Monitoring private communications under the Online Safety Act

Secure communications or online safety? Intercepting private communications to comply with the OSA requires extra care. By **Paul Maynard** and **Shóna O'Donovan** of Covington.

The Online Safety Act 2023 (OSA) is a wide-ranging law aimed primarily at addressing illegal content online. To achieve this goal, the OSA imposes "duties" on providers of in-scope services to, among other things, address illegal content on their services and to take steps to protect children from content that is harmful to them.

These duties apply to providers of various online services, including so-called "user-to-user" (U2U) services. This term is defined to cover services through which users may "encounter" content created by other users, e.g. social media and file-sharing services (s. 3(1)). The OSA notably excludes email, SMS and MMS content from its scope, but does not exempt various types of "over-the-top" (OTT) communications, e.g., chat features in online gaming tools, or app-based messaging services.

It is plausible, therefore, that a provider of an internet-enabled private messaging service might need to consider monitoring the content of communications sent through its service to help it comply with its duties under the OSA. Doing so could, however, be a criminal offence of unlawful interception of communications under Section 3 of the Investigatory Powers Act 2016 (IPA).

The OSA is a developing law, and its intersection with the IPA remains far from clear. That said, however, the IPA arguably permits U2U service providers to intercept communications to comply with their duties under the OSA, at least in situations where the OSA imposes on them a direct legal obligation to carry out such interception. We describe the interaction between the two in more detail in this article.

Use of technologies under the OSA

In principle, it is open to U2U service providers to implement technologies to comply with their safety duties under the OSA, as long as doing so is proportionate to the risks of harm. The OSA also grants Ofcom powers to recommend or require that providers use "proactive" or "accredited" technologies for this purpose, including to identify whether content on their services is illegal – e.g., terrorism or child sexual exploitation and abuse (CSEA) content. In particular:

Powers related to "proactive" technologies: The OSA defines "proactive technology" to encompass technologies that are used proactively (i.e., not in response to user reports), and that analyse content (e.g. to determine if it is illegal) user data and/or metadata (e.g. to determine a user's age or whether a user may be involved in illegal activity) (s. 231).

Ofcom is empowered to recommend, through codes of practice (COP) that it may issue, that providers use a proactive technology to comply with specified duties in the OSA, where Ofcom is satisfied that the use of the technology would be proportionate to the risk of harm (Schedule 4, para. 13(2)).[1] For example, in the Illegal Content Codes of Practice for User-to-User Services,[2] Ofcom recommends that certain service providers that are at a high risk of image-based child sexual abuse material (CSAM) use hash-matching technologies where technically feasible to do so (para. 9.3).

Separately, where Ofcom concludes that a provider has failed to comply with an OSA requirement, it may require that provider to make use of specified proactive technologies (OSA, s. 136(1)).

Notably, the OSA states that providers may use only technologies that analyse user-generated content or related metadata in relation to content that is "communicated publicly," not content that is "communicated privately" (See s. 136(6) and Schedule 4, para. 13(4)). The OSA does not prescribe when content or metadata will be communicated publicly or privately, but does set out factors that are relevant to this assessment (s. 232(1)). These are:

- the number of individuals in the UK who can access the content through the service;
- any restrictions on who may access the content through the service (e.g. a requirement for approval or permission from a user, or the provider, of the service); and
- the ease with which the content may be forwarded to, or shared with, other individuals (s. 232(2)(a)-(c)).

Ofcom's guidance[3] emphasises that this analysis will need to be carried out on a case-by-case basis, but it provides some illustrative examples. In particular, it indicates that where there is "a very large number of users" in a group chat, this is indicative that the content is communicated publicly (Case Study 6). By contrast, content shared from one user to another in a private chat feature of an online dating service is likely to be communicated privately, assuming there is no in-built functionality to forward or share the content.

