

NIP THE BOTS IN THE BUD: PROACTIVELY TAKING DOWN AND PREVENTING THE CREATION OF INAUTHENTIC SOCIAL MEDIA ENTITIES

BY MAX LESSER, SOPHIE MCDOWALL, AND CAT SMITH

OCTOBER 10, 2024

A years-long Chinese influence operation known as Spamouflage has persisted on social media despite numerous attempts by various platforms to remove it.¹ The operation's endurance can be explained to a considerable extent by its exploitation of vast networks of pre-positioned, inauthentic social media entities lying ready for Spamouflage and other malicious actors to deploy.²

The Foundation for Defense of Democracies (FDD) has uncovered more than 25,000 inauthentic Facebook pages with names identical or similar to previously identified Spamouflage entities. While these pages do not appear to be currently engaged in influence operations, several are conducting ongoing financial scams. Taking down these pages (and other similar networks) would not only help to restrain state-backed influence operations like Spamouflage but also to thwart other malicious activity on social media platforms.

Meta and other major social media companies must significantly strengthen identity verification to make it more difficult to create networks of inauthentic entities on social media platforms in the first place. Platforms should implement solutions that preserve privacy while verifying the identity of persons creating new entities.

By nipping the bots in the bud, the community of stakeholders seeking to combat foreign influence operations, scams, and other forms of malicious online activity can move beyond playing whack-a-mole and instead get one step ahead of adversaries.

HOW DID FDD DISCOVER 25,000 INAUTHENTIC PAGES?

FDD previously uncovered 450 Spamouflage entities (i.e., profiles and pages) on Facebook in a network we named the 'War of Somethings.'³ FDD exposed this network in March 2024 and reported it to Meta before publishing its findings. After FDD shared this network with Meta, Meta purged 162 of the 450 Spamouflage entities. 'Entities' is a general term that Meta uses in its own policies referring to social media pages, user profiles, groups, and events.

1. Max Lesser, Ari Ben Am, Margot Fulde-Hardy, Paul J. Malcomb, and Saman Nazari, "Much Ado About 'Somethings,'" *Foundation for Defense of Democracies*, March 27, 2024. (<https://www.fdd.org/analysis/2024/03/27/much-ado-about-somethings>)

2. FDD uses the term "social media entity" as it broadly refers to pages, profiles, groups, and events. Meta uses this term in its own policies. See: "Account Integrity and Authentic Identity," *Meta*, accessed June 9, 2024. (<https://transparency.meta.com/policies/community-standards/account-integrity-and-authentic-identity>)

3. Max Lesser, Ari Ben Am, Margot Fulde-Hardy, Paul J. Malcomb, and Saman Nazari, "Much Ado About 'Somethings,'" *Foundation for Defense of Democracies*, March 27, 2024. (<https://www.fdd.org/analysis/2024/03/27/much-ado-about-somethings>)

The operators of the ‘War of Somethings’ network used fabricated personas and hacked accounts to draw attention to perceived U.S. domestic policy failures ranging from gun violence to drug deaths. The network also criticized U.S. foreign policy, with a particular focus on the Israel-Hamas war, and discussed the 2024 U.S. elections.

Even after Meta took down some of the FDD-reported entities, searches on Facebook for pages with identical names revealed thousands of entities with either identical names or permutations of the original names.⁴

Take, for example, the Facebook profile “Denise Jones.” When researching the ‘War of Somethings’ network, FDD observed “Denise Jones” sharing both English-language content highly critical of the U.S. government and Chinese-language content promoting China with hashtags such as #AmazingBeijing. Based on a variety of distinctive behaviors exhibited by this profile — such as posting largely during Chinese working hours and sharing content almost exclusively from entities associated with Spamouflage — FDD assessed with high confidence that “Denise Jones” was part of a Spamouflage campaign.

A later search by FDD for the name “Denise Jones” generated results that included more than 124 inauthentic pages, all of which were either named “Denise Jones” or included “Denise Jones” in their name. In some cases, the indicator of artificiality was an AI-generated profile photo, as indicated by the presence of surreal images on or around the face. (See Figures 1-2.)⁵ Other cases involved incongruities among the page’s name, photos, description, and behavior. For example, one page named “Denise Jones (Houston)” lists itself as an advertising agency in Houston but uses a sexually suggestive profile photo and primarily shares Vietnamese-language content.⁶



Figures 1-2: AI-generated profile photos for “Denise Jones Online 92061” and “Denise Jones Online 62938”

.....
4. FDD did not conduct a similar search for Facebook profiles because it is more difficult to determine the authenticity of Facebook profiles given that many keep their information private.

5. Denise Jones Online 92061, Facebook, accessed June 4, 2024. (<https://www.facebook.com/profile.php?id=61556228647825>); Denise Jones Online 62938, Facebook, accessed June 4, 2024. (<https://www.facebook.com/profile.php?id=61553686616061>); Denise Jones Online 90082, Facebook, accessed June 4, 2024. (<https://www.facebook.com/profile.php?id=61554188497306>); Denise Jones Online 47832, Facebook, accessed June 4, 2024. (<https://www.facebook.com/profile.php?id=61550806996943>)

6. Denise Jones (Houston), Facebook, accessed July 15, 2024. (Archived version available at <https://ghostarchive.org/archive/ys4Vq>)

Patterns across groups of pages strongly suggested someone created the accounts in batches. Of the 124 inauthentic “Denise Jones” pages, 19 shared the name “Denise Jones Online” followed by a five-digit number. (See Figure 3.) Many “Denise Jones” pages also included identical page descriptions. For example, 18 of them use the tagline “Hi there, want more beer?” in their description.

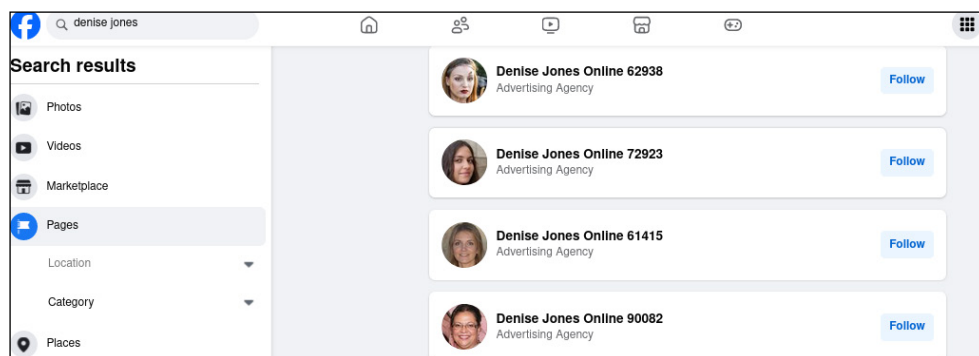


Figure 3: A small sample of fake pages surfaced by entering “Denise Jones” into the search bar for Facebook pages.

To find other inauthentic pages, FDD conducted searches on Facebook for the names of entities previously identified as part of Spamouflage operations not only by FDD but also by the BBC, Graphika, the Australian Strategic Policy Institute, Mandiant, and Microsoft.⁷

With this process, FDD identified 212 Spamouflage entities with associated groups of inauthentic pages. These entities are listed in Appendix A.⁸

After identifying these 212 entities, FDD pulled Facebook page search results associated with each entity. This process identified 50,000 Facebook pages in total, including both authentic and inauthentic pages. Looking for telltale indicators of inauthenticity, FDD identified over 25,000 inauthentic pages with names identical or similar to previously identified Spamouflage entities. Appendix B includes a selection of 22 potential indicators of inauthenticity to illustrate what attributes FDD used to determine a page’s status.

