No end to the end-to-end encryption discussion

Law enforcement agencies have raised concerns over use of end-to-end encryption (E2EE) for years, but now discussion is geared towards protecting children as a new avenue to fight the spread of E2EE. By **Alexander Dittel** of Wedlake Bell LLP.

Privacy enthusiasts take issue with restricted or absent end-to-end encryption (E2EE) in online communications services. E2EE-enabled communications are the most secure. Because of public demand but also for commercial reasons, Whatsapp, Zoom, Messenger, Teams and others have started offering E2EE in some form. However, do users have a right to E2EE?

E2EE is often seen as the epitome of privacy. In a digital world of surveillance by businesses, hackers and state actors, people want to enjoy privacy of their correspondence and communications. E2EE can deliver on this far better than any telecommunications or postal service in the past ever could.

Nevertheless, E2EE is a security feature and there is no express legal obligation to implement it. Conventional encryption, such as SSL and TLS, will likely satisfy any user's desire for security of communications. The enhanced security of E2EE also means that add-on services which require server access may be restricted, e.g. automated responses, connecting further participants, etc. Nevertheless, the proliferation of the surveillance for hire industry and revelations about unlawful state surveillance make E2EE increasingly in demand and, perhaps, even an appropriate base level of security.

However, this trend is now distorted by emerging legislation, such as the UK's Online Harms Bill and the US Eliminating Abusive and Rampant Neglect of Interactive Technologies Act (EARN IT) Act, which encourage platforms to monitor content which could be harmful to children. While counter-terrorism was not good enough a reason to justify this type of measure in recent history, the emerging objective of preventing child sexual exploitation may pave the way for backdoors in encrypted systems. E2EE will likely not be implemented where it would prevent the platform from complying with its monitoring duties, or taking appropriate action needed to avoid civil or even criminal liability.

Not a problem but a solution?

E2EE is often presented as a solution and not a problem. The Information Commissioner's Office (ICO) called it a key enabler for compliance and giving citizens confidence about how their personal data is processed by digital services.[1]

Data is encrypted on the sender's device and travels securely until it is decrypted by the recipient at the other end. The sender uses a public key obtained from the recipient to encrypt the message. The public key is digitally signed by a third-party authority to confirm the veracity of the public key accompanied by the recipient's name. The communication is then delivered and the recipient uses his or her private key to decrypt the message. Apart from the hypothetical possibility that in the distant future quantum computers might break any encryption, no one, not even the service provider, can tamper with E2EE-secured communications.

While companies seem to enjoy putting themselves in a position where they are technically unable to assist law enforcement in accessing communications data, law enforcement are trying to do all they can to detect and prevent crime. According to Rob Jones, a director general at the UK National Crime Agency (NCA), referrals from social media companies led to 500 arrests and has safeguarded 650 children every month in the UK.[2] E2EE has upset law enforcement and raised questions about how candid companies are about reasons to implement it and reasons to withhold assistance to law enforcement. After all, E2EE could be used by criminals who wish to hide their illicit activities.

But what if the service provider has weak security which is exploited by the surveillance for hire industry to gather sensitive details about individuals. What if a company is building profiles based on the content of people's communications and sells them on for advertising? What if law enforcement is engaging in unlawful surveillance which could harm our fundamental rights?

Indeed, the European Data Protection Supervisor's review of Europol's practices suggests the organisation holds large volumes of unstructured communications data which might well include your private communications.[3] Similarly, the European Data Protection Board's report on the implementation of the law enforcement directive highlights failings of data protection supervisory authorities to assert their role against domestic law enforcement authorities.[4] These reports certainly do not inspire confidence.

An appropriate base level of security?

E2EE is very secure. However, communications metadata, such as time, date and recipient details, can still be obtained with a warrant. E2EE is only as secure as the sender's device which could be accessed by criminals or law enforcement under a warrant to recover the private key and access E2EE-secured communications. Another weak point is the security of the recipient's device.

Encryption-in-transit is an alternative to E2EE that enables access to communications by the service provider. Messages are encrypted by the sender's device, delivered to the server where they are decrypted, encrypted again and delivered to the recipient and decrypted again. This solves the important issue of security in transit as well as allowing for additional services which would be restricted under E2EE. It will also allow for the lawful access by law enforcement.

Secrecy of communications is ensured by law, often under the threat of criminal sanctions. Users can also consider the confidentiality undertakings in the provider's terms of service.

