Law Commission
Reforming the law

ABUSIVE AND OFFENSIVE ONLINE COMMUNICATIONS

Summary of Scoping Report

SUMMARY

INTRODUCTION

> **"The development of the internet has caused a seismic shift in the way we communicate as a society, and has brought with it the potential for harm and offence on a huge scale."**
>
> Para 1.38 of the Scoping Report

The rise of the internet and social media in recent decades has fundamentally reshaped the way we engage with each other and as a society. This radical shift has brought many benefits, but there are also associated risks and harms, and **it has proved challenging for the law to keep pace with this rapidly changing environment.**

In February 2018, the Prime Minister announced that the Law Commission was to conduct an analysis of the criminal law in relation to offensive and abusive online communications. This followed our own consultations in 2016 and 2017, in which proposals for such a review were widely supported.

Our agreed Terms of Reference ask us to consider the applicable criminal law, identifying any deficiencies. Our particular focus is whether the criminal law provides equivalent protection online and offline. We also consider whether particular groups in society are more vulnerable to abuse than others.

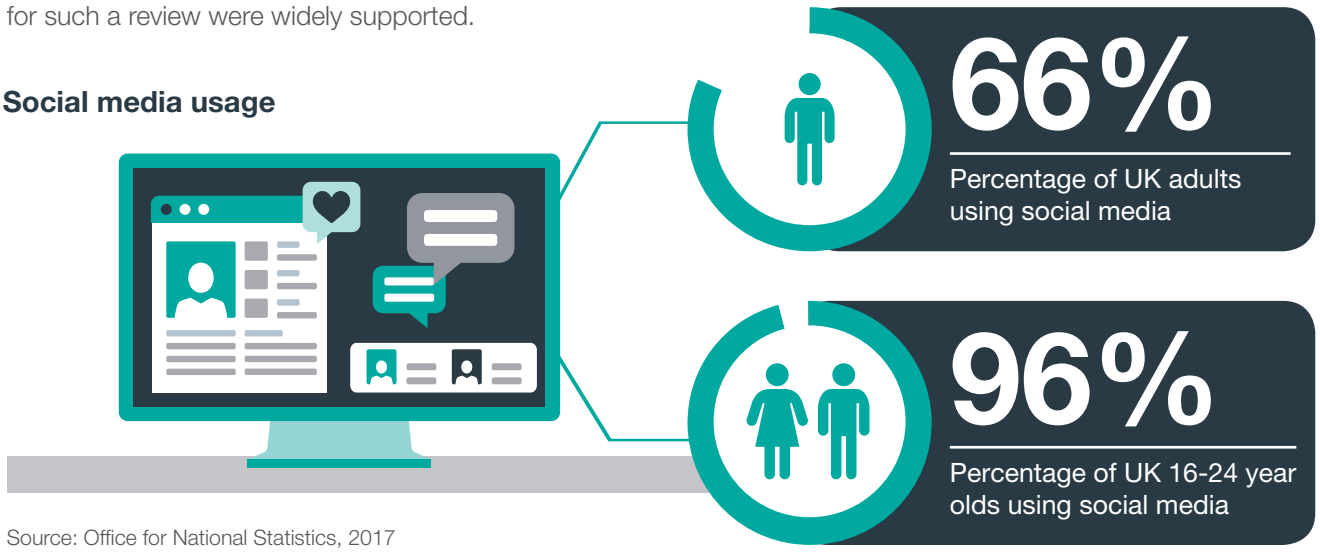
In undertaking this review, we acknowledge that the criminal law is only one means by which online abuse can be addressed. The Government is currently considering the broader context of online harms through its Internet Safety Strategy.

However, we consider that the criminal law has an important role to play in setting standards and deterring and punishing unacceptable online conduct. As one stakeholder put it:

Online abuse is like domestic violence in the 1980s. People used to say it was just something that happened. Police didn't step in on disputes between a husband and wife. But every part of society changed when prosecutions started being brought.

