AN A.S. PRATT PUBLICATION
JANUARY 2024
VOL. 10 NO. 1

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 10 NUMBER 1 January 2024

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Alexandra Jefferies at ..... (937) 560-3067
Email: ..... alexandra.jefferies@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
LexisNexis® Support Center ..... https://supportcenter.lexisnexis.com/app/home/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (518) 487-3385

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [1] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [82] (LexisNexis A.S. Pratt)

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2024–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

UK Data Recording Obligations – Have You Gotten the Message?

By Hayley Ichilcik, Saqib Alam, Annabel Gillham and Jennifer Galloway*

In this article, the authors explain that UK regulators may now be looking to apply additional scrutiny on the use, recording and retention of electronic communications, particularly via encrypted messaging applications.

In recent months, the use of encrypted messaging applications for business purposes has returned to the spotlight. In July 2023, legal challenges surrounding the disclosure of messages on devices used by former Prime Minister Boris Johnson made headlines in the context of the Covid-19 Inquiry. And in August 2023, the UK's energy regulator, the Office of Gas and Electricity Markets (Ofgem), issued a fine in respect of communications relating to wholesale energy trading made via an instant messaging platform on privately owned phones that were not appropriately recorded or retained – the first fine of its kind in the UK. In light of the augmented media attention, it may be that Ofgem and other UK regulators now look to apply additional scrutiny on the use, recording and retention of electronic communications, particularly via encrypted messaging applications.

BACKGROUND

This is not a new area of interest for UK regulators. For example, the Financial Conduct Authority (FCA) took action against an investment banker in 2017 for sharing client confidential information via an instant messaging platform. There has, however, been a spike in regulatory activity in this regard following the Covid-19 pandemic, and the resulting shift towards remote/hybrid working. In particular:

- In January 2021, the FCA issued "Market Watch 66," which warned regulated firms that they must continue to comply with the recording requirements in the FCA's Senior Management Arrangements, Systems

* Hayley Ichilcik, a partner in the London office of Morrison Foerster, specializes in representing financial institutions, corporate clients and senior individuals in highly sensitive litigation, regulatory enforcement matters and internal investigations. Saqib Alam is a tri-qualified English solicitor, New York attorney and Singapore advocate who advises global companies, boards and high net worth individuals facing business-critical issues and helps them resolve such matters from a legal and reputational standpoint. Annabel Gillham, co-managing partner of the firm's London office and a member of the firm's global data privacy team, specializes in employee data protection and data crisis management. Jennifer Galloway, an associate at the firm, advises clients on a wide range of complex dispute resolution matters, including general commercial and corporate litigation, investigations and contentious regulatory matters, and financial services disputes. The authors may be contacted at hichilcik@mofo.com, saqibalam@mofo.com, agillham@mofo.com and jgalloway@mofo.com, respectively.

and Controls sourcebook (SYSC) – specifically, SYSC 10A. The FCA also announced last year that it was holding discussions with a number of UK authorised firms regarding their private device practices.

- In July 2022, the Information Commissioner issued a report to Parliament entitled "Behind the screens – maintaining government transparency and data security in the age of messaging apps" which found there to have been extensive use of private correspondence channels by Ministers, and staff employed by the Department of Health and Social Care. The report recommended that a further review be established (in addition to that being undertaken by the Covid-19 Inquiry in respect of issues specific to the pandemic) to look at how different, non-corporate communication channels are being used across the government. Updated guidance on the use of "non-corporate communication channels" was subsequently issued by the Cabinet Office on 30 March 2023.

- More recently, in April 2023, the Prudential Regulation Authority (PRA) imposed a substantial fine relating to one firm's failure to (amongst other things) implement adequate policies and procedures surrounding the retention of business-related correspondence and records, in particular those messages exchanged between senior executives, directors and external parties via an instant messaging platform.

This increase in regulatory activity is not limited to the UK. In September 2022, U.S. regulators imposed fines on 16 financial firms following an industry probe that uncovered routine use of applications on staff personal devices such as text messages and other messaging platforms, to discuss business matters with colleagues, clients and other third parties. When questioned on the U.S. clampdown during a press conference on 4 October 2023, the FCA is reported to have noted that "where we know that action is taken by other regulatory authorities overseas we remain in contact with them because it is important that where our firms operate cross-border we have those good supervisory relationships with our fellow international regulators."

