

A video on Policing Cyber Crime: In practice

University of Southampton, ECS, INFO2009 Academic Year 10-11

Keywords

Cyber, Crime, RIPA, Regulation of Investigative Powers Act 2000, DEA, Digital Economy Act 2010, ISP, Internet Service Provider, Police, Encryption, Data Logging, e-fraud

Abstract

Our project considers the issues and acts relevant to **cyber crime**. We focus particularly on the **Regulation of Investigative Powers Act (2000)** and the **Digital Economy Act (2010)** as these recent laws will affect internet users as they have certain implications arising from their use, such as **privacy** concerns and **freedom of speech**. We find that there are conflicting views dependent upon who is affected by these acts such as **ISPs** and the **police**.

Introduction and Method

We decided to investigate how certain acts related to cyber crime affect the **IT industry**, **UK internet users** and **authorities** in practice. **Cyber crime** includes **attacks on computer systems (hacking)**, **content-related crime** such as **child pornography** and traditional crimes such as **fraud/theft** carried out on **computers**. After researching various acts, we found the following to be relevant to policing **cyber crime**: **Regulation of Investigatory Powers Act (2000)**, **Digital Economy Act (2010)**, **Computer Misuse Act (1990)** and **Sexual Offences Act (2003)**. We decided to focus on the **Regulation of Investigatory Powers Act (2000)** and the **Digital Economy Act (2010)**. We arranged, planned and carried out **structured interviews** to get **contrasting viewpoints** on how to police **cyber crime**. We travelled to **Bristol** to meet **face to face** with a **former detective**. In addition, we made contact with the owner of a **local ISP** in **Bracknell** to find out how these acts affect their **procedures** and what they consider to be the **main issues**.

Background Information

Regulation of Investigatory Powers Act (2000)

This act provides a **lawful procedure** to govern the way **authorities** carry out **surveillance** on people (Home Office, 2000).

RIPA is designed to **regulate** the use of **covert interception** and **surveillance** of **electronic data** in the **UK**. It also gives people a right to take **legal action** if their **communications** are **intercepted** without **"lawful authority"**

(Cambridgeshire County Council, 2006). The act was mainly introduced to **enhance national security** and **crime detection**; it plays an important role in **combating criminals online** (Chang et al., 2003)

RIPA covers many aspects of the surveillance laws. It contains **five parts**...

Act parts:

- Part I** The interception of communications and the acquisition and disclosure of communications data,
- Part II** The use of Surveillance and Covert Human Intelligence Sources (informants and undercover officers)
- Part III** Covers the Investigation of Electronic Data protection by encryption
- Part IV** A Framework for Scrutiny of Investigatory Powers
- Part V** Covers miscellaneous and supplemental matters such as consequential amendments, repeals and interpretation (Interference with Property & Wireless Telegraphy) (UK Legislation, 2000)

Digital Economy Act (2010)

DEA is a recent act which **regulates** the **digital media** industry by placing **obligations** on **ISPs** in order to tackle **online copyright infringements**, such as **illegal peer-to-peer sharing** and **downloading of copyright material** (The UK Statute Law Database, 2010).

The act puts more **responsibilities** onto **ISPs**. If they fail to provide the infringer's **IP addresses**, they can be **fined up to £250,000** (JISC Legal, 2010). The **DEA** is compatible with **The Copyright, Designs and Patents Act (1988)** (JISC Legal, 2010).

Currently, this act is only **applicable to large ISPs**. **DEA** will have a **judicial review** in **February 2011** (BBC, 2010) as two of the largest UK **ISPs**, **Talk Talk** and **BT**, claim the act was **'rushed through'** **parliament** without consulting **ISPs** first. Another **controversiality** is the **accuracy** of the act; it supposedly will **result in invading the privacy** of **law-abiding citizens**.

Discussion and Conclusions

Enforcing **RIPA** and **DEA** in practice is not straightforward. We found that **policing authorities** feel they need **greater control** with **less restrictions** in order to police **cyber crime** efficiently. But these acts are enforced in such a way that **passes responsibility** down to **internet service providers**. There could be a **regulating body** for the **internet** but given the vast content and amount of communication this is an almost **impossible challenge**. Additionally there are **conflicting interests** with the **Human Rights Act (1998)**, such as **freedom of speech** and the **European Convention of Human Rights**, in particular **section 8**, which provides one's **"private and family life, his home and his correspondence"** to be respected.

ISP

We held an e-interview with **Adrian Kennard**, the founder of **AAISP**, a local **ISP** based in **Bracknell** which has a presence in many **UK data centres**.

The company was formed in **1997**, before **RIPA** and the **DEA** were passed by parliament and have had to adapt their processes to be compliant. They are conscious of **protecting** their customers' **privacy** and **rights**.

