iRights: THE LEGAL FRAMEWORK

JULY 2015

iRights

[SCHILLINGS]
Law at the speed of reputation

[SCHILLINGS]

INTRODUCTION

Two claims are often made when discussing internet privacy. First, the law cannot keep up with technology. Second, privacy is dead. We think neither is true.

The idea that new technology makes it harder to protect personal information is centuries old. In 1890 academics wrote in The Harvard Law Review:

> "Recent inventions and business methods call attention to the next step which must be taken for the protection of the person and for securing... the right 'to be let alone'. Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life and threatened to make good the prediction that "what is whispered in the closet shall be proclaimed from the house tops".[1]

In the late 19th century the concern was newfangled cameras. Now it is smart phones and social networks. Who knows what it will be tomorrow? Parents, teachers, and organisations in mental health, tech, business, media, culture and law share concerns around these issues. As do young people themselves, demonstrated by the results of iRights' fascinating 'youth juries'.

But the fundamental principle that everyone has the right to enjoy a private life is entrenched in law. This core value means we all have the right to respect and personal dignity by being able to control the sorts of information disclosed about us. Children and young people deserve this more than anyone.

We know from daily experience that there is a vast amount that can be done to protect personal information when people are armed with the right tools.

That experience is borne out through this research. Happily, each of the iRights principles finds support within the law.

Our review does not seek to describe all relevant law but covers the aspects we consider most salient. Whilst there are aspects for improvement, which we have flagged, existing English law is fairly fit to protect and empower young people online.

One benefit we hope to have achieved with this report is pulling together the plethora of different, disparate law into one place, so those looking to enforce or adopt iRights have a first port of call.

But knowing the law is only one part of the solution. In our view, the challenge is ensuring that rights reflected in the law are meaningfully applied. Children and young people should not have to resort to court for protection.

The key weaknesses concern how the law is accessed and applied. To empower children and young people to assert their online rights, more education is needed. And at the commercial end, those providing online services need to respond much quicker to issues and make it easier for them to be raised.

Those in and with power must take the lead and voluntarily seek to apply the spirit of the law, instead of seeing them as an unwelcome backstop.

For those looking to do so, there is no better place to start than with the five iRights principles. Giving effect to these will mean the law is adhered to and children and young people will be far better protected and empowered online.

LEGISLATION REFERRED TO

The Right to Remove

The Communications Act 2003

The Copyright Designs and Patents Act 1988

The Data Protection Act 1998

The General Data Protection Regulation [in draft]

The Defamation Act 2013

The Defamation (Operator of Websites) Regulations 2013

European Convention on Human Rights

Human Rights Act 1998

The Right to Know

The Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013

The Computer Misuse Act 1990

The Data Protection Act 1998

The Electronic Commerce (EC Directive) Regulations 2002

The Right to Safety and Support

The Communications Act 2003

The Coroners and Justice Act 2009

The Criminal Justice and Courts Act 2015

The Criminal Justice and Public Order Act 1994

The Education and Inspections Act 2006

The Malicious Communications Act 1988

The Protection from Harassment Act 1998

The Video Recordings Act 2010

The Education Act 2011

The Right to Make Informed and Conscious Choices

The Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013

The Consumer Contracts Act 2013

The Consumer Rights Act 2015

The Consumer Protection from Unfair Trading Regulations 2008

The Data Protection Act 1998

The Electronic Commerce (EC Directive) Regulations 2002

The General Data Protection Regulation [in draft]

The Minors' Contracts Act 1987

Sale of Goods Act 1979

The Unfair Terms in Consumer Contracts Regulations 1999

The Right to Digital Literacy

The Communications Act 2003

The Education Act 2002

DEFINED TERMS

"**Child**" and "**Young Person**" means a person under 18 unless otherwise stated.

"**Data controller**" means an individual, organisation and/or other corporate body who determines the purposes and manner in which any personal data are, or are to be, processed.

"**Data subject**" means an individual who is the subject of personal data. They are the person whom particular personal data is about.

"**Litigation Friend**" means a person appointed to make decisions about a court case on behalf of a child. A litigation friend brings legal claims on behalf of a child or young person under the age of 18.

"**Personal Data**" means data which relate to a living individual who can be identified from those data or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller. This includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

"**Sticky sites**" means content published on a digital platform or digital technology (including websites, apps, and games) which have the objective of sucking in a child or young user, causing them to want to remain on that platform for extended periods of time and/ or causing them to want to frequently return to that platform for further extensive periods of time.

1. THE RIGHT TO REMOVE

"Every child and young person under 18 should have the right to easily edit or delete any and all content they themselves have created, to own content they have created, and to have an easy and clearly signposted way to retract, correct and dispute online data that refers to them."

A. Children and young people in Europe can ask search engines to remove links to information about themselves which is irrelevant, out-dated or otherwise inappropriate[2]

- This gives children and young people the right to try to exert some control over their search engine results. For instance, they could ask for old school photos which show them in a negative and inaccurate light not to appear. The photos may still be on the school's website (unless they took action against the school too) but would be harder to find as they would not appear in, for example, a Google search.

- The removal request is made by a "take-down notice". There is no cost involved.

- Search engines will consider whether the information is inaccurate, inadequate, irrelevant or excessive[3] and whether they believe it is in the public interest for the information to appear in their search results. One of the ways they will consider what is in the public interest is by looking at the role the child or young person plays in public life. Given young people and children very rarely play a formal role in public life (it is not like, for example, they can be politicians), it would be rare for a search engine to argue there is public interest in publishing information about them on that basis.

- Links to sensitive data, such as information about a child's health, sexuality or religious beliefs, are more likely to be taken down following a request for its removal[4]. Where there is evidence that the search result is causing prejudice to the child or young person, this would be a factor in favour of removing it.

- If the information posted online relates to a trivial misdemeanour which the child or young person was later cleared of and which is no longer – or may never have been – the subject of public interest, the child or young person has good grounds to have the search results removed.

