Computer Abuse Legislation: A Trap for the Unwary?

Huw Fryer
Web Science DTC
Electronics & Computer Science
University of Southampton
hf1g10@ecs.soton.ac.uk

Sophie Stalla-Bourdillon
ILAWS
Faculty of Business and Law
University of Southampton
S.Stalla-Bourdillon@soton.ac.uk

Tim Chown
WAIS Group
Electronics & Computer Science
University of Southampton
tjc@ecs.soton.ac.uk

ABSTRACT

The Computer Misuse Act is the primary law in the UK for computer crime. Its provisions are broad and have yet to be clarified by case law, in a way which could cause problems for a researcher. This paper describes the Act, and analyses some of the possible consequences for researchers.

Categories and Subject Descriptors

K.4.1 [**Computing Milieux**]: Public Policy Issues—*Abuse and crime involving computers*

1. BACKGROUND

Estimates as to the effects of cybercrime on the Web vary wildly. As an example, the report commissioned by the UK Cabinet Office from Detica as to the cost of cybercrime estimated the annual cost to the UK as high as £27bn[4], some 1.8% of GDP. Anderson et al. by contrast declined to provide a firm estimate of overall cost due to insufficient data being available, though they did estimate that the figure was likely to be considerably less than that in the Detica report[2]. In a more technological sense, the Spoofer project[1] from MIT estimated IP spoofing was possible in 23% of networks; whereas only the annual Trustwave survey consistently has a far lower number[2].

A lot of the data about cybercrime comes from surveys, which have their own set of difficulties for extrapolating results. Florêncio & Herley presented a strong assessment of cybercrime surveys, as being "so compromised and biased that no faith whatever can be placed in their findings"[5]. Amongst the difficulties was the difficulties from the concentration of the victims in the population, and the concentration of the losses within the victims requiring survey sizes to be massive in order to ensure a reasonable degree of statistical accuracy. In addition, the tendency for inaccuracies in self-reported figures, and our inability to check the accuracy of responses cast further doubt on the validity[5]. These weaknesses, they argue, have led to many survey results being potentially an order of magnitude out.

Despite their limitations, a survey can arguably provide some insight into the problem. Nevertheless, a Web Science researcher should seek other, more objective methods of research in order to provide evidence for how much faith can be placed in these surveys. This may occasionally require participants to be misled and either obtain retrospective consent if it's possible, or not if it isn't. Whilst this is a strategy which is occasionally required in other more traditional disciplines, in activity related to the Web care needs to be taken to not fall afoul of computer misuse legislation, since interfering with data on someone's computer is an offence in most countries. This paper will provide an outline of some of the issues relating to the Computer Misuse Act in the UK, and things a researcher should consider before conducting an experiment.

2. COMPUTER MISUSE LEGISLATION

The CMA is based around the notion of "Unauthorised Access", with s1 providing as follows:

1. A person is guilty of an offence if
   (a) He causes a computer to perform any function with intent to secure access to any program or data or enable such access to be secured
   (b) The access he intends to secure... is unauthorized
   (c) He knows at the time... that that is the case

This is designed to be interpreted in an extremely broad fashion as illustrated by the interpretation guide in s17. S17(2)(d) provides that data is accessed "has it output from the computer in which it is held (whether by having it displayed or in any other manner); ", and s17(4)(b) provides that "the form in which any such instructions or any other data is output... is immaterial". As such, this would suggest that visiting a website is in itself securing access, and therefore without the owner's consent then one would be committing a s1 offence under the CMA. In order to ascertain whether visiting a website would be contrary to s1

[1] `http://spoofer.cmand.org/`

[2] IP packets have a source and destination address, so the response to a request can go back to the source. By spoofing the source, it is possible to mount a denial of service attack by sending unwanted traffic to a victim

CMA, the nature of what exactly constitutes "unauthorised" in this context needs to be examined.

Early case law, before the common use of the Web established some grounds for unauthorised access, the leading case being *R. v Allison* which emphasised that it is possible for an employee to exceed their authority, even if they are technically allowed to in the course of their job. This would exclude an attack on the database of a website, since, even though it is governed by permissions indicating who can view what, attacking it to bypass the password protection (for example, in an attack like SQL injection) would clearly be exceeding authority. A website is governed by Internet protocols, which facilitate an implied level of consent. A browser makes a request to the server, and it returns content along with a status code. If the request is ok, it will return the content and a status code of 200, and if not it will return a 403 status code and a **Forbidden** message. Some case law suggests that it is slightly more complicated than reliance on the protocols, however.

