E

WIPO
WORLD
INTELLECTUAL PROPERTY
ORGANIZATION

WIPO/ACE/10/22
ORIGINAL: ENGLISH
DATE: JULY 31, 2015

Advisory Committee on Enforcement

Tenth Session
Geneva, November 23 to 25, 2015

THE ACTIVITIES OF THE FEDERATION OF THE SWISS WATCH INDUSTRY IN THE AREA OF PREVENTIVE ACTIONS TO ADDRESS ONLINE COUNTERFEITING

prepared by Carole Aubert, Head of the Internet Unit, the Federation of the Swiss Watch Industry (FH)[*]

ABSTRACT

The Internet allows counterfeiters to reach a global audience at very low cost and minimal risk. Counterfeiters benefit from the anonymity of the Internet and consumers are extensively exposed to the phenomenon. Because there is little to no risk associated with their behavior, perpetrators are eager to develop the online sale of counterfeits, which renders enforcement increasingly complex and sophisticated. Therefore, the issue should be tackled within a global approach that takes into account the various dimensions of the problem. Cooperation between different stakeholders – both private and public – is the key. Such cooperation should firstly aim at developing a better understanding of the phenomenon, through the sharing of information, intelligence, best practices, expertise and experiences. In addition, it is important to change mindsets and stimulate greater respect for intellectual property (IP) rights. Finally, there is a need to work towards the emergence of a global soft law regarding IP enforcement on the Internet.

[*] The views expressed in this document are those of the author and not necessarily those of the Secretariat or of the Member States of WIPO.

I. INTRODUCTION

1. The steady growth of globalized e-commerce has opened a door to a global economy: online trading offers unprecedented opportunities to consumers and businesses to buy and sell goods, nationally, across the borders of the domestic market, and internationally. On a worldwide scale, the Internet reduces cross-border barriers to trade.

2. However, illicit or fraudulent commercial traders of counterfeit products are also exploiting the advantages of e-commerce to offer counterfeit products directly to consumers. The Internet has created new distribution channels, which allow counterfeiters to reach a global audience at very low cost and minimal risk. The counterfeiters benefit from the anonymity of the Internet and consumers are extensively exposed to the phenomenon and can easily buy, knowingly or unknowingly, counterfeited items via this distribution channel. The e-commerce has induced an increasing demand for counterfeits and as a result, an increase in supply.

3. Globalization and the spread of technology, allowing simple, low-cost duplication of popular products, as well as packaging and labeling, are important factors facilitating the increase in intellectual property rights (IPR) violations. For several years a growing share of the sale and distribution of counterfeit products has reportedly originated from the Internet.[1] Counterfeit products are purchased online and shipped overseas by postal and express mail services, often in relatively small quantities that are difficult to detect for customs authorities or law enforcement agencies. Seizure statistics from customs show an increasing share of seizures from air express and postal shipments and a decline in the share of seizures from commercial cargo shipments. This is due to the individual sales performed on the Internet and for a large part on B2B or B2C online marketplaces.

4. Moreover, in most European countries there are fewer and fewer “open markets“ where counterfeit goods can be freely purchased. In such conditions, buyers tend to buy online on virtual marketplaces or standalone websites where the visibility and accessibility of fake watches is obvious.

5. The European Union (EU) reports an increasing number of seizures from postal and air express mail shipments (small consignments) relating to sales on the Internet. Statistics show a continuous upward trend in the number of shipments suspected of violating IPRs. This increase is wholly dependent on air, express and postal traffic, as a result of growth of the e-commerce market.

6. In recent years, thanks to the efforts undertaken by stakeholders (IP owners and European platforms) to clear EU platforms, a shift has been observed: more and more items are sold on non-EU overseas platforms. However, European consumers do not hesitate to order on these foreign sites, as shown from customs seizures at EU borders.

7. Because there is little to no risk associated with their behavior, perpetrators are eager to develop the online sale of counterfeits.

---

[1] International AntiCounterfeiting Coalition (IACC) written submission to the United States Trade Representative (USTR), February 15, 2011, p. 13; Interviews with industry representatives by U.S. International Trade Commission staff, Washington, DC, United States of America, November 3, 2010, and March 1, 2011.

II. WHICH SOLUTIONS TO ADOPT TO TACKLE THIS GROWING PHENOMENON?

8. The fight against counterfeiting is therefore becoming increasingly complex and sophisticated. Existing enforcement methods are limited and tech-savvy counterfeiters are very reactive, creative and up-to-date. Therefore, there is no definitive solution to tackle the online sale of counterfeits, moreover as the Internet is in constant evolution. The response should be global.

9. As the Internet is a channel of transmission, every stakeholder involved in the distribution chain has a role to play, from internet service providers to hosting providers, content delivery networks, search engines, social networks, platforms, online payment processors, express shipping companies, etc.