7. Max Lesser, Ari Ben Am, Margot Fulde-Hardy, Paul J. Malcomb, and Saman Nazari, “Much Ado About ‘Somethings,’” *Foundation for Defense of Democracies*, March 27, 2024. (<https://www.fdd.org/analysis/2024/03/27/much-ado-about-somethings>); Benjamin Strick, Olga Robinson, and Shayan Sardarizadeh, “Coronavirus: Inside the pro-China network targeting the US, Hong Kong and an exiled tycoon,” *BBC (UK)*, May 27, 2020. (<https://www.bbc.com/news/blogs-trending-52657434>); Ben Nimmo, C. Shawn Eib, and L. Tamora, “Cross-Platform Spam Network Targeted Hong Kong Protests ‘Spamouflage Dragon’ used hijacked and fake accounts to amplify video content,” *Graphika*, September 25, 2019. (https://public-assets.graphika.com/reports/graphika_report_spamouflage.pdf); Albert Zhang, Tilla Hoja, and Jasmine Latimore, “The CCP’s increasingly sophisticated cyber-enabled influence operations,” *The Australian Strategic Policy Institute*, April 2023. (<https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2023-05/Gaming%20public%20opinion.pdf?VersionId=QYkBIWncbBU0E1KAhg9mX3TD7kwlWcWj>); Ben Nimmo, Camille François, C. Shawn Eib, and Léa Ronzaud, “Spamouflage Goes to America,” *Graphika*, August 12, 2020. (https://public-assets.graphika.com/reports/graphika_report_spamouflage_goes_to_america.pdf); Ben Nimmo, Ira Hubert, and Yang Cheng, “Spamouflage Breakout,” *Graphika*, February 4, 2021. (https://public-assets.graphika.com/reports/graphika_report_spamouflage_breakout.pdf); Nick Monaco, “Five Ways to Spot a Spamouflage Disinformation Campaign,” *Microsoft Threat Analysis Center*, December 22, 2021. (<https://miburo.substack.com/p/five-ways-to-spot-spamouflage>); Nick Monaco, “Emperor in the Ether: Spamouflage’s Authoritarian Attacks on Democracy and Journalists,” *Microsoft Threat Analysis Center*, December 22, 2021. (<https://miburo.substack.com/p/emperor-in-the-ether>); “Pro-PRC DRAGONBRIDGE Influence Campaign Targets Rare Earths Mining Companies in Attempt to Thwart Rivalry to PRC Market Dominance,” *Mandiant Threat Intelligence*, June 28, 2022. (<https://www.mandiant.com/resources/blog/dragonbridge-targets-rare-earths-mining-companies>)

8. FDD’s own study into the ‘War of Somethings’ network drew from internal data referenced in the report “Much Ado About Somethings.” However, not all the accounts we identified in our internal data were specifically named in the report “Much Ado About Somethings.”

WHAT ARE THESE 25,000 PAGES DOING?

None of the 25,000 inauthentic pages that FDD identified appears to be currently engaged in influence operations. Many of these pages, in fact, appear not to be engaged in any activity at all.

FDD did, however, identify several pages promoting financial scams. For example, one page named “Agent James Smith” claimed to be distributing up to \$7 million in gifts and donations on behalf of FedEx. (See Figure 4.) The page posted photos of FedEx trucks and people receiving jumbo checks from Publishers Clearing House sweepstakes.⁹ Pages named “AGENT SMITH JAMES,” “Agent Peggy Ashley Wilson,” “AGENT JANE ALICE,” and others promoted similar scams.¹⁰

This scam activity suggests that whoever created these vast networks of inauthentic pages did not do so expressly for influence operations. Rather, the operators of Spamouflage likely purchased or appropriated pages from these networks to save the effort of creating their own.



Figure 4: A financial scam promoted by “Agent James Smith”

9. Agent James Smith, *Facebook*, accessed May 19, 2024. (Archived version available at <https://ghostarchive.org/archive/J9IOi>)

10. AGENT SMITH JAMES, *Facebook*, accessed May 19, 2024. (Archived version available at <https://ghostarchive.org/archive/9K2xB>); Agent Peggy Ashley Wilson, *Facebook*, accessed May 19, 2024. (Archived version available at <https://ghostarchive.org/archive/HR5p6>); AGENT JANE ALICE, *Facebook*, accessed May 19, 2024. (Archived version available at <https://ghostarchive.org/archive/HdBSj>)

WHO CREATED THESE PAGES AND HOW?

Many of the 25,000 inauthentic pages display consistencies in naming conventions, page descriptions, and images. For example, the search results for more than 87 of the 212 distinct Spamouflage-related entities included at least one result with the tagline “Hi there, want more beer?” in the page’s description. Thus, in addition to being connected to previously identified Spamouflage accounts, many of the 25,000 inauthentic pages appear to be connected to each other because of their shared features.

Other common features that extended across the inauthentic pages include taglines such as “Vinicius Junior” and “Hello World.” Several pages also include the word “Agent” affixed before the page’s name, often with a photo of a government official as a profile image. Another pattern involves 15-digit numerical strings appended to the end of the page’s name, and another includes exactly four random emojis in the page’s description. Appendix B outlines these patterns and others in more detail.

These patterns demonstrate that whoever created these pages used automation, likely involving tools provided by the black hat marketing website Fewfeed.¹¹ (‘Black hat’ is a term for deceptive and/or manipulative approaches to marketing.¹²) The connection to Fewfeed was plainly visible thanks to page descriptions that read “This page was generated by fewfeed v2” alongside four random emojis.

Fewfeed has a tool that allows users to automatically create Facebook pages with identical descriptions and assign up to 500 random names to these pages.¹³ The tool has a default setting to create pages with the description “This page was generated by fewfeed v2.” It also provides the option to add random emojis at the end of the page description. The tool could also have created other observed clusters of pages with identical descriptions, of which several have random strings of emojis added to them. (See Appendix B).

From the available evidence, one cannot know whether Spamouflage operators used tools like Fewfeed’s automatic page generator, or whether Spamouflage purchased the pages from a separate creator. Indeed, black hat marketers regularly advertise Facebook entities for sale on messaging apps such as Telegram and in fora such as Blackhatworld[.]com.¹⁴ (See Figures 6 and 7.) The ability of Spamouflage’s operators to purchase pre-positioned inauthentic entities may explain the operation’s persistence despite multiple takedowns by Facebook and other social media platforms.¹⁵

11. “Fewfeed,” *Internet Archive*, accessed July 3, 2024. (<https://web.archive.org/web/20240703161318/https://v2.fewfeed.com>)

12. Marketing School, “Black Hat Marketing Internet Marketing Using Unethical Means,” *Marketing School*, November 14, 2020. (<https://www.marketing-schools.org/types-of-marketing/black-hat-marketing>)

13. “Auto Create Business Multiple Pages,” *FewfeeD v2*, accessed July 3, 2024. (Archived version available at <https://web.archive.org/web/20240703153126/https://v2.fewfeed.com/tool/create-bm-pages>)

14. “Telemetry,” *Telemetry*, accessed June 4, 2024. (<https://www.telemetryapp.io>); Selling Bulk Facebook Accounts, *BlackHatWorld*, accessed June 4, 2024. (Archived version available at <https://web.archive.org/web/20240523155736>)

15. Vera Bergengruen, “Meta Takes Down ‘Largest Ever’ Chinese Influence Operation,” *Time*, August 31, 2023. (<https://time.com/6310040/chinese-influence-operation-meta>); Sam Sabin, “Meta Takes Down Largest Online Influence Network in History,” *Axios*, August 30, 2023. (<https://www.axios.com/2023/08/30/meta-largest-influence-network-china>); AJ Vicens, “Meta: Pro-Chinese Influence Operation Was the Largest in History,” *CyberScoop*, August 29, 2023. (<https://cyberscoop.com/meta-china-influence-operation-facebook>)

Purchasing entities from a third party saves time since building new pages would require creating unique emails and solving CAPTCHA puzzles, which seek to deter automated bots from creating entities by generating challenges that, ideally, humans but not computers can pass.¹⁶ Purchasing entities from a third party may also save money since it may eliminate the need to procure phones and SIM cards. Though Facebook usually requires only an email address to create an account, Spamouflage’s operators may need phone numbers to set up or verify email accounts, depending on the email service.