- A child or young person will have a good case to have links to inaccurate or irrelevant information which opens them up to risks such as identity theft or stalking taken offline.

- If a search engine wrongfully handles a take-down notice, it can be reported to the Information Commissioner's Office which may impose a penalty or serve a 'Stop Now' order, requiring organisations to take steps to ensure they comply with the law[5]. The Information Commissioner's Office is a signatory of iRights.

- Where data is inaccurate, there is also an important right to apply to the court for an order to rectify, block, erase or destroy links to the information – see below at section B.

B. In the future, people in Europe may have the right to have personal information removed if they posted it when they were young and do not want it to be online anymore[6]

- If this new law – known as the "Right to Erasure" - comes in, people in Europe will have the right to ask a data controller for personal data to be deleted, especially if the data was uploaded when they were a child or young person. Certain circumstances must be shown to apply, which include where the data is no longer necessary in relation to the purposes for which it was published.

- Other factors, such as the right to freedom of expression, will be balanced alongside the individual's right to erasure.

- If the request for erasure is accepted, all the data must be deleted without delay.

- This new law may address, for instance, the situation where employers and universities have turned away an individual on the basis of a background search revealing transgressions made by the individual when he or she was younger[7]. It would also apply to any information which led the institution to dismiss the young person, even if it is not transgressive.

- In order to have a data controller consider whether data ought to be deleted, it will be enough that the person posted the information when they were a child and that they no longer want it to be available fbecause it is no longer necessary in relation to the purposes for which it was originally collected or because its publication is not, in fact, necessary to protect their vital interests.

- There is not a fixed date for implementation of the law but it is expected to be 2018.

- At the moment the position in England and Wales is that the right for a child or a young person to apply to court for an order to rectify, block or destroy data is limited solely to where the court is satisfied that the data is inaccurate.[8]

C. Children and young people have the right to privacy online.[19]

- Children and young people have the right to respect for their private and family life, home and correspondence and are protected against the wrongful publication of their personal information.

- Children and young people's right to privacy shall not be interfered with by a public authority[20] except in accordance with the law and where it is necessary in a democratic society, where it is in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

- The "rights and freedoms of others" include the right to free speech against which the right to privacy has to be balanced.[21] Where there is a conflict between a child or young person's right to privacy and someone else's right to free speech, the courts must carry out a balancing exercise to decide how much weight should be given to privacy over the other freedom of expression. This is referred to as the 'ultimate balancing test'. Neither right has precedence over the other.[22] There must be an intense focus on the importance of the child or young person's rights being claimed against the rights of the individual asserting his or her right of freedom of expression. The justification for interfering with or restricting each right must be taken into account and the courts should accord primacy importance to the child's interests.[23]

- A child or a young person's right to privacy cannot be interfered with, for example, by individuals or organisations simply to enable them to pursue purely commercial interests. The only legitimate exceptions are the serious ones referred to above.

- What information is private information? One of the tests is whether another person would feel offended if they were placed in the same position as the child or young person. Essentially the Court will look at whether the child or young person has a reasonable expectation of privacy in the information published and will consider a range of factors including:

  - the nature of the information published;
  - whether the child or young person is identifiable from the information published;
  - the child's conduct disclosed in the information;
  - the place at which that conduct was happening;
  - the absence of consent for that information to be published;

- whether it was known or could be understood that the information was private;
- the effect of publication on the child or young person;
- the circumstances in which and the purposes for which the information came into the hands of the publisher.[24]

- Information about a child or young person's physical or mental health or condition; their emotional state; intimate details of personal relationships, financial information and information about their racial or ethnic characteristics is the type of information that a Court would regard as private.

- Private information can be conveyed through a photograph, even if there is no accompanying text. In fact, the law recognises photographs can sometimes be more intrusive than words.

- The law has led to the prevention of, for example, unpixilated photographs of children being published by newspapers and paparazzi agencies if the child's parents have not provided their consent.

- It is important to remember that all children and young people have the right to privacy, not just those connected to people in the public eye.

D. The right not to be defamed online

- The laws of defamation apply equally to children and young people as they do to adults and to the online world as much as to, for example, newspapers.

- A claim in defamation must usually be brought on behalf of a child or young person by their Litigation Friend up to the age 18.[11]

- It is important to remember that just because a statement is upsetting or offensive does not necessarily mean that a complaint can successfully be made in defamation. The courts have long recognised that humour at the expense of others is part of life. At the other end of the scale, if a message contains a statement that is grossly offensive, the person who sent it could have committed a criminal offence.[12]

- There are lots of definitions of the word 'defamatory', but perhaps the most famous is whether the statement would 'tend to lower the person in the estimation of right-thinking members of society generally'.[13] It is also necessary to show that the statement has caused or is likely to cause serious harm to that person's reputation.[14]

- A civil claim can be brought against someone posting defamatory allegations about a child or young person. This is unless certain defences apply (such as that the information is true, it represents someone's honest opinion, is a matter of

public interest and/or the circumstances in which the allegations were made are of the sort that are covered by 'privilege')[15].

- Operators of websites have a defence if they did not post the defamatory statement on their website.[16] That defence will be defeated if the operator is shown to have acted with malice, or if the statement was posted anonymously (so that it was not possible for the child or young person to identify the poster) and the operator was given a 'notice of complaint' but failed to respond to it properly.[17]

- Operators of websites are permitted to remove anonymous defamatory statements when the child or young person has filed a notice of complaint and if the anonymous poster fails to respond or agree to have the statement removed.

- If the anonymous poster tells the website operator he or she does not want to reveal their name or address to the child or young person, or if the poster does not want the defamatory comments to be taken offline, the operator must inform the child or young person that this is the case.[18] They are then left having to try to take action against the individual, notwithstanding the lack of information. This would require an application to the court, seeking an order that the website operator must tell the child or young person who the poster is or where they are located so that the child or young person can take action. This is not guaranteed and can be expensive.