A copy of the full Scoping Report can be found at www.lawcom.gov.uk

Social media usage



Source: Office for National Statistics, 2017

The key offences that we consider throughout the Scoping Report are the "communications offences" under the Malicious Communications Act 1988 ("MCA 1988") and the Communications Act 2003 ("CA 2003"). We analyse the technical aspects of the offences, and also the terms on which they rely, including "gross offensiveness", "obscenity" and "indecency".

We also look at other offences that criminalise various forms of threatening and distressing behaviour, including those found in the Public Order Act 1986 and the Protection from Harassment Act 1997.

Excluded from the scope of this review are terrorism offences, child sexual abuse and exploitation offences, online fraud and contempt of court. These issues are being considered by Government in other contexts.

Our Terms of Reference also exclude consideration of the liability of internet platforms that transmit or store offensive or abusive communications. Internet platforms undoubtedly have a crucial role to play in ensuring the safety of online users, but the focus of this review is squarely on the perpetrators of offensive and abusive online communications.

Throughout this review we have engaged with many individuals and organisations who are impacted by these laws or have detailed knowledge of the surrounding issues. This has included victims of online abuse and the charities that support them, prosecutors, lawyers and academics, civil liberties groups, technology companies, and various parts of Government.

The Scoping Report is structured as follows:

- Chapter 2 outlines how online communication works, and the challenges the online environment presents to the criminal justice system.
- Chapter 3 sets out the particular forms of harm that are experienced by victims of online abuse. This informs our consideration of the criminal law throughout the Scoping Report.
- Chapters 4 to 12 set out the applicable substantive criminal law in more detail.
- Chapter 13 summarises the key conclusions we have reached, and outlines our recommendations for the focus of future reform.

Each of these Chapters is summarised further below.

THE ONLINE ENVIRONMENT

"Online abuse is a widespread phenomenon in England and Wales."

Para 2.154 of the Scoping Report

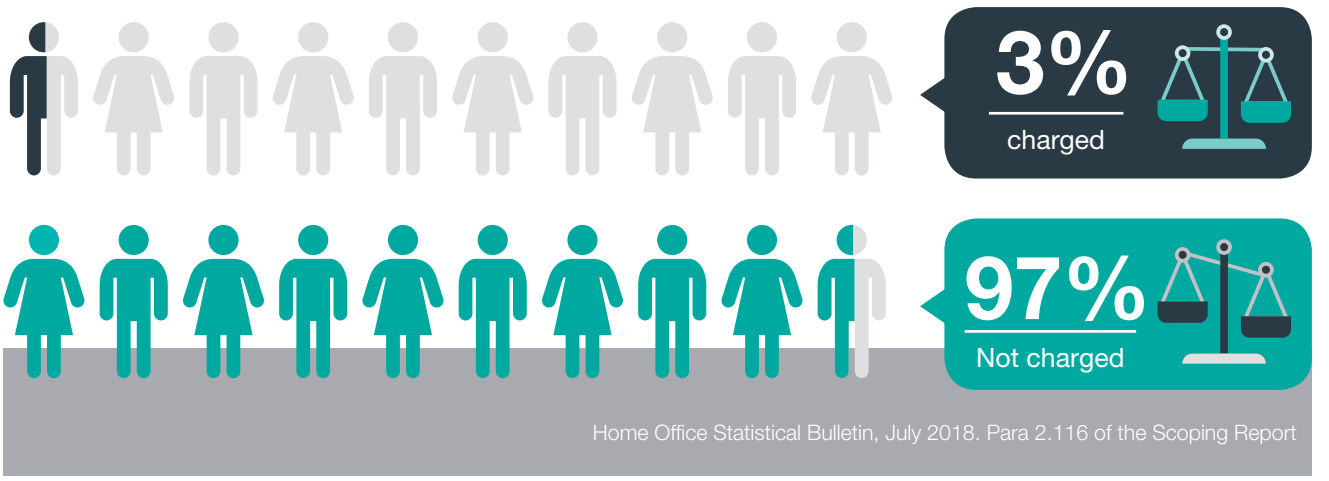
In Chapter 2 we provide some technological background about the development of the internet and the types of communications it facilitates, including website browsing, email and social media. We discuss social networking services, and outline the role of major platforms such as "Facebook", "Twitter", "Snapchat" and instant messaging services in the online environment.

