Home Office

The nature of online offending

Explored from Crown Prosecution Service case files

Research Report 82

Clare Sutherland and Samantha Dowling

October 2015

Acknowledgements

With thanks to the following for their helpful comments and contributions: *Richard Milner, Anthony Madison, Esther George, Andy Feist, Rob Street, Sam Brand, Ian Caplan, Kathryn Roe, Mike Warren, Lorrah Achato* and *Dr. Alice Hutchings*.

With thanks also to the Economic and Social Research Council (ESRC). The first author was funded by an ESRC Student Internship [ES/I021051/1]. Clare Sutherland is currently completing a PhD at the Department of Psychology at the University of York.

Contents

Table of Contents

Disclaimer: 'The views expressed in this report are those of the authors, not necessarily those of the Home Office (nor do they represent Government policy).'

Summary

Aims and methodology

Evidence regarding online offenders is limited and there are key gaps in knowledge around offender demographics, backgrounds and criminal careers. However, online offences and offenders are not easily identified through traditional data sources such as police recorded crime. This report therefore aims to help build understanding of online offenders and the nature of their offending by outlining findings from an analysis of case files held by the Crown Prosecution Service (CPS). The research involved analysis of offences prosecuted and convicted under the Computer Misuse Act 1990 (CMA); the Fraud Act 2006; s.127 of the Communications Act 2003 (CA); and the Malicious Communications Act 1998 (MCA).[1] Random samples of cases were taken in December 2012 to explore:

- the proportion of cases that could retrospectively be identified as committed online; and
- the information that was held in those online cases regarding the characteristics of offenders and the nature of their offences.

Further details of the methodology are outlined in **Section 2** and **Annex A.**

Findings

What is the proportion of cases committed online?

The researchers excluded two-fifths of cases from the analysis because of insufficient usable data available in the files. This resulted in a total of 205 usable cases that could be analysed across all four Acts. **Overall, 25 per cent of all usable cases were committed online and had resulted in a conviction**. Analysis of the usable cases falling under the different Acts found that: **20 per cent of Fraud Act cases, 14 per cent of MCA cases and 6 per cent of CA cases were committed online and resulted in a conviction.** All CMA cases were committed online, but just 62 per cent held usable data for analysis and resulted in the offender being found guilty.

It is difficult to draw inferences about the extent of online offending from the limited pool of cases that reach prosecution and conviction. The small numbers identified in Table 1 do not immediately suggest overwhelming numbers of crimes committed online, but there are several limitations regarding the scope and generalisability of the analysis, which means the numbers identified are likely to be an underestimate. Limitations are detailed further in **Section 3.1** and **Annex A**, but include the following.

- **Many of the CA and MCA cases either held minimal information, which meant that they could not be analysed; or were no longer available in electronic format.**[2] This

[1] This became a notifiable offence from April 2016. Previously, it was a non-notifiable offence.

[2] Where case files are unavailable in electronic format, they are still retained in hard copy. However, due to time constraints the

markedly reduced the number of usable cases available and is likely to have introduced some bias.

- **These cases give some insight into the nature of cases dealt with by the CPS, but do not necessarily reflect all online crimes initially reported to police.** It is not possible to infer from this research the characteristics of cases originally reported to the police by victims, or by the police to the CPS (or those cases that were still 'live'). It is quite likely that the process of attrition from the initial offence to CPS involvement is not uniform.
- **These cases do not reflect those dealt with by the National Crime Agency (NCA),** or in previous years by the Serious Organised Crime Agency and the Police Central e-Crime Unit (both of which are no longer in existence and have been replaced with the NCA). The cases referred to in this research are dealt with by local police and so tend to represent less complex and/or less serious crimes.

Table 1. Number of cases analysed under the four Acts

No. of unique cases	**Computer Misuse Act** (2011–2012)	**s. 127 Communications Act** (2011–2012)	**Malicious Communications Act** (2011–2012)	**Fraud Act** (Q4 2012)	**Total cases**
Sample	37 (all)	100	100	100	337
Usable cases	25	36	50	94	205
Usable online cases	25	3	7	19	54
Usable guilty online cases	23	2	7	19	51

What are the characteristics of online offenders and their crimes?

- Demographics:
  - **the majority of offenders were male** (across all four Acts);
  - age (at the time of the offence) ranged from **17 to 62 years**, but on average offenders were fairly young (30 years old);
  - most were **British and White;** and
  - **spanned a range of occupations** from unemployed to managerial or professional occupations, as well as students.

- Three main motivations for online offending were apparent:
  - **financial** or other profit-focused;
  - **revenge** for losing a job; and
  - **harassment or stalking** (amongst cases under all four Acts**)**.

Other motivations include curiosity, boredom and 'for a joke'.

- Many offences were either **insider enabled** (financial/profit or revenge cases) **or the offender had been in a previous personal relationship with the victim** (harassment or stalking cases). **Most victims appeared to know and have initially trusted the offender, but (offline) circumstances had changed without a suitable online security update.**

research team were unable to consult hard copy files.