E. A young person or child has the right to stop a website from publishing photos or images they have created in which they own the copyright[9]

- If a child or young person takes a photo, they will generally own the copyright in it.

- That means that if they do not want someone else to publish that photo (for example on a friend's blog or digital platform), they can ask for it to be removed.

- Most social media sites, blog spots and website operators have processes which go towards quickly dealing with copyright removal requests.[10]

- There are defences which might apply to a claim in copyright infringement but freedom of expression is not one of them.

- The list of creations in which that copyright is found in also includes literary, dramatic, musical and artistic works, sound recordings, broadcasts and films (this includes videos recorded on a smartphone and uploaded onto the internet).

2. THE RIGHT TO KNOW

"Children and young people have the right to know who is holding or profiting from their information, what their information is being used for and whether it is being copied, sold or traded.

"Children and young people can only be asked to hand over personal data when they have the capacity to understand what they are doing and what their decision means. Terms and conditions aimed at young people must be written so that children and young people can easily understand them."

A. Parental consent would normally be required when collecting personal data from children under 12 [25]

- Children and young people have the right to be presented with digital content and online platforms which, when targeted specifically at them, have been designed in such a way that precautions are taken and good practices adopted to ensure that people handling their data do so fairly[26].
- Some form of parental consent would normally be required before collecting personal data from children under 12[27]. It is for the person processing the child or young person's data to consider the appropriate form for obtaining consent. The Information Commissioner's Office guidance provides two examples:
  - Where information such as an email address and the child's date of birth is being collected, sending an email to the parent may be sufficient;
  - If a child or young person's photograph is being displayed on a website, the data controller may require a signed consent form or email acknowledgement from the parent.
- If a child or young person is asked to provide information about other children or young people (for example, if they want to arrange for a newsletter to be sent to a friend), the digital platform should consider whether they need to take additional measures to reduce any risk to those children and young people[28].

B. Children and young people have the right to try and find out what information any 'data controller' is holding about them, why it is being processed and who it is being shared with[29]

- To try to find out what information a 'data controller' such as an online company holds, a child or young person can make a "subject access request". This is a request, made in writing accompanied by a £10 fee. There is no mandatory form that has to be completed[30]. Subject access requests may be free under the new Data Protection Regulation.

- The child or young person can request:

  - to know what, if any, personal data (such as photos of them, information about their hobbies etc) the organisation is processing, why it is processing the data, which organisations or people the data has been or may be given to and any available information as to the source of the data;

  - to also be given a copy of the information containing the data; and

  - in some cases where an automated decision has been made about them, to know the reasoning behind the decision (although because automated decisions tend to be made about matters such as creditworthiness etc, this seems less likely to apply to a child).

- A child or young person's personal data belongs to them however young they are and even if they are too young to understand about subject access requests.

- When a subject access request for information held about a child is made, the response must be made to the child or young person rather than their parent if the person responding is confident that the child or young person would be able to understand the information they would be provided with[31].

- In most cases, the organisation needs to respond to the subject access request within 40 days.

- A data controller can refuse a request in certain circumstances such as if the personal data is being processed for the prevention or detection of crime. Some of these exemptions are less likely to apply to children and young people than they are to adults.

C. Children and young people have a right to know how and when their information will be used by an organisation operating online

- Children and young people buying goods from a seller have a right to be presented with terms and conditions which are expressed in plain and intelligible language.[32]

- Privacy notices for websites and digital technologies which set out how data is collected and processed, and cookie policies which set out how a website uses cookies, should be communicated in plain language. The draft Data Protection Regulation will also contain rules on 'transparency'.[33]

- Children and young people have a right to be told the purpose or purposes for which their infromation will be used. This can be provided in fairly generic terms, for example, "your personal information will be used to target online advertising at you".

- Children and young people have a right not to have their information used in a way that would unjustifiably have a negative effect on them.[34]

D. Children and young people have the right to have their personal information stored online protected

- It is illegal to access material from a child or young person's computer without their consent.[35] This includes hacking as well as using someone's computer in a way that they have not been authorised to do (eg sneaking a look at someone's emails when they've borrowed their computer to do homework on).

- A third party data controller publishing a child or young person's personal data online has a legal duty to take measures towards protecting that information.[36]

- Children and young people will have the right to know if their personal information has been hacked under the new Data Protection Regulation[37] and the Cybercrime Directive 2013/40/EU (which is due to be implemented in the UK on 1 October 2015).

3. THE RIGHT TO SAFETY AND SUPPORT

"Children and young people should be confident that they will be protected from illegal practices and supported if confronted by troubling or upsetting scenarios online.

"Children and young people have a right to receive an age-appropriate, comparable level of adult protection, care and guidance in the online space as in the offline world. And that all parties contribute to common safety and support frameworks easily accessible and understandable by young people."

Protection and support should be readily available for those that encounter troubling or upsetting scenarios online, but in some instances, the conduct encountered goes beyond this and enters into the realm of criminal behaviour. For the purpose of this report, we restrict ourselves to considering the ways in which the law protects children and young people from criminal conduct.

In all instances it will be necessary to report the matter to the police. The most appropriate route to access the police may vary depending on when and where the criminal behaviour occurs. For example it could be by the young person directly, a friend, a parent or adult with parental responsibility for the young person or by way of a referral from the school.

Children below the age of 10 are deemed not to be capable of committing a crime. Young people below the age of 18 can be prosecuted for a criminal offence. The police and Crown Prosecution Service must have particular regard to whether it is in the public interest to charge someone with a criminal offence if they are between the age of 10 and 18.