It seems that E2EE will satisfy those most sceptical among us but would probably not be demanded by your regular user of a trusted service. Typically, only rare situations would merit the use of E2EE; for example, if commercial parties require enhanced confidentiality of communications. Some people may favour it for personal reasons such as anxieties or mental health. A demand for E2EE might also be driven by a lack of confidence in the legal system and the government or a desire to secure communications that travel to high-risk countries.

Backdoors means no E2EE

No law imposes E2EE and no law bans it. There are many arguments for implementing it and many against. The fact is, if implemented, law enforcement will not be able to recover information which could be crucial for an investigation.

In the UK, access to communications for detecting or preventing crime is subject to the Investigatory Powers Act 2016. Following initial legal challenges and amendments, today's version of the Act includes the double-lock mechanism which means that warrants for the interception of primary and related communications data must be approved by the Secretary of State as well as a Judicial Commissioner. Warrants will only be approved to prevent or detect serious crime subject to a proportionality assessment. Such access should be very rare, targeted and short-lived.

However, if E2EE is in place, there is nothing to access because the data is encrypted beyond recognition. In the aftermath of 9/11 and 7/7, the Data Retention and Investigatory Powers Act 2014 or DRIPA permitted the Government to require telecommunications providers to retain all of our communications data including browsing data for up to a year. The Act was quickly challenged by human rights groups and MPs David Davis and Tom Watson, and ultimately it was declared incompatible with human rights by the High Court and later repealed by Parliament.

In the US, a legislative proposal called CALEA II was expected to force online messaging services providers to insert backdoors into their platforms. The existing Communications Assistance for Law Enforcement Act already requires telecommunications carriers to modify their equipment, facilities, and services, wherever reasonably achievable, to ensure that they are able to comply with authorised electronic surveillance actions. CALEA II was expected to expand backdoors into communications software. The recent Burr Encryption Bill had similar aims. Both legislative proposals have failed.

The ICO points out that accessing encrypted content is not the only way to catch abusers. Other methods include infiltrating abuse rings, listening to reports from children targeted by abusers and using evidence from convicted abusers.

Preventing child sexual exploitation

New legislation is emerging intended to safeguard children online which may affect the ability of organisations to implement E2EE.

The UK's Online Harms bill will impose a statutory duty of care on certain service providers to moderate user-generated content so that users are not exposed to illegal and harmful online content. E2EE will likely have to be weakened to allow companies to comply.

In the US, the EARN IT Act removes platform immunity from child sexual abuse material under Section 230 of the Communications Decency Act. It is said to create a strong incentive for the tech industry to abolish E2EE in a drive to monitor for harmful content.

Conclusion

Why should a majority of people be deprived of a security measure that gives them much needed confidence in the digital world just to be able to pursue a fraction of criminals?

The Government has recently launched a campaign to warn that social media companies are willingly blindfolding themselves to child sexual abuse if they implement E2EE. Without E2EE, law enforcement could be more efficient and effective in pursuing some very troubling offences. Conversely, the ICO suggests that E2EE is a tool that will help safeguard children and that systems without E2EE can be abused.

Curiously, the Government claims it does not wish to ban E2EE and promises a middle way of potential future technical solutions for detecting harmful content without weakening E2EE. However, such a promise is hypothetical and, in the meantime, impending legislation will mean that E2EE will be weakened.

You do not need to ban E2EE to severely restrict E2EE. Once we take that path, who knows where it may lead us?

NO PLACE TO HIDE CAMPAIGN

The government-funded campaign asks social media companies to confirm they will not implement end-to-end encryption until they have the technology in place to ensure children will not be put at greater risk as a result.

Jim Killock, from the Open Rights Group, said: "The way the Government has been using scare tactics damages trust with its citizens. The Government exploiting emotive narratives for their campaign is manipulative and does not provide a balanced view. The truth is that encryption is vital for online safety."

Meta, which has E2EE on WhatsApp, has announced plans to introduce the technology across the rest of its app messaging platforms by 2023.