- **In most cases online criminals were reasonably, but not excessively, technically skilled, or blended social engineering[3] with their IT skills.** They were generally **motivated to offend against a specific victim** (revenge, greed) and had **an opportunity** (victim not technically savvy, not using strong passwords/security questions, not changing passwords, or not going to the police).The more technically skilled offenders tended to have a connection to computers through their studies or occupation.
- **Often, simple security measures** (for example, timely password changes, care over personal data, and quick reporting to the police) **would have stopped or minimised the impact of the crime. A key recommendation from this research is that the public be made more aware of their online vulnerability after an offline change in a trusted relationship.**
- Offenders made many obvious mistakes and often the offline–online link was strong and prosecutors commented that this helped to make a strong case. This raises questions regarding how easy it is to find, or charge, **an offender who is a stranger, overseas or is more highly skilled and careful.** Some of the traditional motivations and personal connections that are observed in 'offline' crimes would also appear to hold true for crimes committed in the online environment.
- **Strong links with online harassment/stalking were evident across a number of cases across all four Acts.** Online stalking and harassment have been documented as relatively under-researched online crime areas (for example, McGuire and Dowling, 2013).

[3] Social engineering involves the use of social skills, or tricks, by the offender to persuade or deceive victims to part with personal details, passwords, and so on.

1. Aims and context

Evidence regarding online offenders is limited and there are key gaps in knowledge around offender demographics, backgrounds and criminal careers. A traditional way of building a picture of offenders is to examine sanctions related to crime types of interest. However, neither police recorded crime nor Police National Computer (PNC) entries readily identify cyber-enabled or other online crimes. The authors therefore decided to build up an understanding of online offenders using case files held by the Crown Prosecution Service (CPS). The small numbers of offences prosecuted under the Computer Misuse Act 1990 (CMA) can be easily identified from CPS case files. However, most cyber-enabled or other online offenders will be charged under other Acts (see McGuire and Dowling, 2013). Although CPS case files do not allow easy identification of offences committed online under other Acts, it is possible to examine case files for offences prosecuted under Acts that would be expected to contain offences committed online (along with other 'offline' cases).

2. Methodology

Random samples of CPS case files were taken in December 2012 to explore:

- how many cases could retrospectively be identified as committed online; and
- what information was held in those online cases regarding the characteristics of offenders and the nature of their offences.

Following discussions with policy colleagues and the CPS, the research focused on offences under the following Acts.

- All 37 cases where individuals were prosecuted under the CMA in 2011–2012. These include offences largely relating to unauthorised access to and impairment of computer material, which make hacking, writing malware or using malware to modify computers an offence.
- A random sample of 100 cases from s.127 of the Communications Act 2003 (CA) in 2011–2012, representing around 4 per cent of all s.127 CA cases during these years. These include offences relating to the sending of grossly offensive, indecent, menacing, false or persistently annoying messages through electronic devices.
- A random sample of 100 cases from the Malicious Communications Act 1988 (MCA) in 2011–2012, representing almost 10 per cent of all MCA cases during these years. These include offences relating to sending threatening, false, indecent or grossly offensive electronic communications intended to cause distress or anxiety.
- A random sample of 100 cases from the Fraud Act 2006 in the last quarter[4] of 2012, representing around 3 per cent of all Fraud Act cases during this quarter. These include offences relating to:
  - fraud by false representation; and
  - possession and making or supplying articles for use in fraud (including electronic articles).

Online offenders were identified as those who had committed an offence either in part, or in full, through a computer, computer network or other internet-enabled device (for example, laptops, smartphones, tablets). Relevant activities included:

- sending or receiving emails;
- use of social networking sites such as Facebook, Twitter or chat rooms;
- use of forums, blogs or websites; or
- communication via online video game networks or Skype.

For more information on the methodology and details of the definitions used, see **Annex A**.

[4] For practical reasons, the fraud sample could only be taken from last quarter because of the time taken for the CPS to process the large volume of fraud cases. Further details are in Annex A.

3. Findings

This section provides a more detailed analysis of findings from this research. It sets out:

- the proportion of cases that could retrospectively be identified as committed online; and
- the information that was held in those online cases regarding the characteristics of offenders and the nature of their offences.

Key themes include:

- motivations;
- victim/offender relationships;
- insider offences;
- serious and/or 'organised' crime cases;
- offending methods;
- harm caused by the offender;
- previous offending; and
- how offenders were caught.

A final discussion considers the implications of these findings and areas for future research.

3.1 What is the proportion of cases committed online?

Limitations regarding the scope and generalisability of the cases analysed means it is difficult to draw wider inferences about the extent of online offending. Caveats to the analysis included the following.

- **Details regarding how crimes were committed (i.e. if they were online or offline) were not available for all cases, resulting in two-fifths of cases being excluded from the analysis.** Cases selected under s.127 of the Communications Act 2003 (CA) and Malicious Communications Act 1988 (MCA) tended to hold minimal information and so were subject to particularly high levels of attrition (see Table 2). This is because these cases were sampled from a longer time frame than the more numerous cases prosecuted under the Fraud Act 2006 (i.e. two years rather than a single, recent quarter). Consequently, some cases had already reached their Crown Prosecution Service (CPS) electronic destruction date – so whilst the cases would have been available at courts in hard-copy files, they were not accessible in electronic format. Limited time and resources meant that the research team were unable to undertake additional court visits to access hard-copy files. As a result this markedly reduced the available sample for CA and MCA cases and almost certainly introduced some bias in the nine cases studied in detail under these Acts (since more serious cases appeared to be archived for longer). The authors were more confident about the number of cyber-enabled cases under the Fraud Act, as there were considerably more complete cases available for analysis.