This is not an exhaustive list but the key legal protections that are available are as follows:

A. It is illegal to harass a child or young person online or via an electronic device[38]

- A child or young person has the right not to be harassed online.
- Cyber bullying, trolling or virtual mobbing could amount to civil harassment if done repeatedly and the person doing it knows or should have known that the conduct will cause alarm or distress.
- It is a high threshold as the law needs to distinguish between unpleasant behaviour, which should still be permitted in a free society, and unacceptable behaviour, to which a punishment should be attached.
- The court can make orders to prohibit a person from harassing someone else.
- Identifying who is behind harassment could be an issue if the perpetrator is acting anonymously. In such circumstances, there are procedures – including "Norwich Pharmacal" applications – which help identify who is behind anonymous posts and accounts. These entail applying to court and their success often depends on how sophisticated the perpetrator is in covering their tracks.

B. It is illegal to send grossly offensive messages to children or young people or about them to third parties

- It is a criminal offence for a person to send an online communication, phone message or communication by any other electronic device which is:
  - threatening or menacing in character, or
  - indecent, obscene, grossly offensive (e.g. highly abusive or insulting), threatening or false
  - intending to cause a child or young person distress or anxiety.[39]
- The offence is aggravated if the language used picks on a child or young person's race, religion, sexual orientation or gender identity.
- An offence is committed simply by sending this kind of message. This means that there is no requirement that the child or young person actually sees the message or is offended by it.

C. It is an offence to use the internet or any electronic device to encourage or assist a child or young person to commit suicide

- This can include putting pressure on another person via social media to commit suicide.[40]

D. The internet cannot be used to sexually exploit a child or young person

- It is an offence to:
  - make, take or permit to be taken, or to distribute or possess, indecent images of a child,[41]
  - with the intent of causing someone distress, post a private sexual photograph or film of them without their consent of the person. This includes situations where someone retweets or forwards, uploads, shares by text or email sexual images or films with the aim of causing distress to the person depicted in the photograph or film.[42] This is the new so-called "Revenge Porn" law.
  - intentionally cause a child to watch another person engaging in sexual activity or view an image of a person engaging in sexual activity, with the intention of obtaining sexual gratification.[43]
  - communicate with a child with the intention of arranging to meet with them to commit a sexual offence against them.[44]

E. A child and young person has the right to be protected against cyber-bullying by their school

- The Head Teacher must put in place measures to prevent bullying among pupils, including cyber bullying.[45]

- Schools can conduct a search for and examine pupils' electronic devices if they think they are likely to be used to commit an offence. The school can then delete files or retain the electronic device if they think there is good reason to do so.

- If the member of staff finds pornographic images on a child or young person's electronic item, they may dispose of the image unless it is extreme in which case they must deliver it to the police.

- The NSPCC and CEOP are very active in this area.

F. Children and young people must be protected from exposure to depictions of violence, self-harm, criminal offences and sexual activity in online videos and games[46]

- Children and young people have a right to be protected from potentially harmful or otherwise unsuitable media content.

- To ensure that children and young people are protected from unsuitable and harmful content in films and videos, the British Board of Film Classification (BBFC) examines and age rates all films and videos before they are released[47], as well as all video games with strong pornographic content.[48]

- As well as this, an additional level of protection is afforded to children and young people from the Video Standards Council (VSC)[49] which protects children and young people from potentially unsuitable material[50] which includes online sites making video games available to the public within its scope.[51]

- User generated postings of violence or other depictions of criminal offences or sexual activity are said to be dealt with by social media technologies on a case by case basis, in line with their policies[52]. If the content constitutes a credible threat of violence, specifically targets an individual and/ or is grossly offensive, indecent, obscene or false, it could result in criminal prosecution.[53]

G. Some mobile phone providers will automatically block age restricted content

- Children and young people can be automatically protected from some age restricted content otherwise readily available to them via their smartphone.

- Content which has been classified as 18+ by the BBFC will be automatically blocked by some providers[54] in accordance with the OFCOM code of practice and the UK Code of Practice for the self-regulation of content on mobiles.[55] Children or young people will not be able to access that content without providing proof of age.

H. Advertisers and media owners have a responsibility to ensure that advertising for video games and films is responsible

- Consideration should be given to protecting children and young people from advertising games or videos which depict, for example, graphic violence and/or the gratuitous use of nudity.[56]

I. Care must be taken when featuring or addressing children in marketing communications[57]

- Children and young people have a right not to suffer physical, mental or moral harm as a result of marketing communications addressed to or targeting children (someone under 16 in this instance).[58]

- Online sellers and online marketers must take care not to promote products that are unsuitable for children and they must not encourage children to copy practices which might be unsafe.[59]

4. THE RIGHT TO MAKE INFORMED AND CONSCIOUS CHOICES

"Children and young people should be free to reach into creative and participatory places online, using digital technologies as tools, but at the same time have the capacity to disengage at will."

A. Care must be taken when communicating marketing to children and young people[60]

- Children and young people have a right to be protected from the impact of irresponsible marketing. Any marketing communications targeted at children (who are under 16 for this purpose) must not exploit their credulity, vulnerability or lack of experience.[61]
- Children and young people have a right not to be made to feel inferior or unpopular for not buying the product being advertised.[62]
- Children and young people must easily be able to judge the size, characteristics and performance of the products being advertised[63] and must be able to distinguish between real-life situations and fantasy.[64]
- Children and young people have a right not to be exposed to marketing communications addressed directly to them which exaggerate what is attainable by an ordinary child using the product. Children and young people have a right not to be exploited because of any susceptibility to charitable appeals and promotions.[65]
- Children and young people must not be actively encouraged by marketing communications to pester their parents or undermine parental authority to purchase a product or urge a child to persuade their parents to buy an advertised product for them.[66]

B. Particular care must be taken when broadcasting gambling advertisements or producing non-broadcast marketing communications about gambling to ensure that children or young persons are not harmed or exploited [67]

- Children (in this case, people under 15) and young persons (aged 16 or 17) have a right to be protected from the temptation of online gambling.