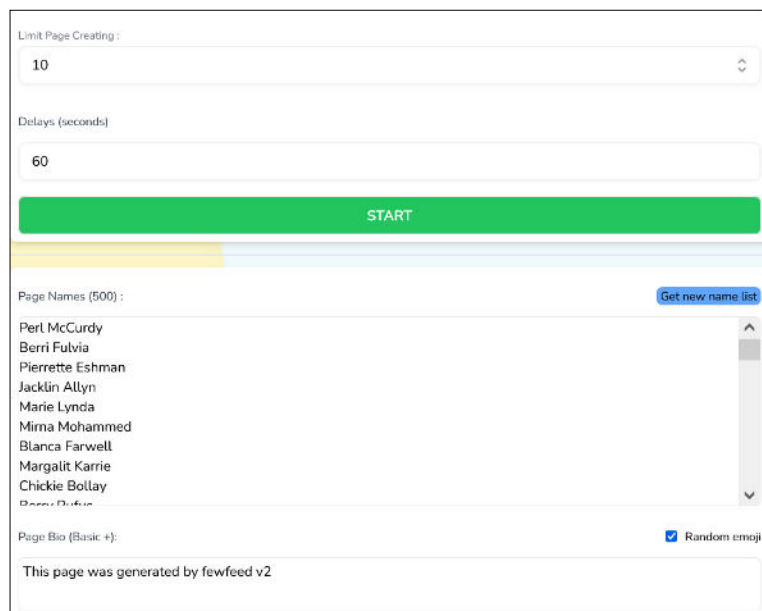


Figure 5: A screenshot of the Fewfeed v2 tool titled ‘Auto Create Business Multiple Pages’

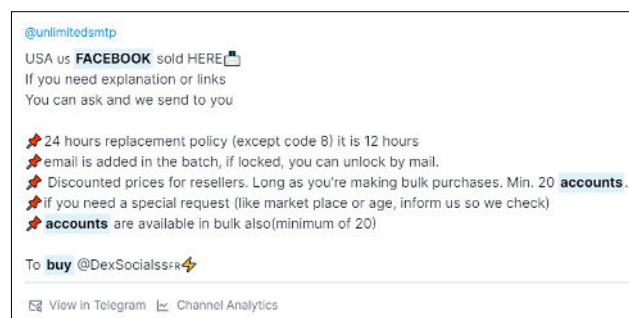


Figure 6: Telegram message advertising Facebook accounts for sale, identified using Telemetry Data Labs

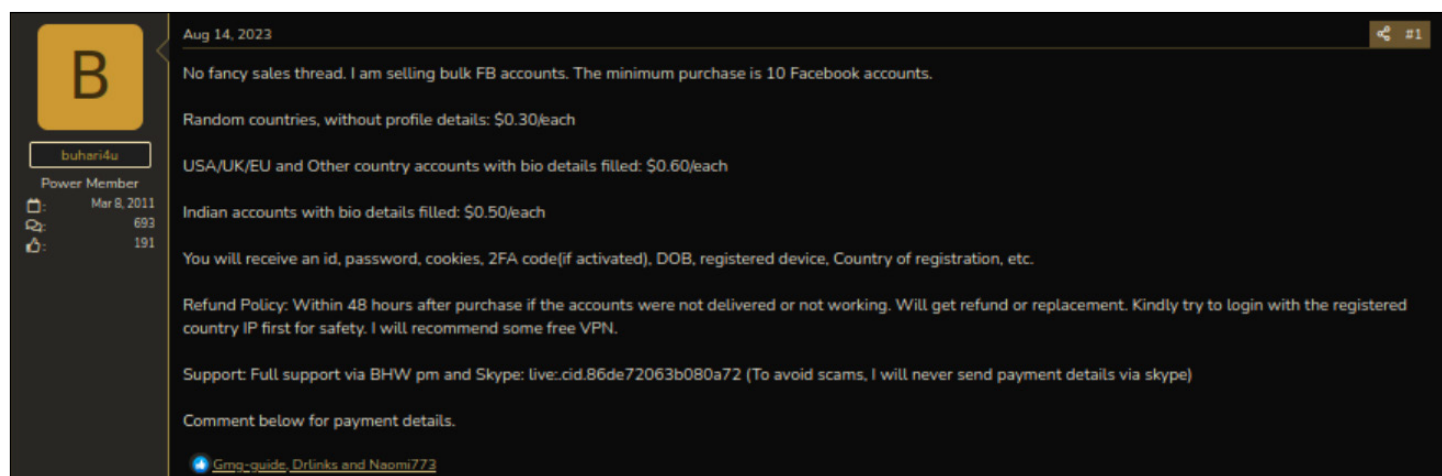


Figure 7: Forum post advertising Facebook accounts for sale on Blackhatworld[.]com

16. CAPTCHA: Telling Humans and Computers Apart Automatically,” CAPTCHA, accessed June 10, 2024. (<http://www.captcha.net>)

RECOMMENDATIONS: ENHANCE TAKEDOWNS AND PREVENT THE CREATION OF INAUTHENTIC ENTITIES

Meta reports that it detects and removes over a billion fake entities each quarter, relying on a combination of technology and human review teams with more than 15,000 contractors.¹⁷ While this effort is laudable, there are still vast quantities of fake entities that enable influence operations, scams, and other illicit activity on Facebook. Meta can do more.

This investigation focuses exclusively on Facebook. That said, Facebook is not unique in the way that state actors are exploiting it.¹⁸ Other social media companies should also take similar action to protect the integrity of their platforms.

1. Strengthen identity verification for account creation while preserving privacy.

Meta currently requires a phone number or email to create an account. Malicious actors can meet these requirements by acquiring fresh phone numbers or emails. For example, they can purchase a prepaid SIM card at a gas station or simply create a new email address. Meta also sometimes requires current users or users trying to create an account to provide a so-called “video selfie” to verify their identity.¹⁹ It is unclear what conditions trigger this requirement.

Requiring a video selfie may feel overly invasive to Facebook users. Moreover, malicious actors may be able to bypass video selfie requirements with AI face swap tools or AI tools that generate videos from still images of faces.

Meta and other social media companies must accordingly strike a balance between verification and privacy. Accordingly, social media companies should explore solutions such as zero-knowledge proofs for identity, which enable people to prove their knowledge about certain information without disclosing the information itself. In the case of identity verification, people could use zero-knowledge proofs to verify aspects of their identity (e.g., citizenship, age, etc.) without disclosing it.

Blockchain technology can also help. Early cryptocurrency researchers focused on blockchain applications for information security.²⁰ A blockchain-based account verification solution for social media could disincentivize undesirable behavior, such as the mass creation of inauthentic identities, by imposing a cost or by creating a reward for alternative behaviors.

17. “Inauthentic Behavior,” *Meta*, accessed June 4, 2024. (<https://transparency.meta.com/policies/community-standards/inauthentic-behavior>); “The People Behind Meta’s Review Teams,” *Meta*, accessed June 4, 2024. (<https://transparency.meta.com/en-gb/enforcement/detecting-violations/people-behind-our-review-teams>)

18. For example, in August 2023, analysts at Meta observed the Chinese influence operation Spamouflage operating across at least 50 platforms in addition to Meta’s own platforms. These additional platforms included YouTube, Reddit, Pinterest, TikTok, Pinterest, Medium, and X. See: Vera Bergengruen, “Meta Takes Down ‘Largest Ever’ Chinese Influence Operation,” *Time*, August 31, 2023. (<https://time.com/6310040/chinese-influence-operation-meta>)

19. “What is video selfie verification on Facebook?” *Meta*, accessed July 11, 2024. (Archived version available at <https://web.archive.org/web/20240711191600/https://en-gb.facebook.com/help/875662883106240>)

20. Adam Back, “HashCash - A Denial of Service Counter-Measure,” *HashCash*, August 1, 2002. (<http://www.hashcash.org/papers/hashcash.pdf>)

2. Assess existing enforcement measures and monitor the market for inauthentic entities.

The 25,000 fake entities that FDD discovered clearly violate Meta’s Account Integrity and Authentic Identity policies, which Meta extends beyond user accounts to “other entities (such as pages groups and events).”²¹ The persistence of the networks identified by FDD indicates that there are gaps in Meta’s policy enforcement.