D.P.P. v Lennon[1] concerned a disgruntled (former) employee who crashed the mail server of his former boss by sending a mail bomb[3]. At first instance, it was held by the magistrate that there was no case to answer, since an email server was designed to receive email. On appeal Keene LJ held that they had erred, and that whilst there was consent to receive emails, they would not have consented if asked whether they could receive 500,000 emails simultaneously and likened it to a householder not consenting "does not consent to a burglar coming up his path [or] having his letter box choked with rubbish"[1]. At around the same time, the magistrate's court in *R v Cuthbert*[6] reached a different decision. This case concerned a security professional who was concerned about whether he had been victim of a phishing attack following a donation to the DEC, so he attempted a directory traversal attack to see if he could discover if it was a phishing site or not. He appended `../../../` which causes the page requested to go "up" three directories into the underlying directory structure, and was found guilty under s1.

Whilst the limit to consent from *Lennon* is sensible, we are still left in some doubt as to what exactly the limit to consent is. *Cuthbert* has no legal precedence, because it was only a magistrates court decision, but it does show the willingness of the CPS to prosecute in these sort of cases. This might be simply theoretical, and the CPS might make a different decision nine years later, but uncertain law can have an unfortunate impact as some cases in the USA have shown. In January 2013 Aaron Swartz committed suicide whilst facing charges relating to computer fraud and wire fraud for writing a script to bulk download journals from the JSTOR repository. Following his death, a bill was proposed to limit the scope of the Computer Fraud and Abuse Act (CFAA)[3]. Another case was that of Andrew Auernheimer who was found guilty under CFAA for downloading customers' email addresses from an unprotected Web page causing AT & T to close the security hole which made this possible. This was recently overturned on appeal, but the court chose – despite the importance of the issues – to ignore them and decide it on the safer option of "venue"[7]

[3]This case would now be tried under s3A CMA, which now makes impairment of a computer an offence following the Police and Justice Act 2006

3. IMPLICATIONS FOR RESEARCHERS

The fear relating to broadly defined laws in this area is usually more of an issue to security researchers who risk prosecution, but does apply to Web scientists as well. Web Science is not solely concerned with the thoughts and feelings of people on the Web, but on the implications or impacts of certain behaviours on the Web in particular in relation to cybercrime. The lack of data which exists in order to validate (or not) survey results means that more direct research is occasionally needed, which could have a danger of contravening the CMA. For example, in attempting to screen scrape a website where the `robots.txt` file doesn't grant permission[4] could be considered unauthorised. Similarly, the connection between malware and cybercrime might lead a researcher to consider what exactly makes the research possible. Investigating to what degree servers are configured correctly could involve making requests to publicly accessible but hidden pages. The recent "heartbleed" scare led to many researchers performing scans on popular websites, for example `https://zmap.io/heartbleed/`, to see how many had patched the vulnerability. Whilst clearly not malicious, performing a public service, and obtaining relevant data, could attempting toexploit an OpenSSL vulnerability really be considered consistent with the CMA?

Generally speaking, these provisions are unlikely to pose a problem to a researcher as long as they are aware that they exist. Yet, as the Auernheimer case shows, judges are not inspiring confidence about their understanding by sidestepping the important issues relating to computer misuse. A risk averse institution could conceivably decide not to back a researcher where laws might be broken, so it is important that researchers are aware of the limits of these laws (as much as possible) so as to be able to argue that their research should be permitted (and not end up in jail).

4. REFERENCES

[1] *DPP v. Lennon*. [2006] EWHC 1201.

[2] R. Anderson, C. Barton, R. Böhme, R. Clayton, M. van Eeten, M. Levi, T. Moore, and S. Savage. Measuring the cost of cybercrime. In *WEIS*, 2012.

[3] BBC. M.i.t consults staff and students over aaron swartz probe. `http://www.bbc.co.uk/news/technology-21182107`, 2013.

[4] Detica. The cost of cyber crime, 2011.

[5] D. Florêncio and C. Herley. Sex, lies and cyber-crime surveys. In *Economics of Information Security and Privacy III*, pages 35–53. Springer, 2013.

[6] J. Oates. Tsunami hacker convicted. `http://www.theregister.co.uk/2005/10/06/tsunami_hacker_convicted/`, 2005.

[7] L. Vaas. Notorious troll and hacker weev has conviction overturned. http://nakedsecurity.sophos.com/2014/04/15/notorious-troll-and-hacker-weev-has-conviction-overturned/, 2014.

[4]See `http://www.robotstxt.org/` for details about the protocol