Good brought by social media quickly being outweighed by the negative

Global IP

By Doris Estelle Long

Doris Estelle Long is the president of Doris Long Consulting, specializing in U.S. and international IPR and information security issues; a screenwriter and producer for VeraKen Productions; and a law professor emeritus at The John Marshall Law School. She has served as a consultant on IPR issues for diverse U.S. and foreign government agencies, including as attorney adviser in the Office of Legislative and International Affairs of the USPTO. She can be reached at prof.doris.long@gmail.com.

Posted March 22, 2016 3:04 PM

In the race between technology and intellectual property, the Internet of Things has become to information security what social media is rapidly becoming to e-commerce: Both present an opportunity for commercial growth where the benefits are many and the risks to intellectual property owners may be even greater.

With the Internet of Things, a fully connected residence offers a level of convenience unparalleled in human history. Your refrigerator can let you know when you run out of milk. Using your favorite social media's new online retail services, it can then send a personal message requesting delivery.

Unfortunately, this convenient digital exchange of information also increases the likelihood that unwanted observers, including hackers and identity thieves, will have access to such personal information.

You may not care if others know your milk drinking habits. However, other data that flows over the IoT, including health and financial information, is a different matter.

The ability to hack the IoT raises what may become the new horror genre of the 21st century — murder by hacking. I have no doubt someone in Hollywood is already crafting a script where inhabitants are murdered by their IoT-powered home because a psychopath has hacked the system. This threat is pure fiction. By contrast, the possibility that social media will become an impenetrable market for counterfeit goods is already becoming an undeniable reality.

Prohibiting trafficking in counterfeit goods has long been an area of international concern. Even the Agreement on Trade-Related Aspects of Intellectual Property Rights, or TRIPS, required special border control measures against the importation of

Yet similar to copyright piracy, the digital environment has proved to be a bonanza for trademark counterfeiters. Unfortunately, present legal mechanisms to combat the problem remain woefully inadequate internationally.

There is no international instrument that prohibits the exportation of counterfeit goods. Many countries have become manufacturing hubs for counterfeiting. So long as these manufacturing activities occur in free-trade zones, or the counterfeit goods are exported and not sold locally, counterfeiters generally can operate with impunity.

Currently, no effective mechanism exists for reducing the proliferation of websites selling counterfeit goods. Domain name and website seizures are popular tools for removing the source of counterfeit goods from the Web. Yet neither effectively prevents the resurgence of such sites under fake names because there is no current international obligation that applicants register using their true identity. To the contrary, the number of counterfeit sites owned by “Mickey Mouse,” or other fictitious characters, is legion.

The intractability of counterfeiting, however, is not due strictly to the lack of international legal mechanisms. Like digital piracy, consumers knowingly buy counterfeit goods because they want the goods but do not want to pay the market price for them. Luxury goods, such as purses and watches, are at the greatest risk because local enforcement efforts are so lax.

In the absence of a perceived threat to public health or safety, local police often refuse to enforce laws against counterfeiting. In fact, bazaars specializing in counterfeit goods actually have a police presence to ensure the safety of their customers in countries as diverse as Peru, China and Russia.

The use of social media messaging as a new basis for commercial transactions threatens to turn this already unfortunate situation into a global disaster. Twitter, Facebook and Snapchat, among others, already offer, or have announced plans to offer, private messaging services between businesses and users as part of a new online retail service.

These private messages could not be easily monitored by mark owners to uncover trade in counterfeit goods. There is no present legal obligation on social media sites to provide such monitoring services or otherwise establish programs assuring that only authorized goods are sold to their users using these new retail systems.

Despite the generally bleak picture for trademark owners, there are recent signs of improvement internationally. A blocking injunction was issued in London last month in *Cartier International v. British Telecommunications PLC* that prohibited five identified online service providers from allowing their users access to identified sites offering counterfeit luxury goods, including montblancebay.com.

These developments are significant because they were taken against websites for which enforcement has long been indifferent, at best, because their proffered goods pose no health or safety threat. Yet even these developments do not provide the international platform necessary to meet either present enforcement needs or future demands posed by the increasing use of social media for commercial transactions.

We are well past the time when prohibitions against the exportation of counterfeit goods, including goods in transit, should be included as a required border measure against counterfeiting. Article 16 of the aborted Agreement on Trade in Counterfeit Goods provides a good starting place, requiring border control over “imports and exports.” But such prohibition should go further and specifically require the application of such restraints to goods “in transit” and in free-trade zones.

We also need an international accord among domain name registrants requiring true name and address registrations for those running commercial sites. Failure to provide such information should result in an automatic block placed on the domain name and the site in question.

Finally, a mechanism allowing for the rapid removal of counterfeit goods from digital commerce must be developed. It is time to apply to trademarks the lessons learned from the various models developed internationally to combat digital piracy. With social media providing even more challenges to protecting consumers and mark owners against the damaging harm of trademark counterfeiting, the clock is ticking. The time for action is now.