In academic discourse, cybercrime is a commonly used but contested term. For our purposes, we distinguish between cybercrime and computer crime more generally. We discuss varying categorisations of different types of cybercrime, and the fact that abusive and online communication forms one subset. In this Scoping Report, we adopt a classification scheme driven by the categories of "offline" offences and behaviours that we have been asked to review: speech and communication offences which are abusive and/or offensive.

We also consider the endemic challenges of policing cybercrime for law enforcement in England and Wales. These include issues within substantive criminal law, alongside investigative, and social and regulatory challenges. We look at challenges including:

- Balancing the application of the criminal law with the qualified right to freedom of expression.
- Working out where the offence is committed from a jurisdictional perspective.
- Dealing with the indeterminacy of the elements of the offences.
- Dealing with investigative challenges presented by online communication including:
  - Getting access to evidence:
    - when it is located outside England or Wales; or
    - when the offender is technologically capable.
  - Technical capabilities and resources of the police.

Percentage of recorded malicious communications offences (whether committed online or offline)



Home Office Statistical Bulletin, July 2018. Para 2.116 of the Scoping Report

  - Role of the internet service providers.
  - The scale of offending behaviour.
- The characteristics of online communication which make offensive and abusive communication so prevalent.

IMPACT ON VICTIMS

Underlying the need for this review is the demonstrable harm that offensive and abusive online communications cause to victims. In Chapter 3 we consider whether the impact of online abusive and offensive communication is qualitatively different to that perpetrated offline.

Through both a literature review and our discussions with stakeholders, we observe that the qualitative effect of offensive and abusive online communications include:

- psychological effects, such as depression and anxiety;
- emotional harms, such as feelings of shame, loneliness and distress;
- physiological harms, including self-harm in the most extreme cases;
- exclusion from public online space and corresponding feelings of isolation;
- economic harms; and
- wider societal harms, such as the impact on people who witness the offending behaviour. For example, where a person witnesses online hate speech.

We acknowledge diverging opinions about whether harms resulting from online abuse vary significantly from harms experienced by victims of offline abuse. A number of victims have advised us that the impact on their lives is different, due to specific characteristics of communication on the internet, including the volume of communications, the reach and permanency of online messages, and the perceived anonymity of the offender.

A Women's Aid survey of survivors of domestic abuse in 2013 found that 45% had experienced abuse online during their relationship. For 85% of survivors surveyed in 2015, this abuse was not only virtual – but perpetrated by a partner, or ex-partner, as part of a pattern also experienced offline.

We reject the suggestion that harms from online abuse should be treated as less serious because they are "avoidable", as victims put themselves in harm's way by remaining online.

> **"The pervasive nature of online communications actually means that online abuse is more likely to be a constant harmful presence in the victim's life."**
>
> Para 3.71 of the Scoping Report

That would place an unreasonable and unfair burden on the victims of such abuse. Such arguments also fail to appreciate the centrality of the online environment to contemporary personal and professional life. As one prominent MP said to us:

When women are being abused online, the advice of the police can sometimes be to "not go online". That's the equivalent of telling women not to go out.

In this chapter we also look at the features of offensive online communications that can aggravate the harm experienced by victims. In particular, we highlight the sometimes devastating impact of collective abuse of an individual.

> **"People [who are abused online] feel shunned by society. It can be compared to being shouted out in a public place and no one responding."**
>
> A stakeholder sharing their experiences of online abuse with us

COMMUNICATIONS OFFENCES

In Chapter 4 we analyse section 1 of the MCA 1988, and section 127(1) of the CA 2003, which we refer to collectively as the "communications offences". These are the most commonly relied on offences in the context of offensive and abusive online communications.