- Marketing communications for gambling must not be created in such a way that will be particularly appealing to children or young people. Children and young people must not be exploited and gambling marketing should not suggest peer pressure or that gambling is a rite of passage[68]. To this end:

  - Marketing communications and advertisements must not suggest that gambling can enhance personal qualities (such as linking gambling to sexual success, enhanced attractiveness or toughness or as providing an escape from personal difficulties or troubles);[69] and

  - Marketing communications and advertisements must not encourage gambling behaviour that is socially irresponsible or that could lead to financial, social or emotional harm, or condone or encourage criminal or anti-social behaviour.[70]

C. Children and young people can ask website operators not to subject them to automated decision-taking[71]

- A child or young person has a right to be told if an organisation makes an automated decision about them. "Automated decisions" are decisions about a child or young person based on personal information that has been put into the online world by them. In practice, children and young people are less likely to be the subject of automated decision making than adults but it is still foreseeable.

- If a child or young person discovers that they are the subject of automated decision making and they have not been told, they can stop this happening by giving written notice prohibiting the business from taking any automated decisions using their personal data.

- New law[72] may broaden the protection afforded to children and young people in respect of 'behavioural profiling'. Under the new law, every child or young person would generally have the right not to be subject to a measure which produces legal effects concerning them or which would significantly affect them, which is based solely on automated processing intended to evaluate certain personal aspects or to analyse or predict the child or young person's location, economic situation, health, personal preferences or behaviour.

D. On the whole, children and young people cannot form contractually binding relationships before they turn 18 years old

- The law recognises that children and young people may not be capable of making informed choices when it comes to entering into contracts online, and assists children or young people who may have unwittingly entered into a contract with an online trader.

- A contract entered into by a child or young person under the age of 18 is usually voidable. It will become binding on the child or young person if, at the age of 18, he or she gives formal consent to the contract.

- In an important exception, contracts for "necessaries" made with children under 18 are enforceable as long as the terms of the contract are not, for example, so harsh or oppressive as to be unenforceable.

- "Necessaries" include life essentials like food, drink, medicine, legal or medical services or an apprenticeship or education.[73] What amounts to a "necessary" item changes with time; interesting questions arise as to whether a smartphone, for example, is a necessity in today's digital age. The burden is on the trader to show that the goods supplied to the child were "necessaries". A child or young person is only bound to pay the reasonable price for the necessaries and not the contractual price, which may be higher.[74]

- Generally, the child or young person must be old enough to understand the nature of the transaction and, if the contract imposes obligations on the child, the child must be old enough to understand the nature of the obligations.[75]

- If a minor enters into a contract to buy goods, some of which are "necessaries" and some of which are not, the minor will only have to pay a reasonable price for the necessaries; the child or young person will not be bound to pay for the remainder of the goods contracted for.[76]

- Any other contract can be cancelled by the child or young person if they can show that they did not fully understand the

implications of the contract.[77] When cancelling the contract, the child or young person will have to return the goods they bought or an equivalent sum of money where the goods can no longer be returned for any reason.[78]

- 'Unfair' contract terms are not enforceable (e.g. if the language is unclear or hidden in the small print), whether the contract is with a child or adult.[79] An example of potentially unfair contract terms is where there are hidden charges in contracts.

- If a child or young person under 18 fraudulently misrepresents their age when purchasing goods, the child can be compelled to return the goods.

- If the child or young person no longer has the goods, they cannot be compelled to pay an equivalent sum to the seller.[80]

E. Contract law protects children and young people who cannot fully understand the significance and implications of a contract

- Children and young people have a right to expect consumer information to be communicated clearly and comprehensibly.[81]

F. Adult permission must be obtained before minors under 16 can buy complex or costly products

- Parental or adult consent must be given to a seller before a person under the age of 16 can buy anything very complicated or costly.[82]

G. A person cannot mislead a child or young person about a product they are selling, or hide information from them

- A trader cannot mislead a child or young person about the price or about the risks associated with the product or engage in a practice which causes or is likely to cause the average consumer to take a transactional decision he or she would not have taken otherwise. It is a criminal offence to do so.[83]

- A trader cannot hide or leave out information which the average child or young person needs to make a decision when thinking about buying the product and where the practice causes or is likely to cause the average consumer to take a transactional decision he or she would not have taken otherwise.[84]

- A trader cannot use aggressive methods to pressure a child or young person to make a choice about purchasing a product which they would not have otherwise taken and where the practice significantly impairs or is likely to significantly impair the average consumer's freedom of choice or conduct in relation to the product concerned through the use of harassment, coercion or undue influence.[85]

- In determining the effect of a commercial practice on the average consumer, where a clearly identifiable group of consumers is particularly vulnerable to the practice or the underlying product because of their age in a way the trader could reasonably be expected to foresee and where the practice is likely to materially distort the economic behaviour of that group, a reference to the average consumer shall mean an average member of that group.[86]

- Online traders and a person providing a service by electronic means must make their email address available to children or young people to make it possible to contact him rapidly and communicate with him in a direct and effective manner in relation to a product being sold online.[87]

- An online trader or service provider shall ensure that any unsolicited commercial communication sent by him by electronic mail is clearly and unambiguously identifiable as such as soon as it is received.[88]

- Service providers must also ensure that any promotional offer they send out to a child or young person (including any discount) is easily identifiable as such. Any conditions attached to the promotion must be easily accessible and presented clearly and unambiguously.[89]

H. The online and app-based games industry must not exploit children's inexperience, vulnerability, credulity including by aggressive commercial practice[90]

- Information about the costs associated with a game should be provided clearly, accurately and prominently up-front, before the child or young person consumer begins to play, download or signs up to the game.[91]

- Those costs should be broken down and specify the initial cost of signing up, any subsequent costs that are unavoidable if the child or young person wishes to continue playing the game and optional extra costs, including in-game purchases.[92]

- Games should not include practices that are aggressive, or which otherwise have the potential to exploit a child or young person's inherent inexperience, vulnerability or credulity or to place undue influence or pressure on them to make a purchase. The language, presentation, design and structure of the game should take account of that.[93]

- A game should not include direct pressures to children or young people to make a purchase or persuade others to make purchases for them.[94]

- Payments should not be taken from the payment account holder unless authorised. A payment made in a game is not authorised unless express, informed consent for that payment has been given by the payment account holder.[95]

- All information about the material characteristics of the game should be provided clearly, accurately and prominently before the child or young person begins to play the game.[96]

5. THE RIGHT TO DIGITAL LITERACY

"To access the knowledge that the internet can deliver, children and young people need to be taught the skills to use and critique digital technologies, and given the tools to negotiate changing social norms.

"Children and young people should have the right to learn how to be digital makers as well as intelligent consumers, to critically understand the structures and syntax of the digital world, and to be confident in managing new social norms. To be a 21st century citizen, children and young people need digital capital."

OFCOM has a duty to promote learning by children and young people about using the internet[97]

- OFCOM, the organisation responsible for regulating the broadcasting and telecommunications industries, has a statutory duty to promote media literacy, which enables people, including children and young people, to have the skills, knowledge and understanding to make full use of services such as the Internet.[98]

- OFCOM's responsibility involves the organisation considering how children and young people put information onto the Internet and understand what the potential risks are with the online world.[99]

Schools are required to teach children and young people about the internet

- Children and young people must be taught a wide range of information about using the internet by their school in accordance with the National Curriculum.[100]
- They must be taught how to use technology responsibly, safely and respectfully from the age of 6 (Key Stage 1).
- They must be taught about keeping personal information private from the age of 6 (Key Stage 1).
- Schools must teach children and young people to be able to identify where to go for help and support when they have concerns about content on the internet and other online technologies from the age of 6 (Key Stage 1).
- From Key Stage 2 level (aged between 7 and 11), children and young people must be taught how to recognise behaviour that is unacceptable in the online environment.[101]
- Schools must ensure that their pupils learn about the opportunities available to them through the internet and other online technologies.
- Children and young people must be taught how to use search technologies effectively including understanding how search results are selected and ranked.
- Children and young people must be taught to be discerning in evaluating what they put online.
- Children and young people must be taught the fundamental principles and concepts of computer science.[102]
- From Key Stage 3, schools must teach children and young people to learn how to select, use and combine a variety of software (including internet services) on a range of devices to design and create a range of programs, systems and content that accomplish their chosen goals, including learning how to collect, analyse, evaluate and present data and information.[103]
- School Inspectors should consider the effectiveness of safeguarding arrangements to ensure that there is a promotion of safe practices, including online safety.[104]

LIMITATIONS OF THE LAW

As the above demonstrates, there is a strong legal framework supporting iRights. But it is somewhat theoretical at present as children and young people are not enjoying the full protection that the law offers. We attribute this chiefly to a lack of implementation, resourcing and education, and the cost, stress and complexity of pursuing legal action to enforce legal rights.

To expand on just a few of the practical limitations with the current system:

- There is a lack of investment in compliance systems. The law provides a child or young person with a right to complain to websites or digital content platforms about intrusive personal material posted online. Yet this legal right is undermined by the number of weeks it can take to process that complaint, in part due to systems not being adequately resourced; meanwhile the offending material remains online continuing to cause distress. The speed with which information can go viral online contrasts starkly with the pace at which rights are protected.

- Compounding this unsatisfactory reality is the fact that it can be extremely hard for a child or young person to know where to direct a request for material to be removed. Many websites do not distinguish between children, young people and adults and therefore a 'same size fits all' policy is applied. There is no legislative requirement for a standardised child-friendly complaint system to be implemented across all forms of digital platforms.

- Further, when a child or young person complains about material posted online, the host is not bound to assist in the blocking and/ or removal until such time as an internal investigation upholds or otherwise determines the complaint. In the case of children and young people perhaps there should be a requirement that upon receipt of a complaint in the required form, the web host or operator must remove the offending material within a certain time frame pending the outcome of an investigation.

- Until the "Right to Erasure" under the draft Data Protection Regulation comes into force, a child or young person needs to show that personal data published online is irrelevant, out-dated or otherwise inappropriate in order to force its removal. Mere distress caused by the content being published is not a legal ground for removal but in most cases, the need for urgent removal arises out of the distress caused.

- The draft Data Protection Regulation is due to be enacted in 2016 following which there will be a two year period to allow businesses to adapt to the new law before it comes into force. This means that children and young people will not benefit from these changes in the law for at least three years. Children and young people need to have the Right to Erasure now.

- The United Nations Convention signed on the Rights of the Child 26 years ago is the gold standard for children's rights. In that time, there has been a technological revolution which has impacted immeasurably on the lives of children with no corresponding change to the UNCRC.

A new protocol that describes how the rights embodied in the UNCRC should be interpreted in digital environments is therefore required.

- The protections offered to children by legislation are not user-friendly and often only present a remedy through taking court action. The Government need to seek better ways in which existing legislation can be routinely implemented on behalf of children and young people.

- There is currently no legal requirement for a business to notify the ICO or the individuals in question of personal data breaches. The only safety net is that businesses will face a higher fine from the ICO if they do not notify individuals of data breaches where those individuals might have been able to do something to limit the impact of the breach on them.

- There is a lack of regulation of sticky sites In particular:
  i. There is no obligation on sticky sites to obtain parental consent before children and young people start using them. Such safeguards exist in other industries; in the food industry the traffic light system used on lots of products allows the potential purchaser to immediately see that a food product is high in fat or sugar, when it is marked red.
  ii. This area calls for greater regulation and mandatory safeguards (perhaps including two factor authentication, with the parent or guardian required to provide consent before use) to ensure that parents of children and young people know which sticky sites are diverting their children's' attention and how much of their money is being spent on such games.

- There is no legal requirement for those involved in the video gaming industry to be a member of the Video Standards Counsel. Further, there is no legislation which underpins the VSC code, undermining the impact it has in reality.