- **These cases give some insight into the nature of cases dealt with by the CPS, but do not necessarily reflect all online crimes initially reported to police.** It is not possible to infer from this research the characteristics of cases originally reported to the police by victims, or by the police to the CPS (or those that were still 'live'). It is quite likely that the process of attrition from the initial offence to CPS involvement is not uniform.

- **The cases included only reflect those dealt with by local police and not by the National Crime Agency (NCA).** At the time of conducting the research (Dec 2012) cases dealt with by the Serious and Organised Crime Agency and the Police Central e-Crime Unit (both of which are no longer in existence and have been replaced with the NCA), were not available to the researchers due to security access issues. The cases referred to in this research are therefore those primarily dealt with by local police and so tend to represent less complex and/or less serious crimes.

Table 2. Number and proportion of total sampled usable and online cases under the four Acts

No. of unique cases	Computer Misuse Act (2011–2012)	s. 127 Communications Act (2011–2012)	Malicious Communications Act (2011–2012)	Fraud Act (Q4 2012)	Total
Initial dataset	37	2,403	1,052	2,958	**6,450**
Sample	37 (all)	100	100	100	**337**
Usable cases (% of initial sample)	25 (68%)	36 (36%)	50 (50%)	94 (94%)	**205**
Usable online crime cases (% of usable cases)	25 (100%)	3 (8%)	7 (14%)	19 (20%)	**54**
Usable online crime cases and guilty verdict (% of usable online crime cases)	23 (92%)	2 (67%)	7 (100%)	19 (100%)	**51**
No. of online offenders found guilty	33	2	7	19	**61**

Note: The number of defendants in the table is higher than the number of cases for the CMA because one case had eight defendants, another had three and a final one had two.

Of the usable cases and where an offender was also found guilty, 20 per cent of Fraud Act cases, 14 per cent of MCA cases and 6 per cent of CA cases were categorised by the researchers as online crimes. Because of the loss of cases under the CA and MCA, the most robust estimate of the extent of online crime is for Fraud Act offences. By calculating the confidence interval (95%),[5] the researchers reasonably expect that the proportion of online

[5] The researchers could calculate a 95 per cent confidence interval (CI) for the proportion of Fraud Act cases that were committed online since there were a reasonable number of them. The 95 per cent CI is ±7.93 so it is reasonable to expect that if the researchers were to resample the Fraud Act cases, the proportion of online fraud cases would lie between 12 and 28 per cent of the total. A 95 per cent CI means that from 100 samples, 95 of these samples would be expected to have

fraud cases would lie between 12 and 28 per cent of the total. In comparison, analysis of initial data from Action Fraud during their roll-out period found that one-third of all fraud reports made to them in 2012 were committed online (McGuire and Dowling, 2013). All the Computer Misuse Act 1990 (CMA) cases would have been committed online by the nature of the legislation, but only small numbers of offences are prosecuted under the CMA each year. The number of cases eligible for analysis in this research was further reduced as only 62 per cent of CMA cases contained usable information and also resulted in a guilty verdict.

3.2 What are the characteristics of online offenders and their crimes?

Table 3 summarises the demographic characteristics of the online offenders studied under the four Acts.

Table 3. Demographic details for online offenders under the four Acts

Demographics (at time of first offence)	Computer Misuse Act	s. 127 Communications Act	Malicious Communications Act	Fraud Act Q4 2012
Total no. of offenders	33	2	7	19
Mean age at time of first offence in case file (range)	31 years (17–58)	41 years (20 years, 62 years)	23 years (17–31)	31 years (18–56)
No. of male (%)	24 (71%)	2 (100%)	5 (71%)	14 (74%)
No. of ethnicity – White (%)	17 (52%)	1 (50%)	5 (71%)	13 (68%)
No. of ethnicity – Other	5 Black; 2 Pakistani; 1 Chinese (8 not known)	1 not known	2 not known	2 Black (4 not known)
No. of nationality – British	20 (1 not known)	Not known	5 (2 not known)	13 (1 Nigerian; 5 not known)

The **majority were male and on average were of a young age.** Most appeared to be **British and White**. They also spanned **a range of occupations,** from unemployed to those in managerial or professional occupations (for example, engineering, accountancy) and included both private and public sector workers, as well as students.

In general, financial offenders were in roles where they had an opportunity to commit fraud (except for those committing ebay-style frauds) and in cases of unauthorised access, individuals had opportunities because of particular access rights to sensitive data or information, given to them as part of their role. More technically skilled offenders often had a connection to computers via their studies or occupation. Similarly, the majority of harassment offenders had a partner or ex-partner.

There was not much detail on their socio-economic status or education.

between 12 and 28 per cent online crime cases in them.

The nature of online offending: Three broad online offender motivations

Three main motivations for online offending were identified through a qualitative analysis of information held in the case files regarding offences identified from the 51 usable online crime cases. They were ascertained chiefly by looking at the statements of the offenders, prosecutors, the police, judges and witnesses. Further methodology details are in **Annex A**.

Financially or profit-motivated offences (28 cases): Twenty-two cases were directly financially motivated, for example, involved stolen personal data or money via online accounts (18 Fraud Act cases; 4 CMA cases). This category also includes six cases where the offender was motivated by indirect personal gain, for example, to facilitate blackmail; to get inside information or take advantage of someone else's 'clean' credit rating.

Work-related revenge offences (4 cases): These were incidents involving the destruction of/blocking access to computer files or systems aimed at employers as an act of revenge, usually after dismissal or because of perceived unfair treatment at work (four CMA cases). Since these form 'criminal damage' offences, there may be merit in exploring cases dealt with under this offence category in future research.

Online harassment or online stalking (14 cases): The third category related to harassment of young/adult females, usually motivated by a mixture of revenge and/or sexual or 'romantic' obsession, and often linked to the victim ending an abusive relationship (six CMA cases; five MCA cases[6]; two CA cases; and one Fraud Act case). Some were 'online stalking' style offences with offenders tending to target multiple victims and appeared less emotionally involved than those targeting a single, known individual (although stalking and harassment overlapped).

Curiosity and other motivations: In some cases secondary motivations were apparent including curiosity, for 'fun' or boredom. In two cases, sexual motivations were evident – one case involved downloading indecent imagery of children and a second involving grooming a female aged under 16.[7] Two further cases involved offenders with mental health problems.

Victim/offender relationships

A strong theme identified in the online cases is that offenders and victims were generally likely to know each other; this was true for 30 of the 51 cases (with a further 18 cases involving strangers and 3 being unclear). In 10 out of 11 harassment motivated cases the offender and victim knew each other very well (usually through a previous relationship). This corresponds with offline stalking characteristics (for example, Reyns *et al.*, 2012).

Insider offences

Just under half (22) cases were assessed as being 'insider offences' (see Table 4). Insider-enabled cases were identified as those where the offender used their status and/or access rights as an employee within a particular company or organisation in order to commit an offence (for example, misusing privileged access rights on sensitive databases). These most commonly

[6] A further two MCA cases involved sending malicious Facebook messages but had no further details and could not be examined further.

[7] Whilst these cases were originally being proceeded under the CA and the MCA, they resulted in guilty pleas for making indecent photographs of a child and causing, or inciting, a child to engage in sexual activity.

involved current employees committing fraud (11 cases, see case example one below), employees seeking some other gain (3 cases), or being driven by curiosity (2 cases). Several ex-employees used inside knowledge to exact revenge on former employers (4 cases). Very particular inside knowledge may be used, for example, in the fraud cases, the offenders had a role that granted them access to and responsibility over resources (for example, IT, finance, HR).

Serious and/or organised crime

There were 11 cases that were assessed as representing more 'serious or organised crime' because they showed planning, sophistication and a propensity to offend.[8] At the time of analysis (February 2013) the definition used to help assess if something appeared to be serious and/or organised was: *"… individuals, normally working with others, with the capacity and capability to commit serious crime on a continuing basis, which includes elements of planning, control and coordination, and benefits those involved. The motivation is often, but not always, financial gain."* (HM Government, 2011). One CMA case involved an insider working at a bank who directed bank funds into her seven accomplices' bank accounts. In another CMA case, a pair of blackmailers corrupted an insider at a telecoms centre to gain victims' details. The other nine cases were individuals working alone (see case example one below). These were included where the offence was serious and indicated a propensity to offend (including three single offenders who were given a Serious Crime Prevention Order).

Table 4. Number of cases where there was evidence of a relationship between the victim and offender; indications of either serious and/or organised crime and evidence of an offence committed by an insider

Online offending cases	Computer Misuse Act	s. 127 Communications Act	Malicious Communications Act	Fraud Act Q4 2012	Total cases
Victim–offender relationship?	15 cases	1 case	3 cases	11 cases	**30**
Insider offence?	13 cases (including 5 with ex-employees)	none	none	9 cases	**22**
Serious or organised crime?	7 cases	none	none	4 cases	**11**

Note: Rows are not mutually exclusive and cases can appear in more than one category.

[8] Three of the cases that appeared in the initial case set from the CPS (under the Fraud Act 2006) were marked as having been dealt with by the Organised Crime Division of the CPS. The authors could not look at the cases without undergoing further security clearance, but they were assured by colleagues in the CPS who did have access that these three cases did not have an online component.

Case example one: Insider-enabled online crime

One case involved an insider working alone. A clerk at a particular company took note of customers' credit and debit details (over 1,400 victims) at first by writing them down, but latterly by using a USB stick to transfer them electronically. He set up a fake business and applied for two electronic card transaction terminals. From the prosecutor's description: *"He began inputting credit and debit card details at a very fast rate using the 'cardholder not present' facility, which allows a retailer to obtain payment via phone."* He attempted to steal over £161,000 but only obtained around £39,000 as one of the card companies noticed something was wrong and blocked his account.

Online offending methods

Some relatively 'advanced', but also routine computer skills, played a part in the online crimes identified. Social engineering and methods involving unauthorised access to work computers were also identified. Often methods overlapped, for example, using social engineering to facilitate unauthorised access to systems.

'Advanced' computer skills: Whilst some of the techniques used by offenders in these cases may not be regarded as 'advanced' for much of the hacker community or computer security experts, there was some evidence of more complex computer skills being adopted than one might reasonably expect for the average person. These included:

- custom-made hacking programmes, PHP scripts, SQL injection, or specific backdoor exploits (including a legal remote access programme) to try to gain access to victims' computers;
- use of programmes and proxy servers designed to hide IP addresses, adding filters to others' email accounts to try and hide crimes;
- use of specific spyware or password decoding software to get personal details; and
- infecting computers with viruses.

Routine computer skills: Examples of routine computer skills being misused included:

- posting or sending offensive or threatening messages through social networking sites or emails;
- making fraudulent claims or offers on websites such as Gumtree, ebay, paypal or other similar websites;
- downloading illegal images; or
- buying payment card details online.

Unauthorised access: This included:

- illegal checks on internal databases;
- offenders using access to accounts when passwords were not changed after they had left their employer;
- using friends' or a partner's information without permission;
- stealing computer equipment with sensitive information on it; and
- misappropriating bank or other finances.

Social engineering: This involved using social skills to trick or deceive others into giving them personal details or access to a computer, for example:

- by accessing and taking over victims' email/social networking accounts by guessing security questions;
- setting up fake social networking site profiles and tricking the victim into adding them as friends;
- phoning up the victim's university and getting them to give out personal details; or
- convincing others to carry out unauthorised access to acquire sensitive information.

See also case example two.

Whilst the numbers of cases are small, some common methods appear to be related to different types of online crimes:

- harassment-style offences tended to use spyware more than other cases (cases under s. 127 CA and the MCA harassment cases feature abusive electronic messages most heavily);
- the revenge-motivated offences tended to use insider-enabled hacking with destruction of or blocking access to computer material;
- the financial offences tended to use insider-enabled unauthorised access, or routine computer and internet use (for example, ebay); and
- offences under all four Acts, and involving all motives, used various forms of 'hacking'[9] and social engineering.

The case file analysis also shed some light on the technical ability of offenders. Offenders did not need to be highly technically skilled. Hack tools for non-specialists were downloadable from the internet and were seemingly not difficult to find. For example, one offender downloaded SQL injection tutorials from the internet on his computer and another used programmes that are freely available online. However, given that these cases did not include Serious Organised Crime Agency and the Police Central e-Crime Unit (now the NCA) cases, it is possible that greater levels of technical skill may be observed in these higher-level cases.

One case in particular was notable in that the offender managed to target at least four main victims and all of their extended social networks using only his Blackberry.

Challenges of technical cases

In a handful of cases the technical elements were complicated. In one example, the prosecutor stated: *"The expert evidence ... was, in my view, too complicated for a jury to understand. I cannot follow it and I suspect most non-experts would be baffled too."* In another case, the interviewing police officer said:

> *"SQLMAP as far as I can make out [he did his own research using Google] is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over a back end database service. Yesterday when I got this I had absolutely no idea what it meant, it was like a foreign language to me to be completely honest with you ... I am assuming it's some sort of security loophole ..."*

[9] 'Hacking' was often used as a generic term in the case files to cover a range of activities to enable unauthorised access, without clarity over what it really involved.

Case example two: Attacks often blend sophisticated computer skills with more simple trickery

“One of the programmes he used gave him an ability to gain access to people's ... email accounts. There is the scope to have thousands of anonymous victims all over the world using this 'hack' ... Once [the defendant] had access to people's email accounts, he would set up a 'filter' ... any email sent to a victim that contained the terms ‘sort code’, ‘exp’ and ‘Amazon’ would automatically be forwarded to his email account and be deleted from the victim's account before they even knew it existed ... In simple terms, it gave [him] complete control over the victim's email account.”

(Prosecutor’s description, CMA case example)

Harm caused by the offender

From the victim statements in the case files, it is clear that offenders caused a range of both financial and non-financial harms to victims.

Evidence available regarding **financial harms** was patchy and was only included in a small number of case files. However, this indicated losses ranging from hundreds to thousands of pounds for individual victims, to tens of thousands of pounds lost by some businesses and companies. The largest single loss identified was for a company losing around £250,000. In general, specific loss figures were only noted where they appeared to involve more substantial sums of money.

In terms of **non-financial harms**, there were a number of physical and emotional impacts apparent from case files analysed. These included the following.

- **Physical impacts such as stress:** One victim stated: *“I am [a] diabetic ... During 2010, my blood sugar levels reached all-time highs, which I believe was partly due to the stress ... I have also got insomnia now, and have been taking sleeping tablets for the past nine months.”*
- **Loss of trust**: This was evident not just for victims of harassment, but also financial victims. One victim stated: *“I have found it difficult to trust anyone, particularly since [he] is a former employee ... and we had no problems with him prior to this."*
- **Potential for ‘real world’/offline danger:** In some cases the offender put the victim at risk via the online offence – for example, in one case the offender used the victim’s details to solicit strangers for sex, leading them to turn up at the victim’s workplace. A further example is outlined in case example three below.

Case example three: ‘Real world’ dangers

“[An ex-partner also changed] her online profile on a dating site to describe her as a paedophile and giving her home address; this resulted in an unknown male attending her home address and trying to gain access. As a result of the incidents, the victim was seriously traumatised and she left her address and could not return until security provisions ... were installed.”

Victims also often mentioned feeling **embarrassed** and expressing concerns over **potential**

damage to business reputation, as well as personal reputation (for example, via credit rating scores).

