WINTER 2018 E-NEWSLETTER

At Digital Mountain we assist our clients with their computer forensics, e-discovery, and cybersecurity needs. For this E-Newsletter, we discuss social media discovery and important strategic legal insights and groundbreaking updates.

Fake Identities on Social Media – An Artificial Brand Boost?

On February 16, 2018, US Deputy Attorney General Rod Rosenstein said in a press conference, “People are not always who they appear to be on the internet.” At the time, DAG Rosenstein was referring to the just announced indictment of 13 individuals for alleged meddling in the 2016 presidential election, but his comment applies to far more than the five counts of aggravated identity theft listed in the indictment. The idea that internet-based identities may not be true and accurate is drawing increased attention. One area of particular interest is social media and the proliferation of fake accounts.

On the surface, a fake social media identity may seem simply juvenile or innocuous: what harm does a fake account, representing a person that doesn’t actually exist, do? Perhaps none. There is no law preventing the creation of fake social media accounts, and the treatment of fake accounts is at the discretion of the social media app provider. Twitter’s policies with regard to fake accounts are vague – there is no language which prohibits a user from creating an entirely fake identity (unlike Facebook, which reserves the right to delete fake profiles). What Twitter does prohibit is impersonation of user accounts, however, the language of the policy may leave room for the creation of nearly identical persona:

> Accounts with similar usernames or that are similar in appearance (e.g. the same avatar image) are not automatically in violation of the impersonation policy. In order to be impersonation, the account must also portray another person in a misleading or deceptive manner (*https://help.twitter.com/en/rules-and-policies/twitter-impersonation-policy?lang=en*).

The language in the last sentence of Twitter’s policy may have caught New York Attorney General Eric Schneiderman’s attention. Following a report by the New York Times, AG Schneiderman opened an investigation into the creation and sale of fake user and authentic accounts being created and subsequently sold as followers by Devumi, LLC. The article details

how Devumi sells followers to users and generates retweets using mass amounts of automated accounts and impersonated user profiles (https://www.nytimes.com/interactive/2018/01/27/technology/social-media-bots.html).

While the average Twitter user may scratch their head at the notion of buying followers, there's a solid commercial reason for doing so: social media influence is big business. Social media influencers, according to the NYTimes article, can earn six-figure salaries by promoting branded products, influence potential employers looking to hire someone whose social media following will guarantee attention, or even increase their political capital by creating the perception of a wide following. Again, though, if the accounts are entirely made up of imaginary users and their only purpose is to inflate the follower count, where's the harm?

The harm is that the NYTimes has allegedly caught Devumi creating fake accounts using the personally identifiable information of real users, stealing real user profiles, and stating on their website that all followers they sell are in fact "high quality," albeit admitting in the same sentence that the accounts may be inactive. For Devumi's YouTube service, they guarantee that they sell "100% Real & Relevant Viewers." According to the NYTimes, there are apparently somewhere in the region of 55,000 instances of impersonation by Devumi, and according to their website, over half a million Twitter followers are available for sale (https://devumi.com/twitter-followers/).

Little Guiding Precedent

New York's Attorney General, along with Florida Attorney General Pam Bondi, and U.S. Senators Jerry Moran and Richard Blumenthal, are all looking to see if there is legal footing to stop Devumi and other like entities from trafficking in fake accounts, as well as pursuing crimes of impersonation and deception. Senators Moran and Blumenthal in a January 30, 2018 letter to the Federal Trade Commission urged the FTC to investigate the practice. Irrespective of which entity undertakes the task, the case will be groundbreaking as no identical case of a company creating impersonating accounts in the service of creating an online service or commodity has been heard before a federal court to date.

Online impersonation cases generally involve a party impersonating via the internet a person with whom the impersonator has some conflict and with intent to harm the impersonation victim or another person or organization with which the victim is associated. The matter of whether Devumi has engaged in identity theft, in creating fake accounts by making minor alterations to the original user's profile data, adds an interesting aspect to the investigations. For example, if the user's Twitter handle is @janedoe999, the Devumi generated account may be @janedo999, or @janedoe9999, and may use an altered or enhanced photo of the original user. This activity in and of itself may not violate any laws and does not violate Twitter's impersonation policy. Whether Devumi's profiting from creating fake accounts based on actual users is identity theft will be determined in due course, and most likely in a court room.

Devumi's intent in impersonating users is to create automated accounts for sale to Twitter users. Whether or not the impersonated account owner is actually harmed by the creation of the fake account isn't immediately evident. Devumi is not alleged to be committing any of the traditional identity theft crimes: harassing or cyberbullying, ruining reputations, using the identity for illegal financial gain such as credit card fraud. As frustrating and unjust as the practice appears, there may not be a case to say that registering an impersonated user as another user's follower causes actual damage to the real user.

The aspect which the FTC is being urged to pursue falls under Section 5 of the FTC Act (14 USC §45) regarding deceptive or unfair marketing practices. Senators Moran and Blumenthal in their letter to the FTC state their belief that Devumi's practices are identity theft and are "distorting the online marketplace" (https://www.blumenthal.senate.gov/imo/media/doc/01.31.2018%20Letter%20to%20FTC%20re%20Devumi%20and%20Fake%20Followers.pdf).
This may end up being the strongest aspect of any case against Devumi, as there is evidence that Devumi's fake followers have translated into financial gain for both Devumi and the purchasers. The sale of fake followers to inflate one's standing and influence in the social media marketplace may constitute a fraud if financial gain was achieved as a result of the purchase of those fake followers. However, in this situation, the action may come against the purchaser of the fake followers by a third party, not Devumi as the seller.

Irrespective of the vagueries of any legal issues which may develop, Devumi, and other companies engaged in similar activities, have created a new ecommerce market, and not just on the sale side of fake followers. Companies such as Distil Networks and Smyte are now selling services to help clients detect and block automated fake followers from parking on their social media accounts. Proving once again, a real solution will arise for any problem, real or fake.

Please direct questions and inquiries about cybersecurity, computer forensics and electronic discovery to info@digitalmountain.com.

UPCOMING INDUSTRY EVENTS

MASTERS CONFERENCE
Dallas, TX: February 28, 2018

THE ASU-ARKFELD 7TH ANNUAL EDISCOVERY
Phoenix, AZ: March 6-8, 2018

SECURING THE FUTURE OF THE INTERNET OF THINGS
San Francisco, CA: March 6-7, 2018

SYMPOSIUM ON SECURING THE IOT
San Francisco, CA: March 6-7, 2018

ABA TECHSHOW 2018
Chicago, IL: March 7-10, 2018

Click here to see more upcoming events and links

Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at various upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com.

DIGITAL MOUNTAIN, INC.
4633 Old Ironsides Drive, Suite 401
Santa Clara, CA 95054
866.DIG.DOCS

www.digitalmountain.com

Contact us today!

FOLLOW US AT: