Law Society of Scotland

Consultation Response

The Right to Privacy (Article 8) and the Digital Revolution

February 2019

Introduction

The Law Society of Scotland is the professional body for over 11,000 Scottish solicitors. With our overarching objective of leading legal excellence, we strive to excel and to be a world-class professional body, understanding and serving the needs of our members and the public. We set and uphold standards to ensure the provision of excellent legal services and ensure the public can have confidence in Scotland's solicitor profession.

We have a statutory duty to work in the public interest, a duty which we are strongly committed to achieving through our work to promote a strong, varied and effective solicitor profession working in the interests of the public and protecting and promoting the rule of law. We seek to influence the creation of a fairer and more just society through our active engagement with the Scottish and United Kingdom Governments, Parliaments, wider stakeholders and our membership.

The Society's Privacy Law and Constitutional Law Sub-committees welcome the opportunity to consider and respond to the Joint Committee on Human Rights' inquiry into *The Right to Privacy (Article 8) and the Digital Revolution*.[1] We have the following comments to put forward for consideration.

Response to questions

Q1. Are some uses of data by private companies so intrusive that states would be failing in their duty to protect human rights if they did not intervene?
- If so, what uses are too intrusive, and what rights are potentially at issue?

We have no data on the extent to which private companies are using data in an intrusive way. However, we can envisage situations where states could be regarded as failing in their duty to protect human rights if they did not intervene.

The safeguards set out in the General Data Protection Regulation[2] as implemented through the Data Protection Act 2018 go a long way to addressing potential concerns in a UK context. However, consumers may not fully understand the potential impact that certain uses of their data might have. Education around consent to use of data may be important in this regard.

[1] https://www.parliament.uk/business/committees/committees-a-z/joint-select/human-rights-committee/inquiries/parliament-2017/right-to-privacy-digital-revolution-inquiry-17-19/

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679

Furthermore, rules must be enforced if they are to fulfil their objective: the protections offered by existing legislation require efficient and effective enforcement. It is therefore imperative that the ICO is fully resourced to carry out its duties.

The most obvious rights at issue are the right to respect for private and family life (Article 8 of the European Convention on Human Rights) and right of data protection, which is recognised as a distinct right, for example under the Charter of Fundamental Rights of the European Union.[3] However, other rights such as freedom of expression might also be affected.

Issues around the impact of data collection and use and the potential impact on democracy have also attracted significant attention. We note in this regard the report of the Information Commissioner's Office to Parliament of 6 November 2018 on its *Investigation into the use of data analytics in political campaigns*.[4]

Q2. Are consumers and individuals aware of how their data is being used, and do they have sufficient real choice to consent to this?

We are concerned that consumers are not aware of all the ways in which their data is being used. Relevant issues to consider in this context include: the (increasing) complexity of algorithms; extent to which personal data is shared with other organizations; and the extent to which personal data is collected, commoditised and used to for personalised marketing.

While some actors uphold the principles of transparency and offer real choice to consent, we are aware that others are still not meeting the basic requirements of the UK data protection legislation and do not offer consumers real choice.

Furthermore, organisations may be naturally averse to publicising how they use personal information a) because innovative ways to use personal data could improve their sales and b) people would not be happy with how their personal data is used.

In terms of consent we are concerned that real consent in the current landscape would be very difficult to achieve, not least as a result of understanding what sharing data looks like and the long-term consequences of that. Most people want access to the service, eg a webpage, and may therefore click the consent button without giving full consideration to consequences of what data might be collected about them and how this could be used. Privacy notices setting out the ways in which data will be used in long and complicated terms are in fact in breach of the legislation, which requires the privacy notice to be

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

[4] https://ico.org.uk/media/2260277/investigation-into-the-use-of-data-analytics-in-political-campaigns-20181107.pdf

"concise, transparent, intelligible and easily accessible".

Q3. What regulation is necessary and proportionate to protect individual rights without interfering unduly with freedom to use and develop new technology?

As above, we consider that the existing legislation offers a good level of protection in principle but in practical terms, enforcement is the deciding factor as to whether it proves effective. The combination of the enforcement of current laws, coupled with the development of new industry-wide standards and their observance, failing which the imposition of greater regulation by new laws, might more comprehensively address the problem than just the current law itself.

At the same time, we understand that the ICO will investigate breaches or concerns but this does not mean it is actively policing the conduct of companies where no such concerns have been raised. Furthermore, enforcement may increasingly require the regulator to be able to develop their own technology and have teams able to understand technological developments if abuses are to be identified and effectively prosecuted.

More generally, questions arise as to culture and how the importance of ethics and ethical use of technology and personal data are promoted. In addition to enforcement, there may be a need for corporate cultural change that addresses these issues in a proactive way, to assess the impacts the development of a business could have on individual rights. Governments and data collecting corporations could work together to establish industry-wide standards of good practice in the management of personal data in a fast-developing business context. This could support the objectives of the law and regulation, which may not always be able to keep pace with new business developments.