Some impacts appeared to be widespread, going beyond the initial victim targeted. In some cases considerable distress and knock-on effects were caused for families, friends and whole social networks, as well as official bodies, sub-contractors and client companies. In one case a company was dissolved after its servers were blocked by an ex-insider, destroying business relationships and the company's reputation. Staff were made redundant, demonstrating the widespread damage the offence caused.

Previous offending

Material in the case files indicated that 26 of the 61 offenders had been involved in some form of previous offending (which had either resulted in a formal sanction or in a police intelligence entry). However, in 25 cases it was not clear if the offender had a previous conviction; exploring the full criminal histories of offenders was not part of the scope of the study.

Offenders involved in financial/profit motivated cases tended to have previous convictions for fraud (both online and offline), shoplifting, theft and forgery as well as other miscellaneous offline offences (for example, public disorder). Previous offending within revenge cases was rarely identified. Offenders in many of the harassment cases, while rarely having a formal criminal record that was known about, did often have a history of offline domestic abuse of their victim (or had targeted other victims before, who did not press charges).

While it would be rash to draw too many conclusions from a sample without the offenders' full criminal histories, the indication is that some offending is by 'new', online-only offenders; whilst others are traditional offenders who have changed their modus operandi, for these offences at least.

Offender reactions to their offence

Some of the case files cast light on offender reactions to their offences. In some cases, they displayed arrogance and a sense that the offender is 'owed' the money/revenge/sexual attention by the victims. This ties into research indicating that one of the top email phrases before an insider fraud includes: *"They owe it to me"* (FBI and Ernst and Young, 2013).

Others did appear to show remorse – mainly in the harassment cases where they did not set out to cause as much destruction as they did, or where they did not realise the impact of their actions. For example, the police description of an offender in one case states: *"At the time he* [the offender] *thought it was a joke* ... [he says] *'I didn't think it would turn out as bad as it has done'."* This might suggest that being confronted with the reality of the offence's impact on the victim – perhaps through a restorative justice process – could be instructive for some offenders. Alternatively, letting the public hear the personal stories of victims of online crime (especially in relation to trolling, harassment, etc.) might be useful in helping to delineate what is legally/socially acceptable to prevent offending and show how online 'jokes' can quickly get out of hand.

Catching or stopping online criminals

How were they caught?

- Most of the financial and profit cases were caught by **internal audits** (both commercial, i.e. for fraud; and public audits, i.e. for personal data theft). One CMA case was **picked up by a bank** when large amounts started being processed by the fraudulent ‘business’. The other bank involved in the case had not noticed, demonstrating the need for financial providers to be vigilant.
- In cases where revenge was the apparent motive, the offence was usually only noticed when considerable damage had already been done (for example, files had been deleted or access had been blocked).
- Most of the harassment cases were picked up by the **victims going to the police**.

Potential barriers to reporting identified in the case files included victim embarrassment and fear. In one case the prosecutor writes: *“The victim states she was so embarrassed about this that she was too afraid to tell anyone what he was doing.”*

Some victims collected their own evidence regarding the case, including printouts of online messages and social networking posts. In one case, the owner of a compromised ebay account suggested the identity of the offender to the victim of the fraud, who then subsequently identified him on Facebook. This does however raise problems about the admissibility of evidence (O'Floinn and Ormerod, 2012) – if victims are collecting evidence, how robust is it and can it always be used by the police and in court?

4. Future research

- If security access allows, it would be useful to explore NCA cases to identify potentially different (i.e. more serious, complex) types of online crime cases and compare these with the cases dealt with by local police in this report.
- Re-sampling and expanding the number of CA and MCA cases might also be useful to provide further supporting evidence given the small volume of usable cases identified for this research. Cases could also be sampled across time to investigate how these offence types are changing with the availability of new communication styles and computer systems.
- Additional analysis of cases falling under other legislation could also be informative, for example, cases under harassment and stalking legislation and also criminal damage offences.
- Further evidence regarding the extent and drivers of attrition between online crime cases reported to the police (and, since April 2013, to Action Fraud) and those reaching the CPS would also be useful. Although a way needs to be found to identify online crime cases at the reporting stage (this might be possible via the Action Fraud data and the online crime flag currently being applied in some police forces).

5. Implications

- **Data limitations mean that the researchers cannot confidently infer how many crimes reaching the courts are being committed online and the numbers identified in this paper are likely to be an underestimate.** Nonetheless, the cases examined still give helpful insight into the nature of the online offending and the offenders that reach court.
- **The majority of offenders and victims were known to each other offline and offences were often brought about by the deterioration or ending of a trusting professional or personal relationship.** Moreover, in many cases, offenders did not need high levels of technical skill to commit their offences. **Simple precautions could have reduced victimisation or minimised the impact of the crime.**
- **Since the ending of relationships seems to represent a point of high vulnerability, a clear area of behaviour change may therefore be getting the public (individuals and businesses) to think about updating online security when relationships break down.** For example, changing passwords, limiting or removing access rights (to email, social networking, work and bank accounts) or even scanning computers if a skilled individual is involved. These changes are ideally carried out before or as soon as offline relationships change.
- **Further awareness amongst the public about the misuse of trust in general may be useful, for example**, always removing passwords from computers you share with friends (you never know who else may use their computer – and your details) or sharing a joint bank account with a partner rather than giving them direct access to a personal account.
- The strength of the offline-online link between offenders and victims also raises questions regarding **how easy it is to find or charge an offender who is a stranger, overseas or is simply more careful.** Prosecutors commented that the offline connections helped to make a strong case. This analysis contains an inherent bias as it only relates to those who were detected, prosecuted and convicted. Less is known regarding those offenders who are not caught and how they differ to those who are.
- **Letting the public hear the personal stories of the victims of online crime might be useful in helping to delineate what is legally/socially acceptable in order to prevent offending.** It might also make it clear to the public how severe the effects can be with misplaced online trust (even when trusting offline friends and family). The use of restorative justice for some offenders could also be explored as a way of exposing them to the reality of the harm that online offending causes to victims.
- **Many open source online tools/software have legitimate purposes,** for example, for software testing. However, **some online tools clearly can be used for teaching people to undertake malicious hacks and other activities. Encouraging reporting and taking down suspicious online tutorials or websites might help to reduce opportunities for some potential offenders** (although it is likely that some of these tools would be on closed or hidden communications forums).