Section 1 of the MCA 1988 criminalises the sending of certain types of communication to another person, where one of the sender's purposes is to cause "distress or anxiety" to the recipient or another person. The relevant types of communication are those which convey a message which is indecent or grossly offensive, a threat, or false information.

Section 127(1) of the CA 2003 criminalises the sending of a message which is "grossly offensive or of an indecent, obscene or menacing character". Section 127(2) of the CA 2003 criminalises sending a message which is known to be false for the purpose of causing "inconvenience or needless anxiety" to another.

The above summary is somewhat of an oversimplification, and we analyse the elements of these offences in much greater detail in Chapter 4.

We find that there are some positive aspects of the offences. For example, because the offences do not require evidence of actual harm caused to victims, they can be prosecuted more easily than "result crimes", which would require such evidence. The broad terms used in the offences also means that they are generally flexible enough to cover the huge variety of offensive and abusive online communications, and provide scope to adapt to future developments.

However, we also make a number of criticisms. In relation to the MCA 1988 offence, we note that it is somewhat unclear whether the offence can be committed by posting on a public forum, with recent case law suggesting its scope might be limited to communications directed specifically "to another".

In relation to the CA 2003 offences, we note that they do not include communications sent over a "private" network, such as Bluetooth communications, suggesting they have failed to adapt to this form of communication.

More fundamentally, we note that the communications offences overlap to a large degree, and there would be benefit in consolidating and rationalising them to reduce confusion, and ensure they keep pace with emerging technology.

Finally, as we explore throughout the Scoping Report, **some of the terms of the offences – such as "gross offensiveness" – are ambiguous, leaving significant discretion to courts and prosecutors.** This can lead to uncertainty and inconsistency, and makes it difficult for the public to understand the line between criminal and non-criminal communications.

Recommendation 1

The communications offences in section 1 of the Malicious Communications Act 1988 and section 127 of the Communications Act 2003 should be reformed to ensure that they are clear and understandable and provide certainty to online users and law enforcement agencies.

"GROSS OFFENSIVENESS"

"Gross offensiveness" is a concept relied on in both the MCA 1988 and the CA 2003, and is probably the most ambiguous and contentious aspect of these offences.

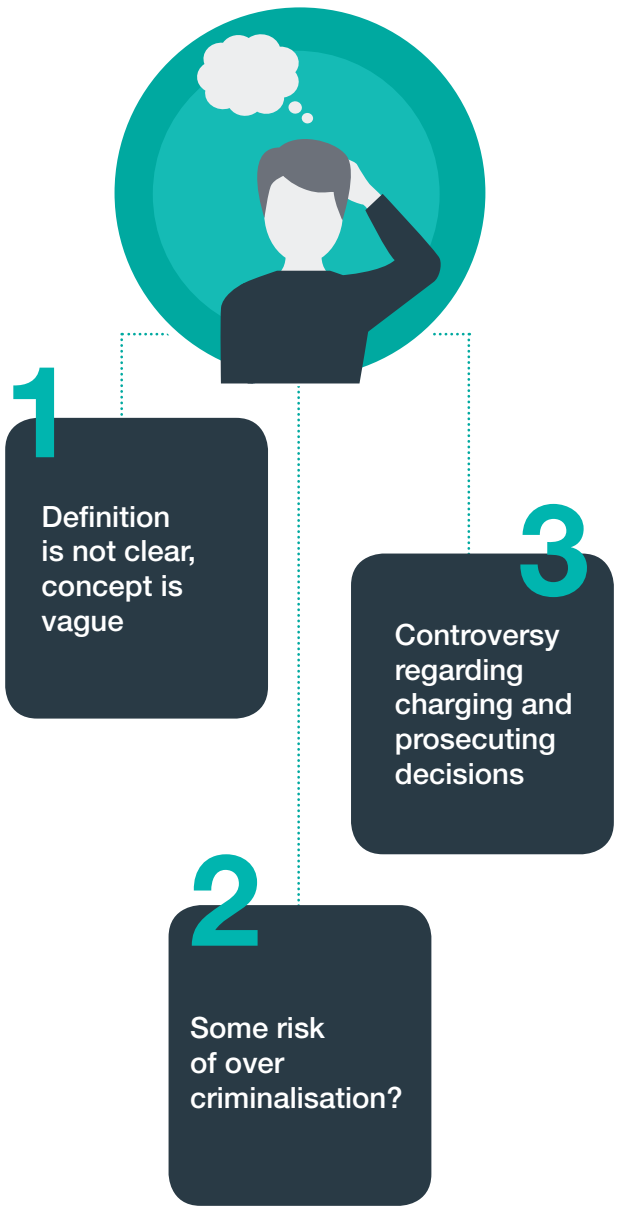
Although the term has been used in statute for over a hundred years, only minimal progress has been made by the courts in defining and clarifying its meaning.

