Tackling Twitter And Facebook Fakes: Identity Theft In Social Media

By Alexander Tsoutsanis, of DLA Piper, Amsterdam.

With over 300 million and 500 million users across the globe, respectively, Twitter and Facebook are in high demand. Equally demanding are the legal challenges both companies face. Much of the legal discussion around these sites today focuses on a key concern: fraud.

Although many users are voluntarily tweeting and posting on their daily lives, this sometimes occurs involuntarily. In growing numbers, people find themselves exposed to fraudulent behavior, with others impersonating them on Twitter and Facebook through fake accounts.

This article briefly explores how to take action against fake social media accounts and also discusses recent developments in the Netherlands, the United Kingdom, and the United States.

Twitter’s and Facebook’s Own Policies

Fake accounts crop up to other scenarios that Twitter has implemented its own “Impersonation Policy.” According to Twitter, users “may not impersonate others through the Twitter service in a manner that does or is intended to mislead, confuse, or deceive others.” Violation of this rule may result in permanent suspension of the account. Individuals are obviously able to obtain such suspension only if they file a complaint with Twitter first.

As part of its own agreement, Facebook also prohibits users from creating an account for someone else without permission. Providing false personal information is also regarded as misconduct. Violations can be reported through Facebook’s standard reporting policy.

Netherlands

There are countless examples of fake accounts in social media. For example, in the Netherlands, the Dutch prime minister found himself embarrassingly exposed to a Twitter account run by a student, disseminating tweets which were, to say the least, politically unhelpful. The prime minister subsequently requested that Twitter remove the account.

Another example involved a well-known Dutch lawyer who did not want to be on Twitter but one day found that she was, much to her own dismay. The lawyer, Benedicte Ficq, filed a complaint with Twitter to shut down the fake account.

However, she also filed her own legislative proposal to prevent such forms of identity fraud on the internet. The proposal was launched in January 2012 and has been submitted to the Dutch Parliament for further consideration. Benedicte Ficq filed a complaint with Twitter to shut down the fake account.

The new proposal is to be considered by the Dutch Criminal Code prohibiting so-called “identity theft.” The proposed sentences are steep, with a maximum of four years’ imprisonment or a fine of 19,000 (U.S.$24,910) or both.

There has been some criticism of the new proposal. It is, for example, unclear whether the new proposal is aimed at deeming a tweet a crime.
benefit in introducing new legislation on 'identity theft'. Users individuales falling victim to fake social media accounts, ranging from privacy to already personal or privacy, even if they cannot rely on a trade mark. The matter of personal information is already regulated in the Data, Civil Code (Article 1115) (i.e., 1900). In addition, the use of someone's photo may be, for example, a fake Twitter account in a closing section of many rights. While such accounts might be deceptively similar to those by fake social media accounts, to obtain an injunction and successfully compelling the account, claims based on misleading advertising or defamation are also possible. The same applies to businesses are able to rely on infringement of their trade mark. However, whether use in the course of trade is involved, most account holders is likely to be balanced against free speech and the extent to which the average user is liable to be concerned. In case of a parody, the cause of action of the right holders or individuals are not.

**How to Tackle Fakes**

Regardless of the available legal grounds, the biggest hurdle for victims is to choose the right avenue and property owners of the holder of the fake account. Legal remedies are effective only if those accounts can be removed. If defamation generally requires knowledge of the identity of the fake profile holder, codes of enforcement although are able to obtain such information from web servers (e.g., through IP addresses), arrests right holders or individuals are not.

This is why, in most cases, victims tend to submit a complaint with, for example, Twitter or Facebook, requesting their removal. Although this has hardly any deterrent effect, it does allow for a speak and effective resolution of most complaints.

If the fake account causes severe damage, the developers should contact them to take down the fake account. Although this is difficult, they can remove all such accounts involved. In Section 528.5 of the California Penal Code, it is a crime to impersonate another actual person on the internet for the purposes of harming, intimidating, or defrauding. The penalties involved boil down to a maximum of one year's imprisonment and/or a fine of U.S.$1,000. The requirement of 'credible impersonation' aims to ensure that 'parody accounts', will still presumably proceed in such cases that the account is a 'fake' or 'parody' and not the real deal.

A similar requirement is also imposed for Facebook and Twitter desmentions, which do allow 'parody accounts', but require the two to not set the content of the profile. By adding a qualifier, such as 'not', 'fake' or 'parody' accounts.

**United States**

Apart from requesting victims themselves to take action against fake social media accounts for, among others, lapsing privacy, social development within the United States show that legislation also underscores the need for addressing the issue of public safety.

For example, in California, the honor bill of Susan and Facebook, a new law was enacted in 2011 specifically aimed at preventing fake social media accounts (effective January 2011). It permits the provision of the California Penal Code in a case where an account is found to be ‘fake’ or ‘parody’ and not the real deal.

The new law states that if a person uses a false identity or a false account to disclose the registration information and personal data, and the information or data is false or misleading. This person, upon the request of another person or the court, shall be required to disclose the true identity and personal data. If the person refuses to disclose the true identity and personal data, they shall be enjoined by a court to disclose the true identity and personal data. In the case of a fraud, the court may order the person to disclose the true identity and personal data.

The new law also states that if a person uses a false identity or a false account to disclose the registration information and personal data, and the information or data is false or misleading. This person, upon the request of another person or the court, shall be required to disclose the true identity and personal data. If the person refuses to disclose the true identity and personal data, they shall be enjoined by a court to disclose the true identity and personal data. In the case of a fraud, the court may order the person to disclose the true identity and personal data.
Where the fake account has caused little damage, it is recommended to file a complaint only with, say, Twitter or Facebook. If the damage is more severe, individuals should consider a two-track strategy. First, it is best to file a complaint with law enforcement officials (e.g., citing 'identity fraud'). Although this does not always result in actual prosecution, lodging the complaint alone often serves as a useful deterrent. Second, following advice by local counsel, bringing a claim in the civil courts should be considered, seeking an injunction and monetary compensation. The Firsht case above shows that such remedies can be quite effective. Whether such civil action makes sense obviously depends on the damage and the costs involved.

Future Developments

On both platforms, the real cause of fake accounts is the low threshold to obtain such an account and the absence of proper verification of user identities. The absence of a proper verification program on Twitter and Facebook causes the user to make their own efforts to ascertain the identity of users. On Twitter, one can follow suggestions made by selected users, advertisers and partners on Twitter's behalf in realizing the non-identities of users or alert Twitter. Recently, Facebook announced that it will be offering a "Verified Accounts" program for selected users. This is, however, limited to prominent public figures and does not include ordinary users.

From a policy perspective, one can wonder whether Internet companies like Facebook or Twitter should have a fiduciary duty to verify the identities of their users. Given the impact of social media today, there is much to be said in favor of such an obligation. In the absence of proper verification, Twitter and Facebook fakes are here to stay.

NOTES


3. Article 1:8 BW; Article 12 BGB; Article 29 ZGB.

Alexander Tsoutsanis is a Senior Associate in DLA Piper’s IP group, based in Amsterdam. He may be contacted at alexander.tsoutsanis@dlapiper.com.