Accredited Technologies: Ofcom may also "accredit" certain technologies for detecting terrorism or CSEA content where they meet minimum accuracy standards, and may require a U2U service provider to use such an accredited technology to identify such content and prevent users from encountering it on their services (ss. 125(12) and 121(2)(a)).[4] Unlike the use of proactive technologies, Ofcom can require U2U service providers to adopt accredited technologies in relation to content communicated both publicly and privately.

Ofcom may also require a provider to develop or source technologies to identify and remove CSEA content, or to prevent individuals from encountering such content, and any such technology must meet accuracy standards set out

in secondary legislation (OSA, s. 121(2)(b)).

The offence of unlawful interception under the IPA

Section 3 of the IPA states that it is a criminal offence to intentionally intercept a communication:

- in the course of its transmission through a telecommunications service (whether public or private) or a postal service;
- where the interception happens in the UK; and
- where the person carrying out the interception has no "lawful authority" for the interception.

Could compliance with the OSA lead to a criminal offence under the IPA?

It seems plausible that a U2U service provider might determine that gaining access to the content of communications is necessary for it to comply with its safety duties under the OSA, e.g., through the use of proactive technologies on messaging apps. Such a provider might also be required to implement a proactive or accredited technology for this purpose. OTT messaging services generally fall within the scope of "telecommunications services" under the IPA, and interception for the purposes of compliance with the OSA might well take place in the UK.

That said, there are some limitations on the scope of the offence of unlawful interception in the IPA. Among them:

- A communication is only "intercepted" where the content is made visible to a person other than the sender or recipient (IPA, s. 4(1)(b)). Obtaining metadata only, for example, would not give rise to an offence under Section 3 IPA, although it could lead to a separate offence of unlawfully obtaining communications metadata.
- Interception also only takes place in the course of the transmission of a communication, i.e., when it is in transit or stored within a telecommunications system—not when communications are stored on devices. Certain technologies might monitor communications stored in, for example, cloud backups rather than messages in transit.
- There is no offence where the telecommunications system is "private"—i.e., not available to the general public—and the operator of the system gives their consent to the interception (s. 3(2)).

If these limitations do not take a provider's activities out of scope of the offence of unlawful interception, they may carry out interception only where they have "lawful authority" to do so. The IPA states that a person will have lawful authority for interception "only where" they meet one or more of the criteria set out in Section 6(1). The existence of a requirement under the OSA to take certain steps alone does not, therefore, appear to create "lawful authority" (although it is unclear how this limitation interacts with the principle of implied repeal in English law when newer statutes automatically revoke conflicting provisions in earlier laws without an explicit statement).

Most types of lawful authority set out in the IPA are available only to law enforcement and intelligence agencies. However, the IPA does permit telecommunications service providers to intercept communications for specified purposes, including for "purposes relating to the enforcement, in relation to the service, of any enactment relating to:

(i) the use of . . . telecommunications services,
(ii) the content of communications transmitted by means of such services" (s. 45(2)).

The IPA's explanatory notes indicate that this might be relevant where a customer has requested that a telecommunications operator filter out harmful, illegal or adult content (para. 132). An "enactment" covers any binding requirement on a provider, which would appear to include the OSA.

As a result, this provision might give providers lawful authority under the IPA to comply with binding requirements to implement proactive or accredited technologies under the OSA. It is less clear that it would authorise interception that is not explicitly legally mandated, e.g., Ofcom recommendations to use proactive technologies.

Section 46 of the IPA also authorises all businesses to intercept communications for "monitoring" and "record-keeping" purposes, where permitted by secondary legislation. The Investigatory Powers (Interception by Businesses etc. for monitoring and Record Keeping Purposes) Regulations 2018 (IP Regs) permit interception of communications that take place in the course of business activities, where certain conditions are met (e.g., express notification to users, and use of intercepted communications for "keep[ing] a record" of certain activities) (IP Regs, paras. 2-4). The IP Regs may therefore give U2U service providers lawful authority to intercept communications in order to demonstrate compliance with their OSA duties, but it remains unclear whether the Regulations permit interception in order to take action to comply with the EU Digital Services Act rather than simply, for example, to keep records of illegal content.

