Canadian Anti-Counterfeiting Network | Réseau anti-contrefaçon canadien

October 15, 2016

National Cyber Security Directorate
13th Floor, 340 Laurier Avenue West
Ottawa, Ontario
K1P5K3

RE: Federal Consultation on Security and Prosperity in the Digital Age
Proposal for a New Federal Office of Counterfeits, Piracy and Fraud

Thank you for the opportunity to participate in the federal consultation on cybersecurity. The consultation is most welcome and comes at a critical time.

The Canadian Anti-Counterfeiting Network (CACN) is a coalition of individuals, businesses and associations that have united in the fight against counterfeiting, fraud and copyright piracy in Canada and abroad. CACN helps prevent the critical and growing problem of intellectual property crime in Canada by raising public awareness, advocating for legislative change, offering training and engaging with law enforcement and government on counterfeiting and piracy issues.

Building a Safe and Resilient Canada

As the consultation document notes, rapid changes to digital technology are having far reaching security, economic and social impacts. The global economy and e-commerce have made combating intellectual property theft a complex and ever changing problem.

Over a decade ago, counterfeit goods were limited in volume and variety – but today, they have escalated to unprecedented levels. Counterfeit and pirated products extend from children's toys, electrical products, automobile and aircraft parts to pharmaceutical products, food and beverages to software, DVDs and media streaming, and luxury goods of all kinds. Many of these illegal products sold online and in retail chains pose a serious threat towards consumer health and safety. Intellectual property theft, counterfeiting and piracy undermine legitimate businesses, depriving these innovative companies of revenue and negatively impacting the millions of people whose jobs in Canada and around the world depend on these vibrant industries.

Security and Prosperity in the Digital Age

We strongly endorse the action areas for more "Cooperation and Capability" and a robust and comprehensive "national cybercrime coordination center to triage, prioritize, and coordinate cybercrime investigations."

Year-over-year, the RCMP has reported a steady increase in the importation and availability of counterfeit goods, which has impacted almost every industry from pharmaceuticals to technology. From alcohol, contact lenses and cosmetics, to computers, medicine, toys and batteries, counterfeit products are readily accessible and putting Canadians in harm's way.

In an effort to protect Canadian innovators, consumers and legitimate businesses from the increasing harms of online piracy, counterfeit goods and illegitimate sites, and to keep pace with rapid technological change, the following is an outline of a proposed federal office to protect Canadians from harmful online piracy, counterfeits and fraud.

The proposed Office of Counterfeit, Piracy and Fraud

The proposed office would be an ongoing rapid response and coordination mechanism against counterfeits, piracy and fraud. The office would provide a space for the Canadian public and industry to collaborate and coordinate with the federal government. It would put Canada in line with its major trading partners including the United States and United Kingdom.

Specifically, the office would protect Canadian consumers, science and innovators with:

1. **Intelligence**
   Identifying the problem in real time – an open federal office to allow the public, rights holders, trade associations, law enforcement and government agencies to report and identify problems in real time. A focused federal office to gather data and focus efforts on real time threats.

2. **Rapid response & enforcement**
   Coordinating a rapid federal response and law enforcement to ensure public safety, the protection of innovators and creators, and a healthy economy by ensuring Canadian consumers can trust the security of online transactions.

3. **Education**
   Lay the foundation for partnerships between industry and law enforcement agencies to provide education among them and to the public through readily available training and timely public service announcements about real time harms and threats to public safety.

Why do we need a new federal office?

Digital trade and commerce is rapidly transforming the Canadian economy, and yet there is currently no effective, accountable, and timely government mechanism to combat the growing problem of online counterfeits and piracy. There is no simple and easy access or entry point for the public or private sector to highlight real-time problems and no clear co-ordination between departments.

Responsibility for counterfeit goods and piracy in Canada is divided amongst many federal departments, including Public Safety, Industry, Health, Finance and the RCMP. In this climate, crime and fraud is allowed to proliferate to the detriment of Canadian science and innovation, the safety and security of Canadians, and the economy at large. For example: The National Anti-Counterfeiting Bureau (NACB) is part of the RCMP's National Police Services providing two areas of expertise: counterfeits (banknotes) and documents (fraudulent legal documents). Its mandate does not include counterfeit goods, piracy or fraud.

Internet security experts warn that pirate sites can severely infect computers and devices, render the user vulnerable to spam, viruses, malware or phishing attacks, and are unsafe for consumers – used to steal personal information such as e-mail addresses and passwords. These pirate sites also pose significantly greater risks of harming consumers and undermining the general security and stability of the Internet ecosystem due to malware. A recent study found that one out of every three piracy websites contains malware and that 45 percent of malware is delivered by "drive-by downloads," which invisibly download malware onto a consumer's computer without the consumer even clicking on anything. Malware on rogue websites represents a clear and present danger to Canadians, who are often children.

The goal of the office

The goal of the proposed office would be an ongoing rapid response and coordination mechanism against counterfeits, piracy and fraud. The office would provide a space for the Canadian public and industry to collaborate and coordinate with the federal government. Technology, tactics and methods change quickly on the internet, and the government requires an ongoing collaborative dialogue with industry to have first-hand knowledge of the issues they face in order to develop strategies to help combat those challenges.

The office would be a means for collaboration and partnerships between government and business, and amongst government departments. Both types of coordination are needed to combat sophisticated fraud in the online environment. Canadian companies are also developing and adapting to emerging technologies and can advise the government on the changing conditions in which they operate. An office will allow the government to implement tangible and timely measures to combat online pirates and counterfeiters and advocate new best practices to protect Canadians from cyber incidents eroding their trust in the security and safety of online transactions.

International Examples

United States - National Intellectual Property Rights Coordination Center (IPR Center)

The U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) led National Intellectual Property Rights Coordination Center (IPR Center) stands at the forefront of the United States Government's response to global intellectual property (IP) theft and enforcement of its international trade laws. The mission of the IPR Center is to ensure national security by protecting the public's health and safety, the U.S. economy, and to stop predatory and unfair trade practices that threaten the global economy. To accomplish this goal, the IPR Center brings together 23 partner agencies, consisting of 19 key federal agencies, Interpol, Europol and the governments of Canada and Mexico in a task-force setting. The task force structure enables the IPR Center to effectively leverage the resources, skills, and authorities of each partner and provide a comprehensive response to IP theft. The IPR Center is led by an ICE-HSI Director with Deputy Directors from HSI and U.S. Customs and Border Protection (CBP).

United Kingdom – Action Fraud National Fraud & Cyber Crime Reporting Unit

In the UK, the National Fraud Intelligence Bureau (NFIB) sits alongside Action Fraud within the City of London Police which is the national policing lead for fraud.

The NFIB takes all Action Fraud report and uses millions of reports of fraud and cyber crime to identify serial offenders, organised crime gangs and established as well as emerging crime types.

The NFIB gets it data through three main channels:

1. Reports from individuals and small businesses (coming either directly or via a police force) made to Action Fraud on the phone or online.
2. Fraud data from industry and the public sector which includes banking, insurance, telecommunications and government departments.
3. A variety of intelligence sources including, but not limited to, national and international police crime/intelligence systems.

Thank you again for the opportunity to make the case for a new Canadian office on counterfeit, piracy and fraud. The office is equally supported by Canada Goose, Music Canada, the Retail Council of Canada, the Motion Picture Association – Canada, CIBC, Facebook, and the CSA Group.

Best regards,

Sundeep Chauhan, B.A., J.D., C.S

Certified Specialist
(Intellectual Property: Copyright)

on behalf of the Canadian Anti-Counterfeiting Network