfully implements the necessary security safeguards that other countries such as India and Estonia have found essential for ensuring user privacy to the greatest extent

[131] For detailed cost analysis of the Aadhaar system, see: World Development Report 2016, Background Paper, "Aadhaar: Digital Inclusion and Public Services in India", Shweta Banerjee Social Protection Team, World Bank Group. http://pubdocs.worldbank.org/en/655801461250682317/WDR16-BP-Aadhaar-Paper-Banerjee.pdf.

[132] Amadeo, Kimberly. "Secrets of the Federal Budget Revealed." The Balance. Accessed December 10, 2017. https://www.thebalance.com/u-s-federal-budget-breakdown-3305789.

possible. We use public key infrastructure (PKI), which ensures that user verification is a truly bona fide and private process, and a national registry that does not link user keys to personally identifying information on the back-end. Moreover, we include design caveats for protocols for many common use cases and problems, from the potential utilization of a token-based scheme for verification, which is one of many possible ways allowing social media companies to leverage the power of key-pair cryptography, to an approach for mitigating and resolving ID loss and fraud. By offering a secure and effective means of verifying an aspect of the digital identities of U.S. residents, our proposal allows for maintaining the integrity of socio-political discourse on online platforms by tackling the widespread and dire problem of fake news being propagated by foreign actors with political incentives to misinform U.S. residents.

7 Contributions

Section 1: All
Section 2: Wajeeha
Section 3: Sharon, Section 3.1.2: Wajeeha, Section 3.1.3: Sharon
Section 4.1: Wajeeha, Section 4.2: Ryan
Section 5: Ryan, Section 5.4.2: Sharon & Ryan
Section 6: All