Conclusion

In summary, U2U service providers will need to think carefully about intercepting private communications on their services in order to comply with their duties under the OSA to minimise risk of committing a criminal offence of unlawful interception under the IPA, as the OSA's duties are not, in isolation, sufficient to permit providers to carry out such interception. The risks are likely to be lower, however, where providers are under an explicit, binding obligation from Ofcom to intercept communications.

Further guidance from Ofcom may be forthcoming, but otherwise, we expect that many areas of uncertainty will need to be addressed by the courts.

AUTHORS

Paul Maynard is Special Counsel and Shóna O'Donovan an Associate in the technology regulatory group in Covington's London office.
Emails: sodonovan@cov.com
pmaynard@cov.com

REFERENCES

1 Although recommendations in a COP are not legally binding, the OSA provides that U2U service providers are "to be treated as complying with a relevant duty if the provider takes or uses the measures described in a code of practice which are recommended for the purpose of compliance with the duty in question." Section 49(1).

2 Ofcom, Illegal Content Codes of Practice for User-to-User Services. 24 February 2025. Available at: www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/illegal-harms/illegal-content-codes-of-practice-for-user-to-user-services-24-feb.pdf?v=391889.

3 Ofcom, Protecting people from illegal harms online: Guidance on content communicated 'publicly' and 'privately' under the Online Safety Act. 16 December 2024. Available at: www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/illegal-harms/guidance-on-content-communicated-publicly-and-privately-under-the-online-safety-act.pdf?v=388093

4 Ofcom closed its consultation on what the minimum standards of accuracy for accredited technologies could be on 10 March 2025.

ESTABLISHED 1987

UNITED KINGDOM REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Cross-border data transfers in turbulent times: The global impact of shifting policies

Nicola Fulford and **Katie McMullan** of Hogan Lovells offer their personal views on what the UK's new risk-based approach means for its competitiveness and EU data adequacy.

Cross-border data transfers have long been the lifeblood of global business, enabling innovation, efficiency, and international collaboration. But as geopolitical tensions rise and regulatory approaches diverge, the legal frameworks underpinning these

Continued on p.3

ICO issued just 18 fines in 2024, and mostly under PECR

Does John Edwards' approach to ICO enforcement safeguard the UK economy, or reduce the possibility of dissuasive penalties for data harms? By **Ralph O'Brien** of REINBO Consulting.

Under the leadership of Information Commissioner John Edwards, it is fair to say the UK's Information Commissioner's Office (ICO) has implemented a strategic shift in its enforcement approach, emphasising engagement and systemic change over the imposition of substantial fines. This philosophy is grounded in the belief that collaborative efforts and remedial actions are more effective in

Continued on p.5

Issue 139 **MAY 2025**

See the publisher's blog at www.privacylaws.com/news/

UNITED KINGDOM
report

ISSUE NO 139 MAY 2025

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

REPORT SUBSCRIPTIONS
K'an Thomas
kan@privacylaws.com

CONTRIBUTORS
Nicola Fulford and Katie McMullan
Hogan Lovells

Ralph O'Brien
REINBO Consulting

Paul Maynard and Shóna O'Donovan
Covington

Jonathan Howie and Katie Hewson
Stephenson Harwood

Jonathan Rush
Travers Smith

Rowenna Fielding
Miss IG Geek Ltd

PUBLISHED BY
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Email: info@privacylaws.com
Website: www.privacylaws.com
Subscriptions: The *Privacy Laws & Business* United Kingdom Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.
Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686
ISSN 2047-1479

"comment

The UK is now firmly on its own path

The Data Protection (Use and Access) Bill (DUAB) will soon be adopted (p.8). Changes are coming to the legislative framework but UK companies are less likely to be fined than their EU counterparts (p.1.). However, the DUAB will give the ICO more fining powers, in effect a much bigger stick, under the Privacy and Electronic Communications Regulations (PECR) which will be matched with those of the GDPR. The ICO has been very active on children's privacy, and it has made many large platforms change their practices by persuasion. Now a new era has started under the Online Safety Act for regulating harmful content for children (p.16).

