

Robust consumer protection laws needed to close internet loopholes

June 15 2010



(PhysOrg.com) -- Governments the world over must do more to safeguard internet shoppers from 'rogue' traders and their online scams, a new study from Queen Mary, University of London suggests.

Entitled International Frameworks and Powers for Enforcing [Consumer Protection](#) over the Internet, the research report, commissioned by the Department of Business Innovation and Skills (BIS), is intended to inform UK government policy on online consumer protection.

Research authors, Dr Julia Hörnle and Professor Ian Walden, both members of the Institute of Computer and Communications Law in the

Centre for Commercial Law Studies at Queen Mary, interviewed 16 enforcement agencies, policy-makers, police agencies, consumer bodies and consumer dispute resolution bodies in seven other countries, including the US, Canada, the Netherlands and Austria, to learn how they are cracking down on internet fraud and protecting consumers online.

“In our research,” says Dr Hörnle, “we found few examples of new ‘internet’ legislation specifically geared towards consumer protection in foreign countries. Such enforcement powers have been given to the police and public prosecutors, in the context of the criminal law, but not yet to consumer protection authorities.”

The researchers also noted that, despite having powers, the police in many countries rarely act in consumer protection cases. “This means many online scams, such as ‘phishing’ and ‘spyware’ fall between the gaps of consumer protection and criminal law - in other words, the ‘rogue’ traders are getting away with it,” warns Dr Hörnle.

“One of the main challenges for protecting consumers online is that the scammer and the consumer may be located in two different countries,” explains Professor Walden. “Online [fraudsters](#) may try to escape law enforcement by systematically targeting consumers in another country.”

For this reason, Julia Hörnle and Ian Walden point out, law enforcement mechanisms cannot be limited to prosecuting ‘rogue’ traders. Combating online fraud requires the co-operation of service providers such as search engines, hosting companies and payment providers, whose services are often abused by unscrupulous criminals.

More international collaboration between those government authorities fighting [internet fraud](#) is, according to the study, also vital to improve consumer protection; this includes data collection through consumer

complaints websites and the sharing of complaints data.

The research authors cautioned, however, that such information sharing raises privacy and data protection concerns which must be addressed, not to mention the cost implication of implementing such law enforcement mechanisms.

“There is certainly a need to balance the investigative and enforcement powers of consumer authorities with the interests of providers and internet users,” acknowledges Professor Walden.

The internet enables businesses to reach a large, international audience at low costs of market entry; this, the study says, in turn enables rogue traders to launch scams and deceptive and fraudulent practices by the same means.

Although the harm suffered by individual victims of these internet scams may be small, resulting in such losses being written off, the study concludes that the cumulative losses can be enormous, which demands that effective enforcement action be taken.

Furthermore, it is important, says Dr Hörnle, to empower consumers themselves to seek redress against ‘rogue’ traders operating between countries. Court procedures across borders are notoriously slow and expensive, so the study recommends affordable alternative dispute resolution (ADR) systems for internet cases.

“It may be too expensive for individual consumers to go to court; therefore, it is important that the cost is spread, for example by consumers joining a group collectively going to court,” adds Dr Hörnle.

More information: According to separate research carried out in January 2010 for the Office of Fair Trading (OFT), about two million

adults in the UK have responded to scams, most commonly those sent by email, in the previous 12 months. Around 49 per cent of scam victims lost more than £50, while five per cent of victims lost more than £5,000.

Provided by Queen Mary, University of London

Citation: Robust consumer protection laws needed to close internet loopholes (2010, June 15)
retrieved 3 May 2024 from

<https://phys.org/news/2010-06-robust-consumer-laws-internet-loopholes.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
--