10. Although the problem can never be completely eradicated, the main goal is to create major disincentives in order to reduce visibility and sales volume of fake items. At the FH, actions are inspired by led intelligence policing life cycle: operational actions, strategic actions and lobbying/enforcement.

11. Intelligence is not what is collected; it is what is produced after collected data is evaluated and analyzed (as “information plus analysis equals intelligence”).[2] Intelligence is critical for decision making, planning, strategic targeting and crime prevention. Therefore the operational basis conducted by the FH’s Internet Unit team is of utmost importance: it is the raw material which brings information where illegal traffic operates. Nonetheless, it is necessary to reach a certain volume of data during the operational phase, in order to obtain sufficient relevant information to fully understand the situation and take appropriate action at the strategic level.

How to proceed accordingly?

12. Regarding standalone websites, the key features are: extensive number of sites dedicated to the sale of fake watches, high volatility and multi-site strategy elaborated by perpetrators. FH response is to target the most visible counterfeiting websites (as consumers will buy on these first), to automate the processes (collecting data and evidences, notification of cease and desist letters) and to follow-up regularly to ensure the effectiveness of FH measures. The strategic phase should then lead to networks’ identification. The FH has developed an in-house tool in order to automate, track, and manage infringing websites collected in this database. What might look like a “whack-a-mole” game is necessary to collect data but bearable as most of the process is now automated.

13. The FH also regularly conducts domain name seizures in the United States of America, as data analysis allows us to find robust websites with generic domain names and hosted in

---

[2] Intelligence-Led Policing: The New Intelligence Architecture, U.S. Department of Justice, Bureau of Justice Assistance, September 2005.

non-compliant countries. In such cases, domain seizures are operated collectively for the FH members. The recovered domains are then used to promote consumers' awareness (ex: www.replicahause.com). Moreover, the ranking of the seized domain is used to supplant other dedicated websites in search engine results in order to reduce visibility of the fake goods, at least for a few months.

14. Regarding marketplaces, the key features are platforms' diversity (even from computer programming point of view), multiple languages and currencies, and a large number of ads to manage within a short period. The FH response is a tailored flexible tool to detect, store and notify infringing ads.

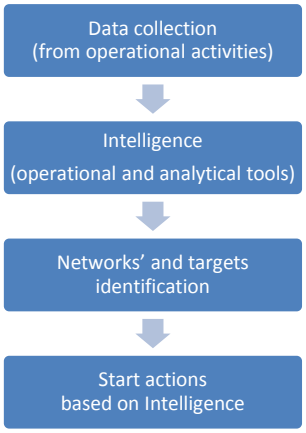
15. Thanks to efforts undertaken by stakeholders, a shift has been observed and monitoring now concentrates mainly on Asian platforms. Famous venues such as eBay or others owned by the two major players in Europe [Schibsted group (Leboncoin.fr or seguademano.es among others) and Naspers (Allegro platforms among others)] have now reduced infringement to an acceptable rate of dubious ads, even if significant differences can be observed among marketplaces owned by the same group. As a result, monitoring carried out by the FH Internet Unit now focuses on Asian or non-EU sites, as these platforms clearly target European consumers. These platforms are displayed in English and very often offer multilingual support; moreover, major credit cards are accepted for payment.

16. Newcomers are indeed social media, which are used for direct sales with local contact as well as for promotion of dedicated websites. New marketplaces are very often available on mobile devices only (Mobile Apps). FH had to adapt its IT tools as well as its strategies in order to include monitoring and intelligence on any new venue.

III. STRATEGIC ISSUES

17. As explained above, the data gathered through the operational phase must not only be stored but analyzed in order to identify strategic targets. The specificities with Internet sales are huge data sets to deal with, which call for specific IT tools. The quick data obsolescence is also an issue, as counterfeiters are reactive and this requires regular monitoring on all previously collected sources. Previous data sets should nonetheless be recorded to establish links and to identify networks. And finally, due to the quantity of information, it is necessary to define priorities according to the offers' visibility. In addition, FH faces a multi-faceted sales strategy, by virtue of the digital convergence: fraudsters promote their illegal products by using a multi-channel strategy. Consequently, a unique seller can be active on social networks, operate various sales platforms under multiple accounts and will manage one if not several dedicated websites. If FH achieves to link all these sources, it will be able to generate a comprehensive seller profile and to define whether any enforcement action is required and under which form, as FH has to be most effective with limited resources.

18. With such amount of information, the challenge is to represent the information in a comprehensible and usable form, in order to detect what are called "hot spots", for instance reluctant host providers or websites operated by the same entity. As a positive aspect, the information is digitally stored. This information could be referred as traces, which could be collected and analyzed.



19. Actions are of course based on enforcement but may be technology-based (ex: requesting a deposit to open a new seller account on a sales platform or implementing an effective enrollment process to check the seller's real identity). Regarding enforcement actions, it is very important to build constructive relationships, collaboration and joint actions with law enforcement as well as to provide training for those engaged in combating counterfeiting.