An analysis of recent cases suggests that prosecutions on the basis of "grossly offensive" communications tend to relate to hate speech and abuse directed at high profile figures.

As we outline in Chapter 5, the concept of "offence" raises particular challenges for freedom of expression. For example, it is not always clear when the expression of an unpopular view, or a joke that is considered by many to be in poor taste, should cross the threshold into criminal conduct.

Despite the introduction of clear prosecution guidelines, there remains a lack of clarity and certainty in this area, and we consider the term should be reconsidered as part of a broader review of communications offences.

Limitations of gross offensiveness



OBSCENITY AND INDECENCY

"Obscene" and "indecent" communications may also amount to an offence under one of the communications offences.

There are also a number of other relevant offences relating to obscenity and indecency:

- the publication of an obscene article contrary to section 2 of the Obscene Publications Act 1959;
- the display of an indecent matter contrary to section 1 of the Indecent Displays (Control) Act 1981;
- the common law offences of "outraging public decency" and "conspiracy to corrupt public morals";
- the offence of exposure under section 66 of the Sexual Offences Act 2003; and
- the possession of "extreme pornography" under section 63 of the Criminal Justice and Immigration Act 2008.

We consider each of these offences and their application to the online environment in Chapter 6.

As with the issues we raised in relation to "gross offensiveness", we note the malleability around the notions of "obscenity" and "indecency" that underpin these offences.

We also outline particular concerns in respect of these offences that arise in the online context, chiefly:

- the potential for private online conversations to be criminalised by section 2 of the Obscene Publications Act 1959, and whether this is desirable;
- a lack of clarity as to whether cyberspace could be considered a "public place" for the purposes of "outraging public decency" and the display of an indecent matter contrary to section 1 of the Indecent Displays (Control) Act 1981; and
- the meaning of "possession" of extreme pornography for the purposes of section 63 of the Criminal Justice and Immigration Act 2008.

Recommendation 2

As part of the reform of communications offences, the meaning of "obscene" and "indecent" should be reviewed, and further consideration should be given to the meaning of the terms "publish", "display", "possession" and "public place" under the applicable offences.

THREATENING COMMUNICATIONS

There are a large number of specific offences that deal with threats in certain contexts in the criminal law of England and Wales, but no overarching framework dealing with threatening statements or communications.

In Chapter 7 we consider the key provisions that might be used to criminalise threatening communications, specifically:

- a threat to kill contrary to section 16 of the Offences Against the Person Act 1861;
- common assault;
- a communications offence under section 1 of the MCA 1988 or section 127 of the CA 2003;
- an offence contrary to sections 4, 4A and 5 of the Public Order Act 1986; and
- a harassment or stalking offence under sections 2, 2A, 4 and 4A of the Protection from Harassment Act 1997.