- There is no requirement for children and young people to be taught about advertising in the digital world; that businesses pay significant amounts of money to advertise and that advertising can be targeted at specific groups of people and age ranges. Arming children with an understanding of advertising will assist them to evaluate the appeal of products they see on social media sites, apps and on YouTube videos.

- A fundamental and well-rehearsed concern is that the web is global and gives children and young people access to digital platforms and technologies all over the world. But legal access to the underlying entities behind these digital platforms for the purpose of enforcing legal rights and empowering children and young people is inevitably difficult wherever they are and particularly if they are outside the jurisdictional reach of Europe. The laws created by England, Wales and the European Union are not necessarily reciprocated by other countries and do not necessarily extend to websites hosted in other countries. It is difficult to enforce an English court order demanding a website take down offensive material against websites in countries outside Europe. When it comes to children and young people, more international co-operation is required.

EPILOGUE

The above demonstrates that the law of England and Wales broadly supports the five iRights.

But, clearly, that's not the whole story as the law is not being actively applied. The results from iRights' youth juries suggest young people do not feel empowered to control personal information.

Compiling some of the most relevant law in one place will help address that. We hope this report will be the first port of call for young people and those seeking protection and empowerment in the digital age.

The next step, in our view, is to help companies adhere to the spirit of the law as well as the strict letter. Our sense is that there's a big appetite to "do the right thing" by children and young people online, but there is uncertainty as to what that entails in practical terms.

Consequently, our next undertaking is to produce guidelines showing what "doing the right thing" looks like in practice. It is essential these are grounded in the real world, so we will be consulting stakeholders to find a way to marry commercial and practical requirements with the pressing need for children and young people to be empowered and protected.

If you would like to provide input please contact Schillings - enquiries@schillings.co.uk - and watch this space for our next report.

LAW AT THE SPEED OF REPUTATION

Schillings assist prominent individuals and businesses wherever they are in the world; whatever their reputation and privacy issues.

From hostile hacks, to cyber-attacks and shaky suppliers, successful individuals and businesses face a huge variety of threats with the potential to negatively affect their reputations. Whether it's identifying threats, defending reputation or protecting privacy, Schillings' multidisciplinary approach safeguards client reputations – whatever the threat.

Likewise, Schillings Family is adept at handling the big, often life changing events in the family lives of successful individuals with skill, professionalism and discretion. Schillings Family also has unmatched experience in representing companies, banks and financial institutions as well as trustees and other third parties who may become involved in financial proceedings upon divorce.

END NOTES

1. 'The Right to Privacy' S. Warren and L. Brandeis (4 Harvard L.R. 193 (Dec. 15, 1890))
2. *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González* (2014) C-131/12
3. Principles 3 and 4, Schedule 1, Data Protection Act 1998
4. Section 2 Data Protection Act 1998; higher conditions for Sensitive Personal Data set out in Schedule 3 Data Protection Act 1998
5. https://ico.org.uk/about-the-ico/what-we-do/taking-action-data-protection/
6. Article 17 of the General Data Protection Regulation [Draft]
7. Articles 6, 16, 17, 19 of the General Data Protection Regulation [Draft]
8. Principle 6 of the Data Protection Act 1998
9. Section 96 Copyright, Designs and Patents Act 1988
10. https://www.facebook.com/help/contact/208282075858952; https://support.twitter.com/forms/abusiveuser; https://www.snapchat.com/terms; https://www.tumblr.com/policy/en/terms-of-service#dmca; https://support.twitter.com/articles/15795-copyright-and-dmca-policy
11. https://www.justice.gov.uk/courts/procedure-rules/civil/rules/part21
12. Section 1 Malicious Communications Act 1988; Section 127 Communications Act 2003; Refer to Section 3 of the Report
13. *Sim v Stretch* [1936] 2 All ER 1237
14. Section 1 Defamation Act 2013
15. Sections 2 – 7 Defamation Act 2013
16. Section 5 Defamation Act 2013; The Defamation (Website Operators) Regulations 2013.
17. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/269138/defamation-guidance.pdf
18. Paragraph 8, Schedule, The Defamation (Website Operators) Regulations 2013; additional provisions outside the scope of this report also apply to the online sphere e.g. s. 10 Defamation Act 2013; s. 1 Defamation Act 1996; Regulation 19 of the Electronic Commerce (EC Directive) Regulations 2002 (SI 2002/2013)
19. Article 8, Schedule 1, Part 1 of the Human Rights Act 1998
20. Which includes a court or tribunal or any person certain of whose functions are functions of a public nature: Section 6(3)(a) and (b) of the Human Rights Act 1998
21. Article 10, Schedule 1, Part 1 of the Human Rights Act 1998
22. Re S (A Child) [2003] EWCA Civ 963
23. *K v News Group Newspapers Ltd* [2011] EWCA Civ 439
24. *Weller v Associated Newspapers Limited* [2014] EWHC 1163 (QB)
25. Part of the remit of the Information Commissioner is to educate UK citizens about data protection law, so the ICO generally provides easy-to-use guides to the rights and responsibilities of data subjects and data controllers under data protection law. All data controllers have an obligation to ensure that data protection policies are communicated in clear and plain language, particularly if the website (for instance) is targeted at a child. Examples of such guides are referred to in this section.
26. https://ico.org.uk/media/for-organisations/documents/1591/personal_information_online_cop.pdf
27. https://ico.org.uk/media/for-organisations/documents/1591/personal_information_online_cop.pdf
28. https://ico.org.uk/media/for-organisations/documents/1591/personal_information_online_cop.pdf.
29. Section 7 Data Protection Act 1998
30. https://ico.org.uk/media/for-organisations/documents/1065/subject-access-code-of-practice.pdf
31. https://ico.org.uk/media/for-organisations/documents/1065/subject-access-code-of-practice.pdf
32. In this sphere see also, for example, the Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013; and Electronic Commerce (EC Directive) Regulations 2002