It is possible, for example, that Facebook did not detect the 25,000 entities because they engaged in very limited activity. Meta’s reporting on its enforcement actions specifies that Meta removes pages “if the name, description or cover photo of a Page or group violates our Community Standards.”²² This means that Meta should remove inauthentic pages — even those that have not yet posted any content — based on the page name and description alone.

To address these gaps in enforcement, Meta and other social media companies should undertake regular red team exercises in which the red team creates networks of inauthentic entities to gauge how long it takes social media companies to identify and respond to them. When inauthentic entities go undetected for a long period of time, the red team can report this gap in enforcement.

Red teams can also test the strength of social media companies’ identity verification and account creation processes. For example, red teams can attempt to create accounts using various email service providers to determine which providers have safeguards that prevent new or little-used email accounts from creating social media entities. Red teams can uncover which email service providers prevent this abuse and which do not so that social media companies can apply further scrutiny to accounts created using addresses from high-risk email service providers.

In addition to conducting red team exercises, social media companies should adopt proactive threat intelligence practices to help prevent the creation of inauthentic entities. In the field of cybersecurity, certain threat intelligence communities infiltrate hacker fora and procure services to gain proactive intelligence. The NATO Strategic Communications Center of Excellence (NATO STRATCOM) has performed similar work in the social media realm. For a series of studies, NATO purchased inauthentic interactions from commercial media manipulation service providers. These studies measured the amplification of benign content on a small scale to reveal weaknesses in social media companies’ ability to detect and respond to platform manipulation.²³

Social media companies can produce proactive threat intelligence by infiltrating and monitoring black hat marketing fora. Social media companies can even anonymously pay for services to observe the behavior of threat actors. As demonstrated in this paper, the same assets can be and are often used to fuel a wide array of malicious social media activity — be it financial scams or influence operations. Understanding more about how people create, sell, and use these assets will help social media companies detect and prevent this wide range of malicious social media activity.

21. “Account Integrity and Authentic Identity,” *Meta*, accessed June 4, 2024. (<https://transparency.meta.com/policies/community-standards/account-integrity-and-authentic-identity>)

22. “Removing Pages and groups,” *Meta*, October 4, 2022. (<https://transparency.meta.com/en-gb/enforcement/taking-action/removing-pages-groups>)

23. Rolf Fredheim, Sebastian Bay, Anton Dek, Martha Stolze, and Tetiana Haiduchyk, “Social Media Manipulation 2022/2023: Assessing the Ability of Social Media Companies to Combat Platform Manipulation,” *NATO Strategic Communications Centre Of Excellence*, March 3, 2023. (<https://stratcomcoe.org/publications/social-media-manipulation-20222023-assessing-the-ability-of-social-media-companies-to-combat-platform-manipulation/272>); Sebastian Bay, Rolf Fredheim, Tetiana Haiduchyk, and Anton Dek, “Social Media Manipulation 2021/2022: Assessing The Ability Of Social Media Companies To Combat Platform Manipulation,” *NATO Strategic Communications Centre Of Excellence*, April 2022. (https://stratcomcoe.org/pdfs/?file=/publications/download/20220429_Social_media_manipulation-FOR-WEB.pdf?zoom=page-fit)

3. Host “clean up” events where independent researchers actively search for inauthentic entities. Share intelligence with other platforms.

To supplement ongoing takedowns of inauthentic entities, social media companies should host regular events where independent researchers and non-profits can actively search for inauthentic entities as a form of public service. Social media companies should ensure these researchers have access to the data necessary to identify as many entities as quickly and easily as possible.

Malicious networks can also operate across online platforms, be they mainstream social media platforms such as Facebook and X, media-sharing platforms such as YouTube, discussion platforms such as Reddit, or others. For example, researchers have documented various Spamouflage networks operating across over 50 online platforms.²⁴ Therefore, social media companies should also expand partnerships with each other to help them better combat cross-platform networks of malicious online activity.

CONCLUSION

By undertaking these recommendations, Meta and other social media platforms can proactively take down and prevent the creation of inauthentic entities in a more effective and efficient fashion. This will make it more difficult for U.S. adversaries to launch influence operations on social media platforms in the first place. Going after the underlying ‘infrastructure of influence’ on social media — be it networks of pre-created inauthentic entities, or the black hat marketing tools and platform policy loopholes that enable malicious actors to create them en masse — will certainly help stem the tide of the seemingly constant stream of malign influence targeting the United States and its allies.

24. Margi Murphy, “Spamouflage Dragon Infiltrates Internet With Clumsy Pro-China, Anti-West Messages,” *Bloomberg*, December 15, 2023. (<https://www.bloomberg.com/news/articles/2023-12-15/pro-chinese-spamouflage-dragon-has-penetrated-social-media>)

APPENDIX A: PREVIOUSLY IDENTIFIED SPAMOUFLAGE ENTITIES

The list below presents Spamouflage entities previously identified by FDD or other researchers, specifically, those that had associated groups of inauthentic entities.

Entities identified as part of the “War of Somethings” network discovered by FDD²⁵

- Isobel Caldwell
- Amelia Murray
- Grace Fisher
- Martha Coles
- Phoebe Smith
- Emily Walsh
- Jared Dolan
- Cecil Walsh
- Heather Robinson
- Sara Jones
- Callie Austin
- Jim Davies
- Raj Shope
- Isabella Fraser
- Santosh Kumar
- Lakshman Kumar
- Janice Collings
- Jibon Shathi
- Zach Simpson
- Lacey Anderson
- Jennifer Johnson
- Dustu Chele
- Tyler Tara
- Claretta Whittaker
- Agus Tina
- Denise Jones
- Merrie
- Erix Boy
- Nakata
- Astri
- Jim Davies
- Sergey Ponomarev
- Amber Jennings
- Juana Gutierrez
- Sabrina Brewer
- Ekaterina Nikitina
- Angie King
- Shashi Kanth
- Dwayne Bartholemew
- Selina Chris
- Antonio Holcombe
- Vickie Frazier
- Brendan Askew
- Chan Emma
- Diana Lin
- Yu Ting Gao
- Ranjan Mandal
- Emily Walsh
- Sara Jones
- Callie Austin
- Emely Ellison
- Eve Parry
- Meghan Bailey
- Lorena Braz Paiva
- Sophia Evan
- Andrea Acosta

25. Max Lesser, Ari Ben Am, Margot Fulde-Hardy, Paul J. Malcomb, and Saman Nazari, “Much Ado About ‘Somethings,” *Foundation for Defense of Democracies*, March 27, 2024. (<https://www.fdd.org/analysis/2024/03/27/much-ado-about-somethings>)

- Elane Shay
- Phoebe Smith
- Richard Kyle
- Aulia Jr.
- Shaun Reece
- Felipe Teixeira
- Todd Chen
- Lauran Bosley
- Mary Joesy
- Md Asadul
- Kate Kane
- Ryan Jai Secend Jai
- Jose Avery
- Montgomery Sandy
- Rita Roy
- Patricia Lin
- Lauren Moulton
- Emery Miller
- Santos Abraham
- Susan Byrne
- Jeffrey Mendez
- Doreen Buchanan
- Derek Frye
- Tracie Bowden
- Donald Rosales
- Kim Nixon
- Anthony Duffy
- Emanuel Kohler
- Stefan Valdes
- Jan Hampton
- Donovan Schultz
- Marth Robledo

- Giovanni Barth
- Dennise Sheppard
- Jensen Smith
- Minh Triết
- Chandudas Chandudas
- Christina Lopez
- Margurite Ortega
- Jennie Kennedy
- Lee Sorensen
- Alica Ellis
- Kim Jack
- Christoper Grier
- Marco Davila
- Henry Lyle
- Leticia Madsen
- Kelly Ferrari
- Guillermo Davis
- Maryln Walters
- Bryant Beard
- Maximo Gentry
- Reginia Tavares
- Morgan Dees
- Morosos Escuintila
- Julio Foley
- Eve Bateman

Entities identified as part of BBC reporting²⁶

- Logan Lee
- Merle Thompson
- Elena Johnson
- Md Joy Jr.