References

FBI and Ernst and Young (2013) Top ten emails used by corporate fraudsters. Available at: http://www.computerworlduk.com/news/security/3418844/top-email-terms-used-by-corporate-fraudsters-published-by-fbi/. Accessed January 2013.

HM Government (2011) *Local to Global: Reducing the Risk from Organised Crime. London:* Home Office.

McGuire, M. and Dowling, S. (2013) *Cyber Crime: A review of the evidence*. London: Home Office. Available at: https://www.gov.uk/government/publications/cyber-crime-a-review-of-the-evidence Accessed October 2013.

O'Floinn, M. and Ormerod, D. (2012) 'Social networking material as criminal evidence', *Criminal Law Review*, 486*.*

Reyns, B. W., Henson, B., Bonnie, S. and Fisher, B. S. (2012) 'Stalking in the Twilight Zone: Extent of Cyberstalking Victimization and Offending Among College Students', *Deviant Behavior,* 33:1, pp 1–25.

Annex A: Methodology

The authors aimed to explore evidence on offenders held in case files by the Crown Prosecution Service (CPS) to help fill knowledge gaps around the characteristics of online offenders and the nature of online offending. The small numbers of Computer Misuse Act 1990 (CMA) cases can be easily identified from CPS case files. However, most crimes with an online component will still be dealt with under other legislation. As CPS case files do not allow easy identification of online offences under other Acts, random samples of cases were taken from other legislation likely to be relevant to online crime to explore:

- what proportion of these could retrospectively be identified as online crimes; and
- what information was held regarding the offenders and the nature of their offending.

The relevant Acts were chosen after discussion with policy colleagues and the CPS. An outline of these Acts and the related offences is given below.

- The CMA includes four offences centred around technology crime.
  - Section 1 covers *"unauthorised access to computer material"* along with Section 2 *"unauthorised access with intent to commit or facilitate commission of further offences".* These sections primarily make hacking an offence.
  - Section 3 covers *"unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer",* which makes it an offence to modify a computer (for example, via malware).
  - Section 3A (introduced in 2008) makes it a further offence to *"make, supply or obtain articles for use"* in Sections 1 and 3, which includes individuals writing malware for others.

- The Fraud Act 2006 outlines three main fraud offences:
  - fraud by false representation (Section 2);
  - fraud by failing to disclose information (Section 3); and
  - fraud by abuse of position (Section 4).

Additional offences with a clear parallel to Section 3A of the CMA include Section 6 *"possession, etc. of articles for use in frauds"* and Section 7 *"making or supplying articles for use in frauds"*. The Fraud Act itself can be used in cases relating to online crime, as Section 2 outlines that false representation can occur via non-human transmission; Section 5 allows loss and gain through fraud to include intangible property; and Section 8 states that articles used in fraud can be electronic.

- Section 127 of the Communications Act 2003 (CA) makes it an offence to send or facilitate the sending of grossly offensive, indecent, obscene or menacing messages through electronic computer networks, as well as false or persistent messages, where the purpose of the messages is to annoy, inconvenience or cause needless anxiety amongst recipients.

- The Malicious Communications Act 1988 (MCA) makes it an offence to send another person a letter, electronic communication, or article of any description that is a threat, indecent, grossly offensive, or is false (or known or believed to be false by the sender), and by sending such a communication intends to cause distress or anxiety.

Methodology for identifying 'online' crimes

The CPS provided unique reference numbers for all of the cases proceeded under the CMA (37 cases), s.127 of the CA (2,403) and from the MCA (1,052) from 2011–2012; along with all of the cases proceeded under the Fraud Act 2006 from the last quarter of 2012 (2,958; a smaller time period chosen for practical reasons since there were so many Fraud Act cases).

All 37 CMA cases were chosen since there were so few of them. From the other three Acts, a random sample of 100 unique cases was chosen from each Act to find out how many cases were online crimes. These 337 cases were examined by the researchers using the CPS Case Management System (CMS) to find out:

- if they were usable (i.e. contained any relevant information that would allow the authors to determine if the crime was committed online or not);
- how many of them had an online element, as per the definition outlined below; and
- whether or not the offenders were found guilty.

Cases are only held electronically by the CPS for a period of one to two years and after this the electronic copy is destroyed. So sometimes there was not enough detail to be able to tell if the case was committed online – where this occurred, the case was regarded as not usable for purposes of this project. It is technically possible to obtain hard-copy case files direct from the courts to help to complete the information, but there was insufficient time to do so as part of this project. Tables A1 and A2 below present detail on the initial dataset and the random sample.

