UDC 347.77

CYBERSQUATTING IN THE UNITED STATES OF AMERICA: LEGAL ISSUES AND TRENDS

TATSIANA SIAMIONAVA
Polotsk State University. Belarus

Our article looks deeper into the phenomenon of cybersquatting by analyzing the most common types of cybersquatting, discussing cybersquatting-related monetization practices, examining the most vulnerable sectors affected by cybersquatting, and recommending ways to combat cybersquatting.

Introduction. Protecting company's intellectual property, including designs, patents, trade names, and domain names, is an essential condition for establishing a successful business. The standard way to protect a brand is to register a trademark, a trade name or a logo that distinguishes the brand from other businesses in the field. The failure to register a trademark may result in financial losses, reputational harm, and circulation of counterfeit. Registering a trademark is also an important step in preventing cybersquatting.

The US Anticybersquatting Consumer Protection Act (ACPA) defines cybersquatting as an opportunistic practice of registering, trafficking in, and using a domain name resembling a trademark belonging to someone else with the aim to profit from it. Cybersquatting started emerging in the middle of 1990s.

Cybersquatters usually aim to resell the domain name back to the trademark owner or benefit from the web traffic generated by the domain name. For example, domain names registered as a result of cybersquatting may include «www.gooogle.com», «faceboook.com», «www.amozon.co.uk», «MikeRoweSoft.com», and «www.parishilton100.net».

The tendency of abusive domain name registration is growing steadily. In 2017, The Arbitration and Mediation Center of the World Intellectual Property Organization (WIPO) received 2.754 complaints related to cybersquatting, 5% more than in 2016. The fraudulent gTLD registrations are anticipated to increase further as new domain name extensions (e.g., .shop) are about to launch.

Types of cybersquatting. Cybersquatters are free to register any available domain names, even if such domain names significantly resemble already registered domain names. Cybersquatters usually use a combination of legal and illegal schemes to get profits. Such schemes may include the following elements: (1) registering domains which include common English words with the aim to resell them in the future; (2) registering mostly mistyped spelling of the names of popular websites; (3) purchasing recently expired domain names; (4) publishing derogatory remarks about a company or a person on the cybersquatted website; and (5) monetizing the content by publishing affiliated links and encouraging users to click on them. As a result of such practices, the owner of the legitimate website may experience serious financial and reputational consequences. At present, there are four dominant cybersquatting types, namely, typosquatting, identity theft, name jacking, and reverse-cybersquatting. They are briefly discussed below.

Typosquatting. Typosquatting is often referred to as «URL hijacking», «a sting site», and a «fake URL». Typosquatters rely on common mistakes made by Internet users when typing a web address into a web browser. Such mistakes include misspelling (e.g., «www.intrenet.com»), different phrasing of a domain name (e.g., «www.internets.com»), other top-level domain («www.internet.net»), and use of Country Code Top-Level Domain (ccTLD) (e.g., «www.internet.co»). More advanced typosquatting techniques exploit visual, hardware, and sound similarities of trademarks. For example, homograph attacks rely on the visual similarity of symbols that can be confused, as well as on letters or strings that might be confused with one another, such as confusion between «vv» and «w» in the domain name «www.bankofthewest.com» («www.bankofthevvest.com»).

To trick Internet users, typosquatters may also create a fake website that resembles the source by using a similar layout, color schemes, logos, and content. Typosquatters use such fake websites to (1) compel legitimate website owners to buy the cybersquatted domain names, (2) generate more web traffic, and (3) spread malware.

Identity theft. Cybersquatters may purchase a domain which was unintentionally not renewed by the previous owner. Cybersquatters use special software applications which allow them to monitor the expiration dates of targeted domain names easily. After registering the expired domain names, cybersquatters may link them with websites which duplicate the websites of the previous domain name owners. Thus, cybersquatters

will mislead the visitors of their websites into believing that they are visiting the websites of the previous domain names owners.

Name jacking. Name jacking refers to the registration of a domain name associated with the name of an individual, usually celebrities and well-known public figures. Name jackers benefit from web traffic related to the targeted individuals.

In the USA, personal names can have trademark protection if they acquire distinctiveness through advertising or long use and establish a secondary meaning. Personal names that do not fulfill this condition cannot be registered as trademarks because many people within the same territory may share the same name. Hence, name jackers may fall outside the scope of the US Anticybersquatting Consumer Protection Act.

The registration of the domain name «Madonna.com» was a typical example of name jacking. The domain name, which is identical to the name of the pop diva Madonna, was used for spreading pornographic materials.

Reverse-cybersquatting. Reverse-cybersquatting refers to an attempt to secure a domain name legitimately owned by another person. Reverse-cybersquatting may include intimidation and pressure to transfer the legitimate ownership of a domain name to the person or organization which owns a registered trademark reflected in the domain name.

It should be noted that reverse cybersquatting may be considered an abuse of domain name dispute resolution procedures. Reverse-cybersquatting may also constitute a tort or an unfair business practice within the meaning of the laws of some jurisdictions and, therefore, entitle the victims of reverse-cyber squatters to compensation for damages.