<http://www.aaisp.net>

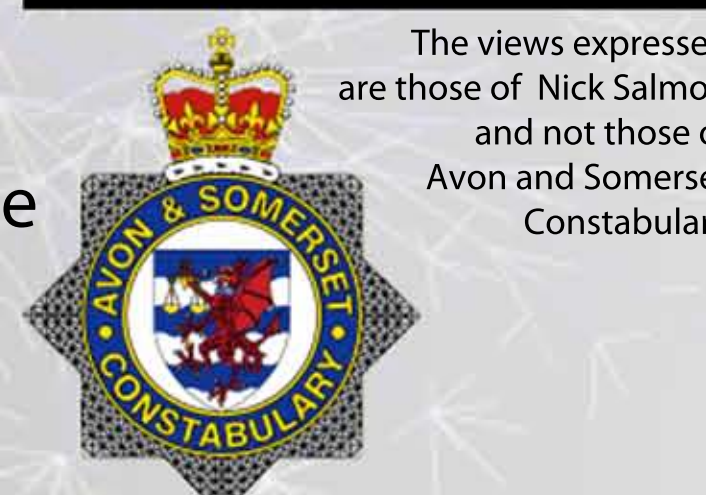


“Puppets of a police state”

Former Detective

We held a **face-to-face** interview with **former detective Nick Salmon** of **Avon and Somerset Constabulary**.

For the last 5 years, he has dealt with serious crimes in **Bristol** including **murder**, **rape**, **bomb incidents**, **fraud** and **cyber-crime**. He now works for a company called **Mitie** who provide security for **Rolls Royce** and is in charge of **security** at **Rolls Royce's** in **Bristol**.



“The internet gives freedom but it comes at a price”

Group 7



Nick Hatter Matt Tucker

Tsang Tze Kin James Acres

Maraim Masoud

We are **Group 7** (tutor group im), the producers of this poster and resource.

Our tutor is:
Dr. Ivan Markovsky: im@ecs.soton.ac.uk

Our members are (pictured above):
James Acres: ja9g09@ecs.soton.ac.uk
Nick Hatter: nh4g09@ecs.soton.ac.uk
Tsang tTze Kin: tkt1g09@ecs.soton.ac.uk
Maraim Masoud: mr17g09@ecs.soton.ac.uk
Matt Tucker: mt9g09@ecs.soton.ac.uk

We would personally like to thank **Adrian Kennard** (founder of **AAISP**) as well as **Nick Salmon** (former detective) for taking time out of their busy schedules to share their views and knowledge with us.

Background image:
http://en.wikipedia.org/wiki/File:Internet_map_1024.jpg

Access our Resources

Access all our resources from EdShare at:
<http://www.edshare.soton.ac.uk/6403/>

Access our primary video resource at:
<http://www.youtube.com/cybercrimeuk>

Primary resource is a video providing an introduction to how cyber crime is policed. The video contains the 'best bits' from an interview we carried out with former detective **Nick Salmon** and also an acted audio version of the 'best bits' from our email interview with **Adrian Kennard**, the founder of **AAISP**.

Access the interviews in full:
Full transcript of interview with **Adrian Kennard**, founder of **AAISP**:
<http://www.edshare.soton.ac.uk/6403/>

Full video interview with former detective **Nick Salmon**:
<http://www.edshare.soton.ac.uk/6403/>

References

- 1-Cambridgeshire County Council(2006).Regulation of Investigatory Powers Act 2000. availale at: <http://www.cambridgeshire.gov.uk/NR/rdonlyres/F26FAB45-2EAE-460F-B061-BCF1A86DAD95/0/RIPAGuidance.pdf>
- 2-Chang, W. Chung, W. Chen, H. Chou, S. An International Perspective on Fighting Cybercrime, In Proceedings of the 1st NSF/NIJ conference on Intelligence and security informatics (ISI'03). USA, 2003, Berlin, Heidelberg: Springer-Verlag, pp 379-384. available at: <http://portal.acm.org/citation.cfm?id=1792094.1792138>
- 3-Home Office, 2000, The Regulation of Investigatory Powers Act (RIPA). available at: <http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/> [accessed on 6 December 2010]
- 4-UK legislation (2000).Regulation of Investigatory Powers Act 2000. available at: <http://www.legislation.gov.uk/ukpga/2000/23/contents>
- 5-BBC, 2010. Net providers get Digital Economy Act judicial review. available at: <http://www.bbc.co.uk/news/technology-11724760> [accessed on 8 December 2010]
- 6-JISC Legal, 2010, The Digital Economy Act 2010 - Implications for UK Colleges and Universities. available at: <http://www.jisclegal.ac.uk/Portals/12/Documents/PDFs/DEA%20Guidance.pdf>
- 7-The UK Statute Law Database,2010, Digital Economy Act 2010. available at: <http://www.statutelaw.gov.uk/content.aspx?activeTextDocId=3699621> [accessed on 8 December 2010]