WHAT ARE THE RECORDING OBLIGATIONS FOR REGULATED FIRMS IN THE UK?

Although the use of encrypted messaging applications is not strictly prohibited (in fact there are legitimate business reasons that may require the use of encrypted call or messaging platforms), regulated firms often have obligations with regards to data records and retention. For example:

- *Regulation 8(3), the Electricity and Gas (Market Integrity and Transparency) (Enforcement etc.) Regulations 2013 (the REMIT Regulations)*: Regulated persons must take reasonable steps to ensure that any communication relating to wholesale energy products is recorded and that a copy is

retained (i.e., stored in a medium that is accessible by Ofgem). Regulation 8(6) also requires regulated persons to take reasonable steps to prevent the making, sending, or receiving of any relevant communication (including on privately owned equipment) that it cannot ensure is recorded or retained in accordance with the REMIT Regulations.

- *SYSC 10A*: Regulated firms must take all reasonable steps to retain a copy of electronic communications that relate to in-scope activities, and that are made with, sent from, or received on, equipment either provided or permitted for business use by the firm. A firm must also take reasonable steps to prevent its employees or contractors from communicating on privately owned equipment that the firm is unable to record or copy. Records of communications must be kept for a period of five years (or seven years, where requested by the FCA).

- *Record Keeping Rule 2.1 of the PRA Rulebook*: Capital Requirement Regulation (CRR) firms and CRR consolidation entities must, in respect of in-scope activities, arrange for orderly records to be kept of its business and internal organisation, including all services, activities and transactions undertaken by it, such that the PRA can fulfil its supervisory tasks and ascertain that the firm has complied with all obligations under the regulatory regime. A firm must retain all records kept by it under this Rule in relation to its Markets in Financial Instruments Directive (MiFID) business for a period of at least five years.

- *Regulation 40 of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (Money Laundering Regulations)*: A relevant person must keep records of any documents and information obtained to satisfy the customer due diligence requirements in the Money Laundering Regulations, as well as sufficient supporting records in respect of a transaction that is the subject of customer due diligence measures or ongoing monitoring to enable the transaction to be reconstructed.

WHAT DOES COMPLIANCE LOOK LIKE IN PRACTICE?

The starting point for compliance with relevant regulatory requirements is for firms to have in place clear policies and controls for the use, recordkeeping and retention of telephone conversations and electronic communications by employees or contractors. The key questions are, however, (i) what can firms do to ensure that their policies are effective, and (ii) what additional steps can firms take to ensure compliance with those policies?

Firms should consider the following:

1. *Regular Review of Policies*: Existing policies should be reviewed regularly and updated to address new risks, including developments in software and technology. These policies should make clear the consequences of any breach. Any gaps in data retention or recordkeeping should be addressed without delay.

2. *Training*: Appropriate training should be provided to employees/contractors both at induction and at regular intervals to ensure that the relevant policies are known and understood. Refresher training should be required when policies are amended or updated. Completion of any training could include a declaration by employees/contractors that the relevant policies have been followed.

3. *Monitoring*: There is always a risk of inadvertent or deliberate breach. It is therefore important for firms to have procedures in place to monitor business communications such that irregularities and any potential malpractice are detected at an early stage. Data protection obligations, telecommunications laws and employee privacy rights should be taken into account in advance of any such monitoring, and organisations should consider completing a data protection impact assessment in advance of implementation.

4. *Internal Investigations and Disciplinary Action*: To the extent that potential breaches are identified, appropriate internal investigations should be conducted, with findings sufficiently escalated so that lessons can be learned and policies updated as necessary. Should the investigation result in any findings of wrongdoing or breach of policy, appropriate disciplinary action should be considered.

The management of records by UK government departments and public authorities should be guided by practice recommendations on data recording and retention, including relevant Codes of Practice presented to Parliament pursuant to the Freedom of Information Act 2000.