26. Benjamin Strick, Olga Robinson, and Shayan Sardarizadeh, “Coronavirus: Inside the pro-China network targeting the US, Hong Kong and an exiled tycoon,” *BBC* (UK), May 27, 2020. (<https://www.bbc.com/news/blogs-trending-52657434>)

Entities identified as part of Graphika reports²⁷

- Michael Welsh
- Lida Wong
- Helena Hart
- Regina Montgomery
- Malcolm Daly
- Yiyi Chen
- Li Sandy
- Peng Lei
- Dali Le
- Polina Novikova
- Oksana Rodionova
- Irina Ivanova
- Nhu Vu
- Tuong Cuc
- Kay Payne
- Alicia Carpenter
- Jean Miles
- Lois Peters
- Sandra Barnes
- Mae Murray
- Jessica Harvey
- He Jingrun
- Francis W
- Victor Chan
- Spencer Taggart
- Charles Carter
- Robert Collins
- Isaac Jones
- Daniel Evans

- Christopher Garcia
- Richard Turner
- Joseph Williams
- Steven Turner
- Kyler Lewis
- Kimberly Miller
- Anna Conner
- Kelly Bell
- Paula Smith
- Hannah Marie
- Angie Evans

Entities identified by the Australian Strategic Policy Institute²⁸

- Mike Ahmed
- Lori Gutierrez
- Yui Aragaki
- Renea
- Nora Gonzalez
- Jeanette Torres
- Jackie Garcia
- Sonya Bell

27. Ben Nimmo, C. Shawn Eib, and L. Tamora, “Cross-Platform Spam Network Targeted Hong Kong Protests ‘Spamouflage Dragon’ used hijacked and fake accounts to amplify video content,” *Graphika*, September 25, 2019. (https://public-assets.graphika.com/reports/graphika_report_spamouflage.pdf); Camille François, C. Shawn Eib, and Léa Ronzaud, “Spamouflage Goes to America,” *Graphika*, August 12, 2020. (https://public-assets.graphika.com/reports/graphika_report_spamouflage_goes_to_america.pdf); Ira Hubert and Yang Cheng, “Spamouflage Breakout,” *Graphika*, February 4, 2021. (https://public-assets.graphika.com/reports/graphika_report_spamouflage_breakout.pdf)

28. Albert Zhang, Tilla Hoja, and Jasmine Latimore, “The CCP’s increasingly sophisticated cyber-enabled influence operations,” *The Australian Strategic Policy Institute*, April 2023. (<https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2023-05/Gaming%20public%20opinion.pdf?VersionId=QYkBIWncbBU0E1KAhg9mX3TD7kwIWcWj>)

Entities identified by Microsoft Threat Analysis Center²⁹

- James Maddison
- Carla Walker
- Donald Marshall
- Brett Ferguson
- Anthony Robert
- Jiang Peter
- Peter Douglas
- Nick Wells
- Fred Valerie
- Edward Allen
- George Gonzalez
- Steven Baker
- Robert Hall
- Beverly Jiminez
- Alice Bell
- Charlotte Walker
- Scarlett King
- Charles Brown
- Patti May
- Ken Howell
- Lee Conway
- Virginia Gay
- Eric Rutherford
- John Osborne
- Milagros Geraldo
- Honor Carter
- Roman Peter
- Abigail Dennis
- Jim Green

Entities identified by Mandiant³⁰

- Karen Diaz
- Kimberly Allen
- Nikki Brown
- Yasmine Kelly
- Jackie Eberhart
- Jessica Smith
- Teresa Brown
- Gladys Wright
- Jennifer Foster
- Tara Garcia
- Heather Parks
- Anita Bell
- Ashley Wilson
- Brown Emily
- Gonzales Bonnie
- Tamara Smith
- Jane Alice
- Betty Li

.....
²⁹. Nick Monaco, “Five Ways to Spot a Spamouflage Disinformation Campaign,” *Microsoft Threat Analysis Center*, December 22, 2021. (<https://miburo.substack.com/p/five-ways-to-spot-spamouflage>); Nick Monaco, “Emperor in the Ether: Spamouflage’s Authoritarian Attacks on Democracy and Journalists,” *Microsoft Threat Analysis Center*, December 22, 2021. (<https://miburo.substack.com/p/emperor-in-the-ether>)

³⁰. “Pro-PRC DRAGONBRIDGE Influence Campaign Targets Rare Earths Mining Companies in Attempt to Thwart Rivalry to PRC Market Dominance,” *Mandiant Threat Intelligence*, June 28, 2022. (<https://www.mandiant.com/resources/blog/dragonbridge-targets-rare-earth-mining-companies>)

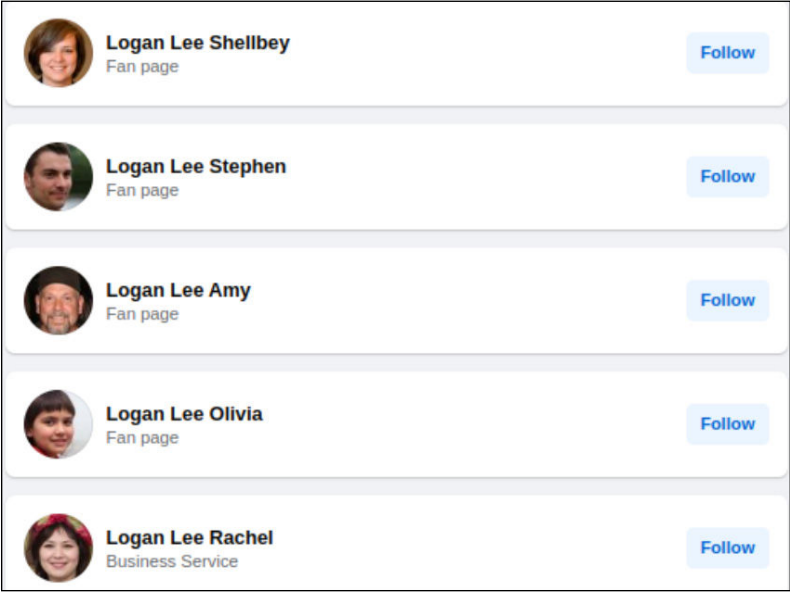
APPENDIX B: PATTERNS ASSOCIATED WITH INAUTHENTIC PAGES IDENTIFIED BY FDD

This appendix provides an overview of significant patterns observed within the 25,000 inauthentic pages identified by FDD. It offers high-level descriptions of each pattern, with a screenshot framing five examples of each. The patterns not only indicate inauthenticity but also suggest batch creation — that is, that the pages were created en masse and likely with automation. These pages generally have very limited or no activity and followers.

1. AI-generated “deepfake” profile photos

Numerous influence operations and other forms of malicious social media activity employ AI-generated “deepfake” profile photos. FDD identified many pages with such photos. The pages shown below provide a small sample.

To demonstrate that these profile photos are all deepfakes, FDD superimposed semi-transparent versions of each profile photo upon each other. This demonstrates that the eyes of each profile photo are centralized and aligned with each other, a textbook indicator of deepfake faces.³¹



31. Ben Nimmo, Camille François, C Shawn Eib, and Léa Ronzaud, “IRA Again: Unlucky Thirteen,” *Graphika*, September 1, 2020. (https://public.assets.graphika.com/reports/graphika_report_ira_again_unlucky_thirteen.pdf)

2. Combination Names

FDD identified a pattern combining multiple names into strings of three or four names. Many of these combinations appear highly improbable, even combining names typically associated with different genders or different regions. For example, “Heather Robinson Deividas Šimkus,” seen below, combines a female name of English-language origin with a male name of Lithuanian origin. Many of the inauthentic pages with combination names reiterate their names in the page description, as seen in the sample below.