Professor David Erdos of the University of Cambridge notes on LinkedIn that just three (UK) GDPR fines have been issued on average in each of the last five years. Erdos writes that substantive scrutiny by the Tribunal and the Courts has been lacking, and there has also been an absence of holistic oversight by Parliamentary committees[1]. However, lately, the ICO has confirmed a £3 million fine on Advanced Software Group (p.12). *O'Carroll v Meta* (2025) represents a different way of achieving a result – the ICO assisted an individual in a case settled by Meta and confirmed that targeted advertising is direct marketing (p.12).

So the UK's differences from the EU are evident – it remains to be seen whether the EU Commission will revise the GDPR due to its general simplification agenda. We expect to hear more about this policy development very soon, but it is likely that reliefs will be mainly targeted at SMEs. A crucial part of the new global order affected by events in the US is international data transfers – read an analysis on p.1.

The DUAB will introduce changes to the ICO's structure. The ICO's job advert for the Interim CEO said that the role will be filled by a person who is a "people-orientated and visible leader, who can maintain high levels of motivation and cooperation, setting and embedding a culture of curiosity, collaboration, impact and inclusion to deliver regulatory interventions that improve people's lives, reduce burdens, promote economic growth and innovation and enable efficient public services."Anyone?

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

1 See www.slideshare.net/slideshow/public-enforcement-of-uk-data-protection-promise-reality-and-future-f89a/277667696

Contribute to PL&B reports

Do you wish to contribute to *PL&B UK Report*? Please contact Laura Linkomies, Editor (tel: +44 (0)20 8868 9200 or email: laura.linkomies@privacylaws.com) to discuss your idea, or offer to be interviewed about your organisation's data protection/Freedom of Information work.

Join the Privacy Laws & Business community

The *PL&B United Kingdom Report*, published six times a year, covers the Data Protection Act 2018, the Freedom of Information Act 2000, Environmental Information Regulations 2004, Privacy and Electronic Communications Regulations 2003 and related legislation.

PL&B's United Kingdom Report will help you to:

Stay informed of data protection legislative developments.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Learn about future government/ICO plans.

Understand laws, regulations, court and tribunal decisions and what they will mean to you.

Be alert to privacy and data protection law issues and tech developments that will affect your compliance and your reputation.

Included in your subscription:

1. Six issues published annually

2. Online search by keyword
Search for the most relevant content from all *PL&B* publications.

3. Electronic Versions
We will email you the PDF edition which you can also access in online format via the *PL&B* website.

4. Paper version also available
Postal charges apply outside the UK.

5. News Updates
Additional email updates keep you regularly informed of the latest developments.

6. Back Issues
Access all *PL&B UK Report* back issues.

7. Events Documentation
Access *PL&B* events documentation, except for the Annual International Conferences in July, Cambridge.

8. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of legislation, and sources for specific texts. This service does not offer legal advice or provide consultancy.

9. Free place at a *PL&B* event
A free place at a *PL&B* organised event when booked at least 10 days in advance. Excludes the Annual Conference. More than one free place with Multiple and Enterprise subscriptions.

privacylaws.com/reports

"Given the rate of change in law, regulation and business practice, it is essential to have concise and up-to-date information. *PL&B* is always relevant and continues to offer great value."

Adam Green, Chief Risk Officer, Equiniti

International Report

Privacy Laws & Business also publishes *PL&B International Report*, the world's longest running international privacy laws publication, now in its 39th year. Comprehensive global news, currently on 180+ countries, legal analysis, management guidance and corporate case studies on privacy and data protection, written by expert contributors

Read in more than 50 countries by regulators, managers, lawyers, and academics.

Subscriptions

Subscription licences are available:

- Single use
- Multiple use
- Enterprise basis
- Introductory two and three years discounted options

Full subscription information is at privacylaws.com/subscribe

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.