33. The ICO emphasises the need for transparency in this context: https://ico.org.uk/media/for-organisations/documents/1610/privacy_notices_cop.pdf
34. Fair processing: https://ico.org.uk/for-organisations/guide-to-data-protection/?template=pdf
35. Section 1 Computer Misuse Act 1990
36. Principle 7, Schedule 1 Data Protection Act 1998
37. http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.
38. Protection from Harassment Act 1997
39. Section 1 Malicious Communications Act 1988; Section 127 Communications Act 2003.
40. Section 59 Coroners and Justice Act 2009
41. Section 1 Protection of Children Act 1978
42. Section 33 Criminal Justice & Courts Act 2015
43. Sections 12 and 13 Sexual Offences Act 2003
44. Section 15 Sexual Offences Act 2003
45. Section 89(2) The Education and Inspections Act 2006
46. http://www.bbfc.co.uk/sites/default/files/attachments/BBFC%20Classification%20Guidelines%202014_0.pdf
47. Video Recordings Act 2010
48. Page 11 of http://www.bbfc.co.uk/sites/default/files/attachments/BBFC%20Classification%20Guidelines%202014_0.pdf
49. http://videostandards.org.uk/VSC/
50. http://videostandards.org.uk/VSC/origins.html
51. http://www.pegionline.eu/en/index/id/232/
52. https://support.twitter.com/groups/56-policies-violations; https://www.facebook.com/policies/; https://www.snapchat.com/terms; https://www.tumblr.com/policy/en/terms-of-service
53. http://www.cps.gov.uk/legal/a_to_c/communications_sent_via_social_media/index.html#a04; http://www.cps.gov.uk/legal/a_to_c/communications_sent_via_social_media/index.html
54. http://www.o2.co.uk/help/everything-else/age-restricted-content-and-age-verification; http://talkmobile.co.uk/restricted
55. http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/ukcode.pdf; http://www.mobilebroadbandgroup.com/documents/UKCodeofpractice_mobile_010713.pdf
56. http://www.cap.org.uk/~/media/Files/CAP/Help%20notes%20new/Guidance_video_games_and_films.ashx
57. Section 5 CAP Code
58. Rule 5.1 CAP Code
59. Rules 5.1.4 and 5.1.5 CAP Code
60. Rule 5 CAP Code
61. Rule 5.2 CAP Code
62. Rule 5.2.1 CAP Code
63. Rule 5.2.3 CAP Code
64. Rule 5.2.3 CAP Code
65. Rules 5.3.1 and 5.3.2 CAP Code
66. Rule 5.4.2 CAP Code
67. Rule 16.1 CAP Code; Rule 17.3 BCAP Code
68. Rule 16.3 CAP Code; Rule 17.3.9 BCAP Code
69. Rule 16.3 CAP Code; Rule 17.3.7 BCAP Code

70. Rules 16.3.1 and 16.3.16 CAP Code
71. Section 12 Data Protection Act 1998; Articles 19 and 20 of the General Data Protection Regulation [Draft]
72. Article 15 of the General Data Protection Regulation [Draft]
73. *Walter v Everard* [1891] 2 QB 369
74. Section 3 Sale of Goods Act 1979
75. Chitty on Contract, 8-0003, p 757
76. Chitty on Contract, 8-015, p 762
77. *R v Oldham Metropolitan BC, ex p. Garlick* [1993] 1 FLR 64
78. Section 3 Minors' Contracts Act 1987
79. Regulations 6 and 8 of the Unfair Terms in Consumer Contract Regulations 1999; Section 62(1) Consumer Rights Act 2015
80. Chitty on Contract, 8-052, p 779
81. Section 9(1) Consumer Contracts Regulations 2013 (SI 1999/2083)
82. Rule 5.2.4 CAP Code
83. Regulation 5, The Consumer Protection from Unfair Trading Regulations 2008
84. Regulation 6, The Consumer Protection from Unfair Trading Regulations 2008
85. Regulation 7, The Consumer Protection from Unfair Trading Regulations 2008
86. Regulation 2(5), The Consumer Protection from Unfair Trading Regulations 2008
87. Paragraph c of Schedule 2, Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013 (no. 3134); Regulation 6(1) Electronic Commerce (EC Directive) Regulations 2002 (no.2013)
88. Regulation 8, Electronic Commerce (EC Directive) Regulations 2002 (no.2013)
89. Regulations 7 and 8, Electronic Commerce (EC Directive) Regulations 2002 (no.2013)
90. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/288360/oft1519.pdf
91. Principle 1 of the Principles for Online and App-based Games (Office of Fair Trading)
92. Principle 1 of the Principles for Online and App-based Games (Office of Fair Trading)
93. Principle 6 of the Principles for Online and App-based Games (Office of Fair Trading)
94. Principle 7 of the Principles for Online and App-based Games (Office of Fair Trading)
95. Principle 8 of the Principles for Online and App-based Games (Office of Fair Trading)
96. Principle 2 of the Principles for Online and App-based Games (Office of Fair Trading)
97. http://stakeholders.ofcom.org.uk/market-data-research/other/media-literacy/
98. http://stakeholders.ofcom.org.uk/market-data-research/other/media-literacy/; Section 11 Communications Act 2003
99. http://stakeholders.ofcom.org.uk/market-data-research/media-literacy-pubs/
100. s. 84 (3) Education Act 2002
101. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/335116/Master_final_national_curriculum_220714.pdf
102. http://www.computingatschool.org.uk/data/uploads/CASPrimaryComputing.pdf ; http://www.computingatschool.org.uk/data/uploads/cas_secondary.pdf
103. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/335116/Master_final_national_curriculum_220714.pdf
104. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/391531/School_inspection_handbook.pdf

CONTACT

Schillings
+44 (0)20 7034 9000
enquiries@schillings.co.uk
www.schillings.co.uk

www.schillings.co.uk