	Cori Robinson Heather Robinson Consulting agency Cori Robinson Heather Robinson	Follow
	Heather Robinson Chiranjeevi Vuggili Personal blog Heather Robinson Chiranjeevi Vuggili	Follow
	Heather Robinson Anthony Opeday Women's clothing store Heather Robinson Anthony Opeday	Follow
	Heather Robinson Mike Larson Community Center · 1 follower Heather Robinson Mike Larson	Follow
	Heather Robinson Deividas Šimkus Women's clothing store Heather Robinson Deividas Šimkus	Follow

3. “Hi there, want more beer?” Tagline

One of the first patterns FDD identified includes the tagline “Hi There, Want more beer?” as the page description. FDD identified this tagline on thousands of pages. It was also mentioned in a Facebook Scam Reporting Group as part of a scammer’s pages.³²

	Amelia Chapman Murray Stark Business Center Hi there, want more beer?	Follow
	Amelia Watkins Rehutal Murray Women's clothing store Amelia Watkins Rehutai Murray	Follow
	Jill Murray Amy Amelia Musician/band Hi there, want more beer?	Follow
	Josh Murray Amelia Chapman Women's clothing store Hi there, want more beer?	Follow
	Kevin McMurray Amelia Wilson Baby & children's clothing store Hi there, want more beer?	Follow

32. Chris Stroisch, *Facebook*, March 24, 2023. (Archived version available at <https://ghostarchive.org/archive/cZ3tn>)

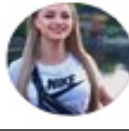
4. “Vinicius Junior” Tagline

FDD identified a pattern including “Vinicius Junior” in the page description. Vinicius Junior is a Brazilian soccer player.

	Sara Jones Fan page Vinicius Junior	Follow
	Sara Jones Fan page Vinicius Junior	Follow
	Sara Jones Business Service Vinicius Junior	Follow
	Sara Jones Fan page Vinicius Junior	Follow
	Sara Jones Fan page Vinicius Junior	Follow

5. Russian-Language Taglines

This pattern involves uniformly recurring taglines with various Russian words in their page description. FDD identified repetition of the following words in page descriptions of inauthentic pages: Кофейня (coffee house), Фестиваль (festival), Танцор (dancer), Журналист (journalist), Фотостудия (photo studio), Магазин одежды (clothing store), and Актер (actor).

	Dennis Abigail Festival · Always open Фотостудия	Follow
	Gonzales Bonnie Festival · Always open Фотостудия	Follow
	King Angle Real Estate · Always open Фотостудия	Follow
	King Angle Restaurant · Always open Фотостудия	Follow
	Hampton Jan Restaurant · Always open Фотостудия	Follow

6. Pages Listed as Vietnamese AIDS Resource Center

FDD identified a pattern of pages with (often identical) human names and no profile photos, all categorized as AIDS Resource Centers and allegedly located in Vietnam.

	Tường Cúc AIDS Resources	Follow
	Tường Cúc AIDS Resources	Follow
	Tường Cúc AIDS Resources	Follow
	Tường Cúc AIDS Resources	Follow
	Tường Cúc AIDS Resources	Follow

7. Tagline “a”

Similar to “Hi there, want more beer?” and “Vinicius Junior” taglines, FDD identified another pattern of pages with the single character “a” in their page description.

	Jennifer Johnson Movie/television studio · 1 follower a	Follow
	Merrie Marketing Agency · 1 follower a	Follow
	Jennifer Johnson Movie/television studio a	Follow
	Jennifer Johnson Movie/television studio a	Follow
	Jessica Smith Movie/television studio a	Follow

8. Page Names Matching Description Ending in 15-Digit Numerical Strings

This pattern involves pages with combined names in which the page description is the name of the page followed by a 15-digit number.

	Carter Sawyer Charles Mckee Baby & children's clothing store Carter Sawyer Charles Mckee - 192614304101075	Follow
	Carter Sawyer Khloe Charles Visual Arts Carter Sawyer Khloe Charles - 1080612391976317	Follow
	Finnley Charles Blaise Carter Women's clothing store Finnley Charles Blaise Carter - 128753240528981	Follow
	Finnley Charles Blaise Greyson Marketing Agency Finnley Charles Blaise Greyson - 123377808095874	Follow
	Finnley Charles Blaise Bruce Spa, Beauty & Personal Care Finnley Charles Blaise Bruce - 139225689474222	Follow

9. Four Random Emojis

One pattern includes pages with page descriptions including four random emojis without additional text or content — for example, “.”



Merrie Ruyle
Product/service



Follow



Merrie Nesta
Product/service



Follow



Merrie Leonsis
Product/service



Follow



Merrie Armanda
Product/service



Follow



Merrie Glaudia
Product/service



Follow

10. Three Random Emojis and Dates

FDD identified a pattern involving page descriptions with three random emojis and a date and timestamp — for example, “ — 2022-11-21 04:11:17.”



KoBay Emely Ellison Crabtree
Personal blog
👤 ❄️ 🌻 - 2022-11-22 14:11:58

Follow



KoBay Emely Ellison Crabtree
Personal blog
🐾 🍄 ❤️ - 2022-11-20 22:11:59

Follow



KoBay Emely Ellison Crabtree
Personal blog
🌱 🐸 🍌 - 2022-11-21 04:11:17

Follow



KoBay Emely Ellison Crabtree
Personal blog
😄 🐟 🦾 - 2022-11-21 04:11:17

Follow



KoBay Emely Ellison Crabtree
Personal blog
👤 🌙 🌐 - 2022-11-21 04:11:17

Follow

11. Identical Japanese Tagline

This pattern involves page descriptions with identical Japanese taglines. Specifically, the pages include the phrase “株投資】誰でも稼げる米国株投資～富裕層になるための鉄則～,” which translates to: “[Stock Investment] Investing in U.S. stocks that anyone can earn ~ Iron rules for becoming wealthy ~.”

	Atsuhiko Nakata Financial Services 【株投資】誰でも稼げる米国株投資～富裕層になるための鉄則～	Follow
	中田敦彦 - Nakata University Financial Services 中田敦彦が「教育系YouTuber」として学べる動画を毎週4本更新（火・水・土・日）もっと学びたい人は中田敦彦主催のコミュニティ「PROGRESS」へ！入会...	Follow
	中田敦彦Nakata University Financial Services 【株投資】誰でも稼げる米国株投資？富裕層になるための鉄則	Follow
	中田敦彦Nakata University Financial Services 【株投資】誰でも稼げる米国株投資？富裕層になるための鉄則	Follow
	Atsuhiko Nakata 【株投資】 Financial Services 【株投資】誰でも稼げる米国株投資～富裕層になるための鉄則～	Follow

12. Emojis and Identical Vietnamese Tagline

FDD identified a pattern involving page descriptions with three emojis followed by a period and an identical Vietnamese tagline. This pattern included, for example, “. Nghiêm Cấm sử dụng cho mục đích trái pháp luật của Việt Nam,” which translates to “Use for purposes contrary to Vietnamese law is strictly prohibited.”