We conclude that none of these offences are ideally adapted to online communication, and the large number of overlapping offences that might be pursued in the context of threatening and menacing communications can be a source of confusion.

An overhaul of the law of threats more generally is beyond our terms of reference for this project, but we have observed that there is scope to clarify the role of the communications offences in relation to threatening communication.

HARASSMENT AND STALKING

"There is arguably a mismatch here between the forms of harm that are occurring online and the response of the criminal justice system."

Para 8.208 of our Scoping Report, talking about the criminal law's response to harassment by a group of people.

Online harassment and cyber stalking has emerged as a significant concern in the internet age, which has been further exacerbated by the rise of social media. Offences of harassment, and stalking, are dealt with under the Protection from Harassment Act 1997 ("PHA 1997"). These offences criminalise "a course of conduct" which "amounts to harassment" of another person.

In Chapter 8 we note that a very wide variety of "conduct" can amount to harassment or stalking under the PHA 1997, and this can include online behaviour, offline behaviour, or a combination of both.

As we note in Chapter 3, one type of behaviour that stakeholders raised particular concerns about was the impact of "pile on" abuse online. One stakeholder described to us the experience of being persistently called "you fucking bitch":

Maybe one off it doesn't matter, but when you have 500 coming into your inbox, 500 people saying it, maybe you don't think that.

Behaviour of this kind can be experienced as a very intense form of harassment by victims. However, at present, the criminal law does not treat it as such.

"In practice, it appears that the criminal law is having little effect in punishing or deterring forms of "group abuse."

We list examples at para 8.207 of our Scoping Report

While there are provisions in the PHA 1997 that could be used in cases of collective harassment, these are complex and do not appear to be well understood or widely used.

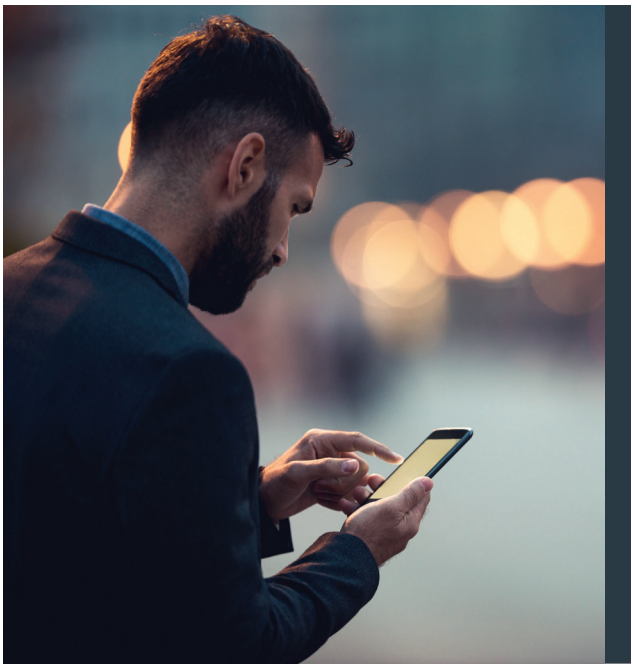
Our provisional conclusion is that future reform could consider whether there is particular conduct associated with "pile on" harassment, such as coordinating and inciting this behaviour, which could be more effectively targeted by the criminal law.

Recommendation 3

In addition to reform of the communications offences, there should be a review to consider whether coordinated harassment by groups of people online could be more effectively addressed by the criminal law.

HATE CRIME ONLINE

Hate crime laws aggravate the seriousness of criminal offending where the perpetrator is motivated by, or demonstrates hostility towards a victim based on certain characteristics that the victim has, or is presumed to have. The five protected characteristics are race, religion, sexual orientation, disability and transgender status, but the criminal law does not operate in exactly the same way across each of these characteristics.



In addition, there are several specific hate crime offences. In the online context, the most relevant of these are the offences of "stirring up" hatred based on race, religion or sexual orientation, found in the POA 1986.