IV. MONITORING AND COOPERATION WITH TECHNICAL INTERMEDIARIES

20. Basically, it is very important to establish smooth cooperation with all major stakeholders, in order to be efficient without burdensome requirements from technical intermediaries.

21. With sales platforms, FH analyzes primarily legal and technical requirements in order to define how to report infringements in the most efficient way, bearing in mind that FH acts on behalf of about fifty different brands. Some platforms have developed sophisticated reporting tools and FH includes these in its monitoring tool. On less developed platforms FH sends automated notifications by email. Subsequently after an observation phase, FH tries to define how to enhance the reporting process and how future infringements may be avoided for instance by implementing filters on certain products categories with specific keywords or price range. Detection of repeated offenders is very important, but this is made possible only by having a detection tool and effective measures enforced by the platforms (such as deposit, entrance fee, effective seller identification, etc.).

22. With hosting providers, the FH monitoring tool enables the identification of favorite web host companies. This helps then to establish a direct contact with these companies in order to prevent them from offering their services to infringers. Very often a solution is found as their customers often breach their own Terms of Use, which oblige customers to refrain from illegal activities. As mentioned in the Introduction, counterfeiters are tech-savvy and very reactive. Thus, new forms of hosting have emerged, such as cloud hosting or content delivery networks. Even if these forms of services are initially intended for legitimate purposes, counterfeiters have quickly understood the benefits of anonymity that could be gained by using these new online services, in order to obfuscate and conceal their identity more deeply in the anonymity of the World Wide Web. Technology-neutral regulations should be enacted in order to have a comprehensive approach to legal issues, including liability of technical intermediaries which are non-compliant.

23. Some other intermediaries are of utmost importance in fighting against online fraudsters, they are essential to Internet sales, as they benefit from a certain monopoly (limited choice, few alternatives) and induce high opportunity costs for counterfeiters if they have to change their

service provider. In recent years, the focus has been on payment processors and express shipping companies for these reasons. Their cooperation may result in an effective sales network's disruption. Moreover, at some point the cooperation may result in a physical contact which could be crucial to identify the final real individual or "brick and mortar" company behind illegal internet sales.

24. What has been done and covered so far by payment industry and more precisely credit card companies, which have played a key role in this traffic, should be underscored. It is now possible to cooperate in order to identify and close merchant accounts. As a result, less websites accept credit card payments and owners of these dubious shops try to convince consumers to use alternative payment methods (such as bitcoins or webmoney). The RogueBlock™ IACC initiative[3] has demonstrated where the majority of money raised through sales of counterfeit is stacked. This is already a victory, as consumers are very often short-term tempted. If consumers had to unveil their identity with a Western Union or a bank wire transfer, they would think twice before buying. Education and awareness of major acquiring banks, payment service providers and credit card networks are of utmost importance.

25. FH considers that lobbying should be reinforced towards shipping companies, as online sales are always sent through express shipping companies or EMS. A solution should be found to detect and prevent repeated offenders from using these companies' services. As several millions of fake items are shipped on an annual basis, the global revenue generated by such transport companies could not be considered negligible anymore. Once again, greater awareness and cooperation should be the definite issue in order to achieve a satisfying compromise with IP owners.

V. AWARENESS RAISING ACTIVITIES

26. Finally according to laws of supply and demand, awareness raising activities should moreover focus on consumers as they may curb the offer of counterfeit by buying genuine products. FH strives to educate consumers by bringing their attention on the risks they incur for themselves on illegal websites.

27. In addition, FH has set up a decoy website (http://replicaswisswatch.com/) which seems at a first glance to be a website selling fake watches but turns into a prevention message after a few seconds. The message focuses on the risks incurred when a fake watch is ordered. For instance, criminals behind the fraudulent website have access to buyer's personal details, including name, address and credit card details and this information could also be collected and reused for criminal purposes (identity theft, credit card abuse, etc.). Other issues may be discussed such as links with other criminal activities and money laundering.

28. There is still a lot to do in this matter as consumers are often tempted by counterfeit items even if they have the choice not to buy such illegal items.

[3] http://www.iacc.org/online-initiatives/rogueblock.

VI. CONCLUSION

29. In its daily fight FH considers that there is no definitive solution. As the Internet is under constant evolution, persistence is needed in order to follow fraudsters that today still stay one step ahead. A global approach is required, and FH approaches from several angles at the same time.

30. Things may change in the future. Cooperation between stakeholders (public / private) is the definitive way in order to develop a comprehension of the phenomenon by promoting and sharing information, intelligence, best practices, expertise and experiences as well as to create an environment to change opinions and stimulate greater respect for IP rights. There is an urgent need to enhance the emergence of a set of global Internet “soft law” enforcement rules as criminals are masters in knowing how to get past the rules.

[End of document]