Lee Delaware Logan
Newspaper
🔒🚫🇻🇳. Nghiêm Cấm sử dụng cho mục đích trái pháp luật của Việt Nam

[Follow](#)



Rudy Miller Emery 46939
Newspaper
🔒🚫🇻🇳. Nghiêm Cấm sử dụng cho mục đích trái pháp luật của Việt Nam

[Follow](#)



Kyle Nehemiah Richard
Newspaper
🔒🚫🇻🇳. Nghiêm Cấm sử dụng cho mục đích trái pháp luật của Việt Nam

[Follow](#)



Peter Roman Calum 789626
Newspaper
🔒🚫🇻🇳. Nghiêm Cấm sử dụng cho mục đích trái pháp luật của Việt Nam

[Follow](#)



Davis Zayn Guillermo 211598
Newspaper
🔒🚫🇻🇳. Nghiêm Cấm sử dụng cho mục đích trái pháp luật của Việt Nam

[Follow](#)

13. Alleged Government Agents

One pattern includes pages with the title “Agent.” The page names are often identical — for example, multiple pages are named “Agent Jessica Smith.” Several pages with this naming pattern promote financial scams and contain taglines like “Claimed your own winning money from me.” There is a subset of pages with this naming pattern using photos of government employees as profile photos. Pages in this subset are mainly categorized as “Governmental Organizations.”



Agent Jessica smith

Government Organization · 2 followers · 10+ posts in the last 2 weeks

Okay can I help you to get the agent as soon as possible.....Give me your full name and address to confirm your winnings money

Follow



Peggy Wanczyk Agent Ashley

Government Organization · 7 followers

I'm MAVIS . Kindly DM me now to claim your Grant money and PCH winnings today 🙌🏻

Follow



Agent Peggy Ashley Wilson

Government Organization · 1 follower

Follow



Peggy Ashley Wilson Agent

Government Organization · 1 follower

Follow



Agent Peggy Ashley wilson

Government Organization

Follow

14. “Online” with Five-Digit String and Variations

FDD identified another pattern involving a page name incorporating the word “online” with a five-digit numerical string at the end. Variations include the phrase “online shope” appended at the end of the page name, often with a two-digit string afterward, and others.



Amber Jennings Online 44628
Advertising Agency

[Follow](#)



Amber Jennings Online 83630
Advertising Agency

[Follow](#)



Andrea Acosta Online 43858
Advertising Agency

[Follow](#)



Angie King Online 60991
Advertising Agency

[Follow](#)



Angie King Online 81286
Advertising Agency

[Follow](#)

15. Elegance Tagline

This pattern involves pages with descriptions including the phrase “Where elegance and excellence converge, a haven of refined beauty.”



Jennifer Johnson
Government Organization
Where elegance and excellence converge, a haven of refined beauty 

Follow



Jennifer Johnson
Government Organization · 1 follower
Where elegance and excellence converge, a haven of refined beauty 

Follow



Jessica Smith
Government Organization
Where elegance and excellence converge, a haven of refined beauty 

Follow



Jessica Smith
Government Organization
Where elegance and excellence converge, a haven of refined beauty 

Follow

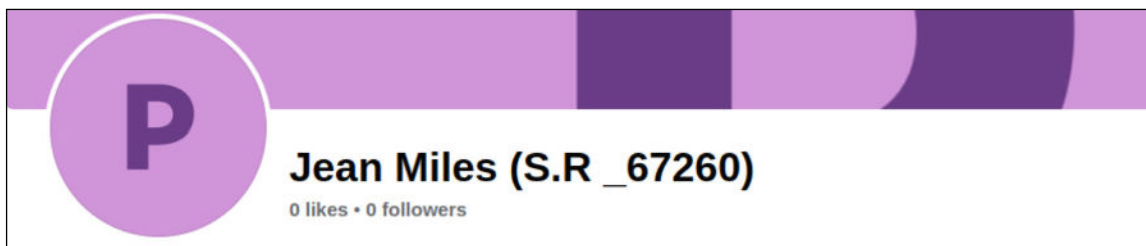
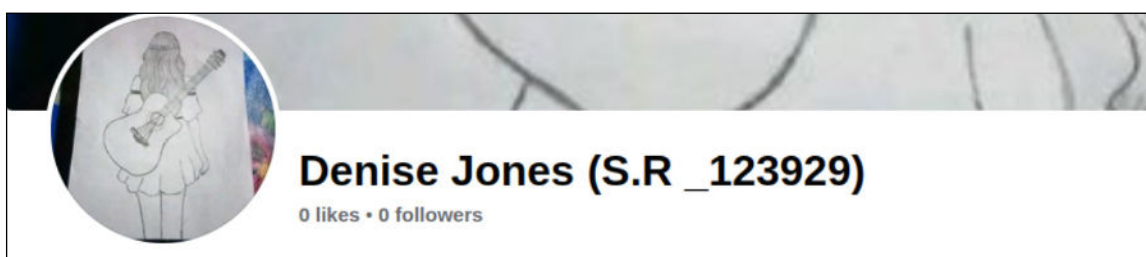
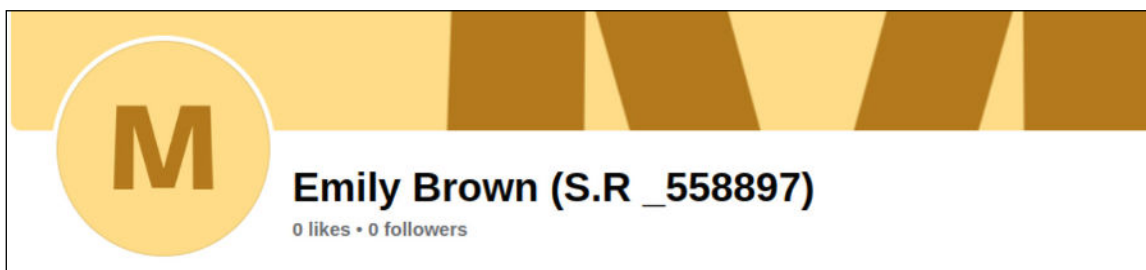


Jessica Smith
Government Organization
Where elegance and excellence converge, a haven of refined beauty 

Follow

16. S.R. in Page Name

FDD identified pages with names including “S.R.” One subset includes two names followed by “S.R_” and a six-digit or four-digit number — for example, “Charles Carter (S.R_123456).” Another subset involves pages named “Md Asadul Islam” with the phrase “S.R Service_” ending in a four-digit or five-digit numerical string.



17. Decimal Names

Another pattern includes a two-word name with three-digit numbers including one decimal space. After the three-digit number, the page names include one other name — “Jack Kim 22.3 Stefan.”



Jack Kim 19.3 Megan
Community

Follow



Jack Kim 22.3 Amora
Community

Follow



Jack Kim 22.3 Devon
Community

Follow



Jack Kim 22.3 Amora
Community

Follow

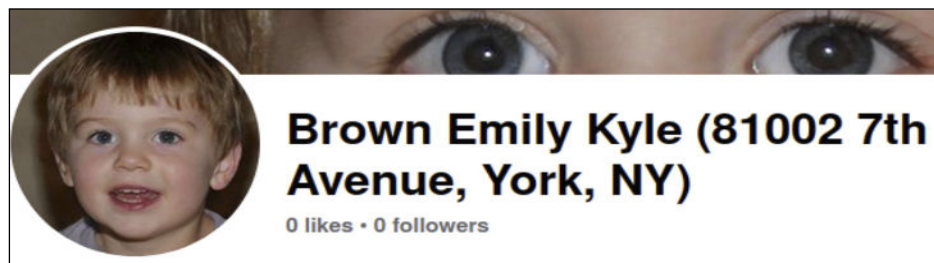
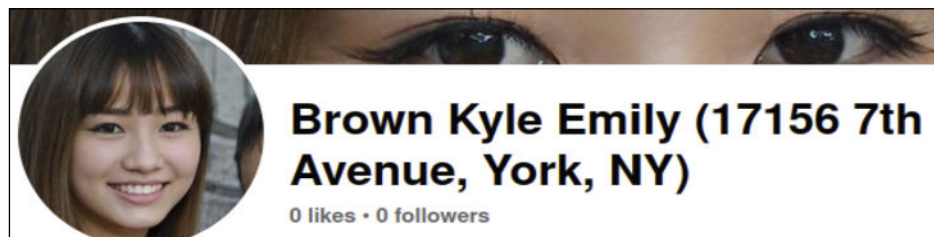
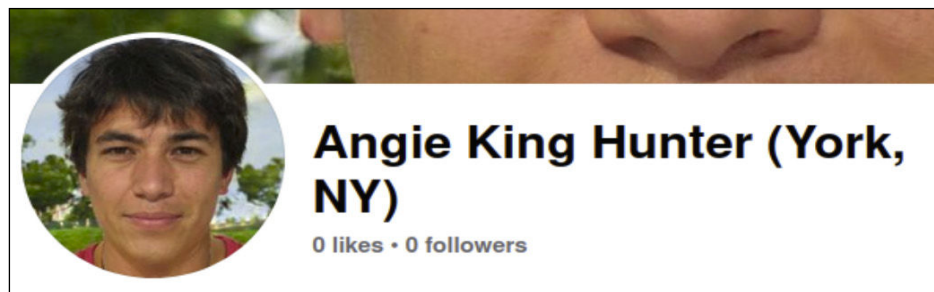