Prosecution of "stirring up" offences is rare. In practice, the majority of online hate speech is pursued as one of the communications offences (though other POA 1986 or PHA 1997 offences may also be used).

In Chapter 9 we note the proliferation of online hate speech. We observe that in addition to the currently protected characteristics, abusive communications that are targeted at women – because they are women – are highly prevalent online. Participants at our stakeholders' experiences event were particularly concerned about the extent of online content that has the effect of "devaluing women or degrading them sexually", and the damaging impact this has on both the direct targets of such abuse, and on society more generally.

The issue of gender-based hate crimes will be considered as part of the Commission's broader review of hate crime laws commencing in 2019.

"In this Report we note that gender-based online hate crime, particularly misogynistic abuse, is a particularly prevalent and damaging concern."

Para 9.140 of the Scoping Report

In the specific context of online abuse, an issue that we identify is whether hateful speech directed towards people with a particular personal characteristic should be prosecuted under generic categories such as "grossly offensive" or "menacing" speech, or whether a category of "hateful communications" should be more explicitly addressed in the criminal law.

Recommendation 4

The Law Commission's reviews of hate crime and communications offences should include consideration of:

- the disproportionate targeting of women online, including through explicitly misogynistic language and sentiment; and
- the effectiveness of the existing offences in labelling and punishing hate speech.

PRIVACY OFFENDING AND DISCLOSURE WITHOUT CONSENT

The internet and social media have changed society's expectations around personal privacy, with many now choosing to send or publish an enormous amount of personal information online.

Unfortunately, this also increases the scope for personal information to be abused by others. Abusive conduct such as "non-consensual disclosure of private sexual imagery" and "doxing" have now emerged as significant sources of harm to victims. In the most extreme cases, this has led to self-harm and even suicide.

In Chapter 10 we consider the key offences that exist to prevent such abuses, including:

- data protection offences, most notably under the Data Protection Act 2018;
- the offence of "disclosing private sexual photographs and films with intent to cause distress" contrary to section 33 of the Criminal Justice and Courts Act 2015; and
- the offence of voyeurism contrary to section 67 of the Sexual Offences Act 2003.

In considering the effectiveness of these offences in the online environment, we identify two main concerns:

- whether the harm caused by emerging technology such as "deepfake" pornography is adequately dealt with by the criminal law; and
- whether there are adequate remedies to deal with the most serious privacy breaches.

We suggest these as two possible areas for further law reform.

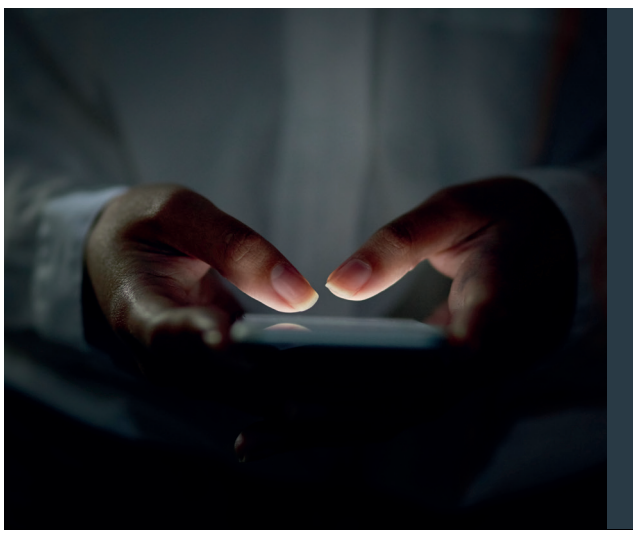
Recommendation 5

The criminal law's response to online privacy abuses should be reviewed, considering in particular:

- whether the harm facilitated by emerging technology such as "deepfake" pornography is adequately dealt with by the criminal law; and
- whether there are adequate remedies to deal with the most serious privacy breaches.