• *See noplacetohide.org.uk/*

AUTHOR

Alexander Dittel is a Partner in Technology at Wedlake Bell LLP.
Email: adittel@wedlakebell.com

REFERENCES

1 ico.org.uk/media/about-the-ico/documents/4018823/ico-e2ee-paper-02112021.pdf
2 www.theguardian.com/uk-news/2022/jan/22/nca-says-end-to-end-encryption-challenge-law-enforcers
3 edps.europa.eu/press-publications/press-news/press-releases/2022/edps-orders-europol-erase-data-concerning_en
4 edpb.europa.eu/system/files/2021-12/edpb_contribution_led_review_en.pdf

ESTABLISHED 1987

UNITED KINGDOM REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

The future for low-value data breach claims

Not every data breach is worth High Court time – a relief for the companies involved. By **Katie Hewson**, **Olivia Fraser** and **Kate Ackland** of Stephenson Harwood LLP.

As the number of low-value claims arising out of personal data breaches (Data Breach Claims) continues to grow, a recent flurry of High Court judgments suggests that judicial patience with certain such claims is wearing thin. This should be welcome news for controllers and processors, as the Courts are demonstrating a pragmatic approach to Data Breach Claims and demonstrating how the

Continued on p.3

UK: Data protection shake-up looks certain

No clarity over details yet but change is coming in one form or another – and fast. By **Laura Linkomies**.

On announcing the Brexit Freedom's Bill (no text available yet), the government stated on data and AI that the bill aims to facilitate the UK "moving in a faster, more agile way to regulate new digital markets and AI and creating a more proportionate and less burdensome data rights regime compared to the EU's GDPR."

The government is now in the middle of analysing the thousands of responses it received to the consultation *Data: A New Direction*, but we

Continued on p.5

Issue 120 **MARCH 2022**

UNITED KINGDOM
report

ISSUE NO 120 **MARCH 2022**

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
Katie Hewson, Olivia Fraser and Kate Ackland
Stephenson Harwood LLP

Gary Brooks
Data Protected Limited

Alexander Dittel
Wedlake Bell LLP

Laura Brodahl and Jan Dhont
Wilson Sonsini Goodrich & Rosati

Simon Airey, James Dobias, Joshua Domb and William Merry
McDermott Will & Emery UK LLP

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

Information is key and data protection a human right

Law enforcement agencies, in the US especially, have for years criticised end-to-end encryption. Yet it is a surprising move that the UK government is advocating radical changes. End-to-end encryption (E2EE) is already used in WhatsApp, iMessage and Signal apps. Now Meta plans to add it to Facebook Messenger and Instagram direct messages in 2023. The UK's *No Place to Hide* campaign, backed by the Home Office, states that online privacy and cyber-security must be protected, but how they can be balanced with safety measures? The immediate focus here is the detection of child sexual exploitation and abuse but it is certain that reasons extend to other criminal activities. Read our correspondent's views on p.10

Warfare today, whether in Ukraine or elsewhere, is also a cyber war – fake news, destroying communications capabilities etc. Websites of several Ukrainian banks and government departments became inaccessible immediately after Russia's attack.

The European Union was already planning to help Ukraine fight off cyberattacks from Russia before the conflict started. In the UK, the National Cyber Security Centre has called on organisations in the UK to bolster their own online defences.

Cyber-security incidents within the UK are on the rise and get reported (sometimes) to the ICO, which issues regular statistics (p.6). Data protection and cyber-security are of course interlinked. The new National Cyber Strategy aims to ensure that the UK remains confident, capable and resilient in the fast-moving digital world (p.18).

In this edition, we report on the marketing aspects of the government's proposal for a revised data protection regime (p.7) and what the future holds for this consultation (p.1).

Data Protection Officers can find comfort in the recent indications that low value privacy claims will be dismissed in the High Court (p.12). It does seem a waste of expensive court time which could be used for more serious and high-value cases.

I hope you find this issue informative and useful for your role. Any feedback is always very welcome.

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

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 and Privacy and Electronic Communications Regulations 2003.

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 and events. You can then click straight through from the search results into the PDF documents.

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 in Data Protection, Freedom of Information and related laws.

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

7. Events Documentation
Access UK events documentation such as *PL&B 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.

privacylaws.com/reports

"Fantastic documents which provide a useful snapshot of the data protection landscape all in one place that can be easily digested around your busy working day. The split between International and UK allows you to focus on areas of interest as you require."

Angela Parkin, Group Head of Data Protection, Equiniti

International Report

Privacy Laws & Business also publishes *PL&B International Report*, the world's longest running international privacy laws publication, now in its 36th year. Comprehensive global news, currently on 165+ 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.