Jack Kim 22.3 Rocky
Community

Follow

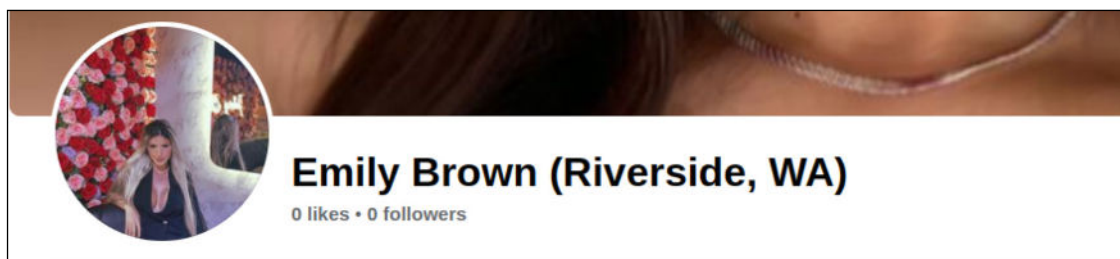
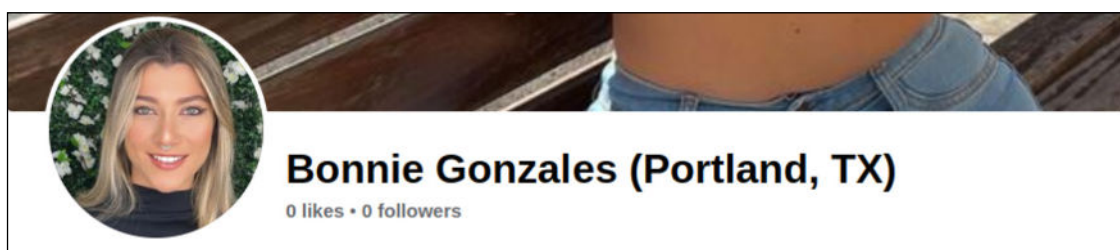
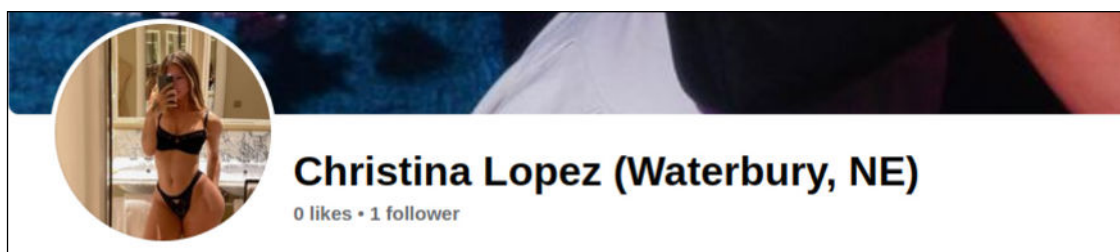
18. Inaccurate Address Information

FDD identified a pattern involving pages with identical or similar human names followed by an address that does not exist. Most included some version of “(York, NY)” and some with more specific addresses — for example, “7th Avenue.” York is a small town of around 3,000 people that does not contain the addresses included in these page names. Whoever created these accounts might have meant to put New York City.



19. Pages categorized as models with locations listed in the page name

This pattern includes pages categorized as models that include parentheses at the end of the page name enclosing names of various U.S. locations — for example, “Elena Johnson (Santa Clarita, CA)” and “Phoebe Smith (Green Bay, WI).”



20. “Hello World” Tagline

FDD identified another pattern involving the phrase “Hello World” in the page description.

	LilMerrie Pharmacy Hello World	Follow
	Merrie Pharmacy Hello World	Follow
	Merrie Pharmacy Hello World	Follow
	MerrieNadya Pharmacy Hello World	Follow
	OdelleMerrie Pharmacy Hello World	Follow

21. Generated by Fewfeed v2

One pattern involves pages with the description “This page was generated by fewfeed v2” followed by four random emojis. These pages reference the website Fewfeed, which offers various social media services, including the automatic creation of multiple Facebook pages. The page creation tool default setting creates pages with the tagline “This page was generated by fewfeed v2” with an option to add emojis to the end.



Merrie Meisel

Product/service

This page was generated by fewfeed v2 🤖👤📱💪

[Follow](#)



Merrie Parcel

Product/service

This page was generated by fewfeed v2 🤖👤👤👤

[Follow](#)



Merrie Giverin

Product/service

This page was generated by fewfeed v2 🤖👤👤👤

[Follow](#)



Merrie Shrier

Product/service

This page was generated by fewfeed v2 🤖👤👤👤

[Follow](#)



Merrie Dow

Product/service

This page was generated by fewfeed v2 🤖👤👤👤

[Follow](#)

22. Repeated Russian Names + Alphabetical Strings

FDD identified a pattern involving pages with two Russian names connected by a dash or period — such as Irina-Ivanova or Ekaterina.Nikitina — followed by strings of apparently random letters. A subset also includes four-digit numbers after the string of random letters. All pages have the page type “Spa, Beauty & Personal Care” and no page activity.



Ekaterina-Nikitina-lierahyka1975

Spa, Beauty & Personal Care

[Follow](#)



Ekaterina-Nikitina-starmennades1971

Spa, Beauty & Personal Care

[Follow](#)



ekaterina.nikitina.v

Spa, Beauty & Personal Care

[Follow](#)



Irina-Ivanova-teczfobiset1988

Spa, Beauty & Personal Care

[Follow](#)



Irina-Ivanova-tysiganme1975

Spa, Beauty & Personal Care

[Follow](#)

Foundation for Defense of Democracies (FDD)

FDD is a Washington, DC-based nonpartisan research institute focusing on national security and foreign policy.

FDD's Center on Cyber and Technology Innovation

The Center on Cyber and Technology Innovation (CCTI) seeks to advance U.S. prosperity and security through technology innovation while countering cyber threats that seek to diminish it. CCTI promotes a greater understanding within the U.S. government, private sector, and allied countries of the threats to and opportunities for national security presented by the rapidly expanding technological environment.

FDD's Barish Center for Media Integrity

FDD's Barish Center for Media Integrity addresses the national security threats posed by misinformation, disinformation campaigns, and influence operations waged by foreign adversaries against the United States and allied democracies.

Max Lesser is the senior analyst on emerging threats at FDD's Center on Cyber and Technology Innovation. Max previously served as head of U.S. policy analysis and engagement at Darktrace Federal, where he analyzed and engaged with policy initiatives surrounding artificial intelligence and cybersecurity. **Sophie McDowall** is an intern at FDD's Center on Cyber and Technology Innovation and studies science, technology, and international affairs at Georgetown University's Walsh School of Foreign Service. **Cat Smith** is an engineer, author, and independent researcher specializing in narrative evolution and information ecosystems. She is currently affiliated with the DISARM Foundation.

FDD values diversity of opinion and the independent views of its scholars, fellows, and board members. The views of the authors do not necessarily reflect the views of FDD, its staff, or its advisors.