FALSE COMMUNICATIONS

Deliberately false communications that are sent with the intention to cause another "distress or anxiety" or "annoyance, inconvenience or needless anxiety" may amount to an offence under section 1 of the MCA 1988 or section 127(2) of the CA 2003.



In Chapter 11 we note that these offences are relatively unusual examples of the criminalisation of "false" communications. Aside from fraud offences, the criminal law generally does not criminalise false communications except in certain, specific contexts such as public safety laws, electoral laws, and administration of justice offences. "Fake news", for example, while recognised as an increasingly serious public harm, is not usually a criminal matter.

It is striking, therefore, that the fault threshold for false communications under section 127(2) of the CA 2003 in particular is set relatively low, merely requiring an intention to cause "annoyance, inconvenience or needless anxiety".

In practice, when deciding whether or not to pursue a prosecution, the Crown Prosecution Service will carefully consider whether it is justified in law (bearing in mind the right to freedom of expression) and in all the circumstances in the public interest. However, the issue we have identified is that there is a significant mismatch between the wording of the statute, and the much higher threshold of harm and culpability at which prosecutions are likely to be pursued. Our concern is that this makes the law unclear and uncertain. We suggest that the terms of reformed communications offences concerning false communications should more closely reflect a threshold at which criminalisation is proportionate and justified.

Conversely, we have also noted that certain potentially very harmful false communications are currently not criminalised where there is no malicious ulterior intent; for example, dangerously false health or safety advice. Given the extent of reliance placed on online sources, we consider that criminal deterrence in the most serious cases is worthy of further consideration.

Recommendation 6

As part of the reform of communications offences the threshold at which malicious and "false" communications are criminalised should be reviewed.

ENCOURAGING CRIME ONLINE AND OTHER INCHOATE OFFENCES

In the final substantive Chapter we consider how the internet may be used to encourage harmful and criminal behaviour, noting the very broad terms of sections 44 to 46 of the Serious Crime Act 2007.

We also briefly consider other forms of "inchoate" liability for online offending, such as conspiracy and attempt, and how this might apply to offensive and abusive online communications.

We conclude by suggesting that notwithstanding the broad reach of Serious Crime Act 2007 offences, there are two important contexts which are arguably not currently criminalised:

1. the "glorification" of certain types of violent crime (for example, the glorification of acid attacks or knife crime); and
2. the encouragement of self-harm online.

We do not make any final conclusions, but suggest these issues could be considered in the context of a further review of communications offences.

Recommendation 7

The glorification of violent crime online and the encouragement of self-harm online are issues which should be considered in the context of the review of communications offences.

CONCLUSION

We conclude the Scoping Report by summarising the key findings we have made as to the current criminal law regarding offensive and abusive online communications.

We find that although there are some ambiguities and technical issues with the law, the breadth of the current communications offences means that in most cases there are criminal offences available for offensive and abusive online communications in circumstances where similar behaviour offline might be criminalised. In some cases, they capture words and behaviour that would not be a criminal offence offline.

It is not clear, however, that offensive and abusive online communications are always treated and pursued as seriously as offline equivalents by law enforcement agencies and prosecutors, or indeed by the general public.

We also find that although criminal offences do exist, in many cases these could be improved so they are clearer and more effectively target serious harm and criminality. At present the available offences are both under inclusive and over inclusive in certain respects.

In summary, we recommend that a second stage of this project should consider:

- reform and consolidation of the communications offences, so that they are clearer and more proportionate;
- consideration of how the law may cater more effectively for the specific harm caused to an individual who is subjected to a campaign of online harassment; and
- a review of how effectively the criminal law protects individuals from abuses relating to their private life, with particular reference to the non-consensual sharing of private imagery.

Additionally, the Government has recently asked the Law Commission to consider a broad review of the law of hate crime in England and Wales. Our intention is that some of the observations in this Report, such as the role and effectiveness of the law in addressing hate speech, will be addressed further in the context of this separate review.

The full Scoping Report can be found at www.lawcom.gov.uk