Monetization Practices. Cybersquatters employ at least the following five techniques to obtain profits from their activities: (1) domain parking; (2) ransoming domain names; (3) affiliate marketing; (4) hit stealing; (5) scams. These five techniques are examined in more detail below.

Domain parking can be defined as redirecting a domain name to a website that contains advertisements for the purpose of generating web traffic.

Ransoming domain names refers to the use of domain names for spreading ransomware. It usually blocks access to the files of the infected systems until the victim pays a ransom. Some forms of ransomware (e.g., Locky) decrypt the files of the infected system, thus making the recovery of the encrypted files virtually impossible.

Affiliate marketing means redirection to web pages used for selling product and/or services in exchange for commissions on the sales of those products and/or services.

Hit stealing is the practice of referring an Internet user who visits a website associated with a cybersquatted domain name to the website of a competitor.

Scams related to cybersquatting may include, for example, identity theft and credit card fraud. By way of illustration, operators of cybersquatting websites may announce that people who register accounts on their websites may win various prizes. The personal data collected in this way can be used for identity theft.

Most vulnerable sectors affected by cybersquatting. The website of the World Intellectual Property Organization (WIPO) indicates that, in 2017, most domain name cybersquatting cases were related to the following 5 areas of commerce: (1) fashion (10% of cases); (2) banking and finance (9% of cases); (3) Internet and IT (9% of cases); (4) retail (8% of cases); and (5) biotechnology and pharmaceuticals (7% of cases). In 2015, multinational corporations, including «Hugo Boss» (62 cases), «Philip Morris» (60 cases), and «Electrolux» (48 cases) were the most active complainants.

Combating cybersquatting. The domain name registrars can contribute to the fight against cybersquatting by requiring potential registrants of domain names corresponding to registered or unregistered trademarks to present trademark certificates or authorizations from trademark holders. However, the main actor in counteracting cybersquatting is the Internet Corporation for Assigned Names and Numbers (ICANN), the organization responsible for maintaining the global domain name system, which allows victims of cybersquatting to resolve their disputes by using procedures organized under the Uniform Domain Name Resolution Policy (UDRP). Such procedures are quicker and cheaper than traditional litigation.

Before submitting a UDRP claim, one needs to meet the following conditions:

The complainant has to have a registered or unregistered trademark. Evidence proving the existence of such a trademark should be submitted to the arbitrational panel.

The complainant has to explain how the trademark owned by him is identical or confusingly similar to the disputed domain name.

The complainant has to prove that the holder of the disputed domain name does not have the rights in the disputed domain name.

The complainant must prove that the disputed domain name was registered in bad faith.

Commenting on the importance of the UDRP, WIPO Director General Francis Gurry states: « By combating opportunistic domain name registration practices, WIPO's services help consumers to find authentic web content and enhance the reliability of the Domain Name System».

Despite the effectiveness of the UDRP, owners of trademarks willing to preserve their good reputation should rely not only on post-factum measures to remedy the effects of cybersquatting, but also take preventive measures aiming to reduce the risks of cybersquatting. For example, trademark owners may register domain names which are confusingly similar to their trademarks, thus preventing cybersquatters from registering those domain names.

Conclusion. Cybersquatting has become a lucrative online practice that may negatively affect the reputation of well-established commercial brands. The owners of such brands may face legal challenges related to overcoming their cybersquatting issues. This is because the demarcation line between the legality and illegality of cybersquatting is difficult to draw, as the phenomenon combines both legitimate and illegal activities.

Although domain name disputes related to cybersquatting and related practices can be resolved in a timely and affordable manner through UDRP procedures, preventive measures can save trademarks owners the fees for initiating such procedures.

REFERENCES

1. 15 U.S. Code § 1125 – False designations of origin, false descriptions, and dilution forbidden. Cornell University Law School, 2017. – Mode of access: https://www.law.cornell.edu/uscode/text/15/1125. – Date of access: 04.01.2018.
2. About Cybersquatting. ICANN, 2017. – Mode of access: https://www.icann.org/resources/pages/cybersquatting-2013-05-03-en. – Date of access: 04.01.2018.
3. Anti-Cybersquatting Piracy Act (ACPA). Harvard University, 2017 https://cyber.harvard.edu/property00/domain/legislation.html . – Date of access: 04.01.2018.
4. Cybersquatting Cases Up in 2017, Driven by New gTLDs'. WIPO, 2017. – Mode of access: http://www.wipo.int/pressroom/en/articles/2016/article_0003.html . – Date of access: 04.01.2018.
5. Dimitrova, M. Most Ludicrous Ransomware in 2017'/ M. Dimitrova // SensorTechForum, 2017. – Mode of access: http://sensorstechforum.com/ludicrous-ransomware-2017. – Date of access: 04.01.2018.
6. The Anti-Cybersquatting Consumer Protection Act (ACPA). JUX. Mode of access:http://jux.law/the-anti-cybersquatting-consumer-protection-act-acpa/ – Date of access: 04.01.2018.
7. Trends in Cybersquatting and Internet Domain Names in 2017. WIPO, 2017. – Mode of access: https://www.youtube.com/watch?v=8v3iua8QZ-8 . – Date of access: 04.01.2018.