In order to classify a case as committed 'online', the authors used a pilot definition for an online crime 'flag' that was being trialled and tested by the Home Office with a small number of police forces during 2013 via the Annual Data Requirement.[10] In 2013 the trial definition stated that an online crime had occurred when:

> *"On the balance of probability, the offence was committed, in full or in part, through a computer, computer network or other computer-enabled device. This included sending or receiving emails; use of social networking sites such as Facebook, Twitter or chat rooms; use of forums, blogs or websites; messaging services such as Blackberry Messenger (BBM) and communication via online video game networks or Skype. The terms 'computer, computer network and other computer-enabled devices' include those offences committed using: desktop computers or laptops, in the home or in the workplace; mobile phones, smartphones, tablets and other telecommunications devices linked to computer networks; and any other identifiable computer system or network that produces, processes and transmits data."*

Please note that the definition used for the online crime flag has been further developed and refined following feedback from police leads since this research was conducted.

[10] The Annual Data Requirement (ADR) is a list of all routine requests for data made to all police forces in England and Wales made under the Home Secretary's statutory powers. In the 2014/15 ADR a pilot definition of online crime was included, and forces were asked to provide data on all offences that fell under this definition on a voluntary basis. This was with a view to further refining the definition and then requesting data from all forces on a mandatory basis from 2015/16 onwards.

Methodology for analysing the characteristics of online offenders and their offending behaviours

All 23 viewable and convicted cases under the CMA were examined in more detail to gain information on the characteristics of online offenders and the nature of their offending. In addition, 2 cases under s.127 of the Communications Act, 7 cases under the MCA and 19 cases under the Fraud Act were also examined in detail as they were classed as usable, committed online and where the offenders were also found guilty. Note: The sampled cases could contain multiple offenders and so the report sometimes refers to numbers of offenders instead of numbers of cases.

Demographic and other personal information on the online offenders were gathered from the files and a qualitative thematic analysis was carried out to examine the nature of online offending. The authors initially planned to examine motivations for offending and methods of offending as main themes, but during the course of analysis other themes emerged as a result of the information that was available (for example, exploration of serious organised crimes; victim/offender relationships and how criminals were caught).

Quality assurance: In order to ensure accuracy in the data obtained from the case files and consistency in the approach to classification of information, the authors reviewed and checked each other’s cases. In cases, for example, where it was not clear to one of the authors if a case met the definition of ‘online crime’, the case would be assessed separately by the other author and then a joint decision made. Where disagreement arose then a third person would be brought in to help decide.

Data summarising the initial datasets and the random samples

Table A1. Number of defendants in the four Acts (and Stage 1 samples)

Defendants	Computer Misuse Act	s. 127 Communications Act		Malicious Communications Act		Fraud Act	
	Initial/Sample	Initial	Sample	Initial	Sample	Initial	Sample
No. of defendants	61	2,675	110	1,158	102	3,624	127
Average no. of defendants per unique case	1.7	1.1	1.1	1.1	1.0	1.2	1.3
% (and number) male	79% (48)	82% (2,186)	82% (90)	87% (1,007)	90% (92)	76% (2,767)	72% (91)

Notes: All Computer Misuse Act cases were examined. The number of defendants is greater than the number of cases because multiple defendants can be in one case.

Table A2. Proportion and number of defendants by outcome for the four Acts (and Stage 1 samples).

Outcomes	Computer Misuse Act	s. 127 Communications Act		Malicious Communications Act		Fraud Act	
	Initial/ Sample	Initial	Sample	Initial	Sample	Initial	Sample
Guilty and mixed guilty pleas[1]	69% (42)	79% (2,113)	75% (83)	78% (904)	79% (81)	80% (2,880)	72% (92)
Conviction after trial	16% (10)	4% (113)	4% (4)	5% (56)	7%(7)	6% (233)	9% (11)
Proved in absence	0	<1% (7)	0	<1% (2)	0	<1% (7)	0
Acquittal after contest[1]	8% (5)	2% (55)	0	4% (41)	3% (3)	2% (83)	<1% (1)
Judge directed acquittal	2% (1)	0	0	0	0	<1% (5)	0
Case dropped[1]	5% (3)	13% (361)	20% (22)	13% (145)	11% (11)	9% (343)	17% (21)
Discharged committal	0	<1% (1)	0	0	0	<1% (15)	0
Admin finalised	0	1% (16)	1% (1)	1% (6)	0	2% (55)	2% (2)
No case to answer	0	<1% (9)	0	<1% (4)	0	<1% (3)	0

Notes: All Computer Misuse Act cases were examined. Percentages may not sum due to rounding. The number of defendants is greater than the number of cases because multiple defendants can be charged in one case. Multiple charges can also be brought about for the same defendant.

[1] Please also note that these outcomes can refer to other offences charged or pleaded guilty to later than the initial proceedings and so there is not a direct one to one correspondence between these outcomes and the Act they are recorded under here. For example, someone could have been charged with fraud, but pled guilty to theft and this would be recorded here as a guilty offence in the Fraud Act column.

ISBN: 978-1-78246-907-0

ISSN: 1756-3666