For instance, such standards could demand more corporate self-awareness of the potential impact of business developments and include annual reporting of what risk management and other steps have been taken by a company to avoid harm/abuse in the use of data. Innovation in the use of personal data has produced many benefits, but there is also now greater understanding of the downsides of its industrial scale usage. This might even require corporate structures which allow for challenge/questioning within the company itself.

The idea would be for industry itself to place greater emphasis than it has on the analysis of the potential downsides of existing or new business models. It should proactively be addressing these issues, rather than just reacting to the latest scandal. If companies do not take these issues seriously there would be the risk that they could lose the trust of consumers; face greater regulation by governments; or face penalties under data protection or competition laws. Any of these considerations could seriously affect a company's bottom line, or even existence.

The combination of the enforcement of current laws, coupled with the development of new industry-wide standards and their observance, failing which the imposition of greater regulation by new laws, might more comprehensively address the problem than just the current law itself.

There is a further policy question to be considered in terms of regulating against more "active" harm that might be occasioned by use of personal data. For example, recent stories on young people committing suicide have referred to that fact that they often gain data on how to kill themselves on social media sites.[5] The vulnerable young person may have chosen to access information which is their right. However, many sites actively profile users and are developing algorithms to guide people to topics they might be interested based on their search history: in such cases, such automatic direction would be deeply concerning and could ultimately impact upon human life (although we do not take a view on whether it would infringe the right to life *per se*). Similarly, algorithms could be used to actively identify people who may have suicidal thoughts and even offer help and support.

Q4. If action is needed, how much can be done at national level, and how much needs international cooperation?

We anticipate that international cooperation on enforcement of data protection laws will become increasingly important. The digital environment renders traditional physical borders increasingly irrelevant and businesses can operate in and from multiple jurisdictions. Regulators and law enforcement agencies will therefore need to work collaboratively to provide global solutions to global compliance issues if data protection and privacy rights are to be properly protected.

International cooperation may be needed to respond to challenges posed by businesses at both ends of the spectrum. Where a business operates with limited infrastructure, there may be challenges with identifying the locus of operations and taking action against those infringing rights. Similarly, where eg a company has offices in numerous locations, coordinated action may pave the way for more effective enforcement across all the relevant jurisdictions. This may be particularly pertinent where there are deliberate attempts to exploit the individuals whose data is being misused or abused.

International cooperation would also be an essential component of creating industry-wide standards, as referred to in our response to question 3.

[5] https://www.bbc.co.uk/news/av/uk-46966009/instagram-helped-kill-my-daughter

Q5. To what extent do international human rights standards, such as the UN Guiding Principles on Business and Human Rights, have a role to play in preventing private companies from breaching individuals rights to privacy?

International human rights standards can be helpful in promoting protection of individuals' rights, including privacy rights. Often businesses will wish to take proactive steps to avoid breaching the right to privacy and international standards may therefore be viewed in a positive light by businesses keen to act responsibly. Customer/consumer trust and the need to avoid reputational damage can often act as a "soft" enforcement power (although this should not be relied upon in preference to legal enforcement mechanisms). Global principles such as the UN Guiding Principles on Business and Human Rights can be helpful in setting a standard for compliance which will be understood and respected internationally. If they are well publicised, public commitment to upholding these principles could therefore help create and reinforce consumer trust. In practical terms, the high profile of these principles also leads to generation of significant resources which can help businesses with practical aspects of day-to-day compliance. This is one of the tasks undertaken by the Office of the High Commissioner for Human Rights but other bodies, including sector-specific organisations, can bolster these efforts. For example, in the context of legal services, the International Bar Association publishes practical guides for business lawyers and bar associations along with training tools and articles to assist lawyers in their compliance efforts, which we have supported.[6]

However, as referred to above, where businesses are less inclined to take proactive steps, State enforcement may be required. Here too, the UN Guiding Principles may prove beneficial: as noted in a recent report on *Implementation of the UN Guiding Principles on Business and Human Rights* by the European Parliament's Directorate-General for External Policies "Unanimous endorsement … has made the UNGPs a legitimate document to be taken up in discussion with states around the world, that otherwise would not even enter into discussion about human rights and business."[7] The principles therefore provide a starting point for discussions with States, which in turn mean they are more likely to private companies operating in their jurisdiction to account.

For further information, please contact:

Carolyn Thurston Smith
Policy Team
Law Society of Scotland
DD: 0131 476 8205
carolynthurstonsmith@lawscot.org.uk

[6] See https://www.ibanet.org/LPRU/Business-and-Human-Rights-for-the-Legal-Profession.aspx

[7] See http://www.europarl.europa.eu/RegData/etudes/STUD/2017/578031/EXPO_STU(2017)578031_EN.pdf at p8