AN A.S. PRATT PUBLICATION
NOVEMBER – DECEMBER 2017
VOL. 3 • NO. 9

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 3 NUMBER 9 NOVEMBER/DECEMBER 2017

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@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
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (937) 247-0293

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 [303] (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

(2017–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, 718.224.2258. 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 Government Proposes Cybersecurity Law with Serious Fines

By Mark Young*

The UK government recently published a consultation on plans to implement the EU Directive on security of network and information systems. This article summarizes the UK government's plans, including which organizations may be in scope, and the proposed security and incident reporting obligations.

The UK government recently published a consultation[1] on plans to implement the EU Directive on security of network and information systems (the "NIS Directive," otherwise known as the "Cybersecurity Directive"). The consultation includes a proposal to fine firms that fail to implement "appropriate and proportionate security measures" up to EUR 20 million or four percent of global turnover (whichever is greater).

This article summarizes the UK government's plans below, including which organizations may be in scope — for example, in the energy, transport, and other sectors, as well as online marketplaces, online search engines, and cloud computing service providers — and the proposed security and incident reporting obligations.

Organizations that are interested in responding to the consultation had until September 30, 2017 to do so. The UK government will issue a formal response within 10 weeks of this closing date, and publish further security guidance later this year and next. A further consultation on incident reporting for digital service providers will be run later this year; the government invites organizations that are interested in taking part to provide appropriate contact details.

BACKGROUND AND CORE SECURITY AND INCIDENT REPORTING REQUIREMENTS

The European Parliament adopted the NIS Directive on July 6, 2016 following a previous informal political agreement. EU Member States have until May 9, 2018 to implement the NIS Directive into national law.

Among other things, the NIS Directive imposes security and incident reporting obligations on:

---

* Mark Young is a partner at Covington & Burling LLP advising clients on data protection, cybersecurity, and intellectual property matters. He may be reached at myoung@cov.com.

[1] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/636207/NIS_Directive_-_Public_Consultation__1_.pdf.

- operators of essential services ("OESs") in the following sectors:
  - energy (electricity, oil, gas);
  - transport (air, rail, road, maritime);
  - banking;
  - financial market infrastructure;
  - health;
  - water supply; and
  - digital infrastructure (IXPs, DNS service providers, and top level domain ("TLD") name registries); and
- some digital service providers ("DSPs"), *e.g.*, online marketplaces, online search engines, and cloud computing services.

The security and incident reporting requirements for OESs and DSPs are similar, but DSPs are subject to lighter supervision by competent authorities.

WHICH ORGANIZATIONS WITHIN THESE SECTORS WILL BE IN SCOPE?

OESs

Member States have until November 9, 2018 to identify specific OESs in each sector and subsector in their jurisdiction that satisfy the following criteria under the Directive:

- provide a service that is essential for the maintenance of critical societal and/or economic activities;
- the provision of that service depends on network and information systems; and
- an incident affecting those systems would have significant disruptive effects on the provision of that service.

The UK government proposes to determine operators that should be subject to the UK law by considering the various sectors, subsectors, and essential services, and applying identification thresholds. Here are some examples:

Sector	Subsector	Essential Service	Identification Thresholds[2]
Energy	Oil	Oil transmission (upstream)	Operators with throughput of more than 20 million barrels of oil equivalent ("boe") of oil per year.
		Oil transmission (downstream)	Operators which provide or handle 500,000 tons of fuel/per year.
	Gas	The function of supply (the sale or resale of gas) to consumers	Gas suppliers (incl. aggregators where they act as suppliers) that meet the following two criteria (both must apply): - use of smart metering infrastructure; - supply > 250,000 consumers.
		Gas (transmission)	Network operators with the potential to disrupt supply to > 250,000 consumers.
		Gas (distribution)	Network operators with the potential to disrupt supply to > 250,000 consumers.
Transport	Air transport	Owner or operator of an airport	Owner or operator of any aerodrome (i.e., airport) with annual terminal passenger numbers greater than 10 million.
		Air carriers	Air carriers with more than 30 percent of the annual terminal passengers at any individual UK airport that is in scope of the Directive and more than 10 million total annual terminal passengers across all UK airports.
Digital Infrastructure	n/a	Top Level Domain Name Registries	Operators who service an average of 2 billion queries or more in 24 hours.

[2] The consultation document states that unless indicated otherwise, these thresholds are national thresholds.

The government will designate as an OES each operator that it deems to meet the criteria, and the relevant competent authority will issue notifications.

In line with the Directive, the identification process for OESs is not being carried out for the banking and financial market infrastructure sectors that are within the scope of the Directive. This is because sector-specific provisions that are at least equivalent to those specified in the Directive already exist.

DSPs

The scope of the NIS Directive has been controversial since the Commission published its original proposal back in February 2013. One of the main challenges during the legislative process involved agreeing which online or digital service providers, if any at all, should be regulated. Ultimately, it was decided that only online marketplaces, online search engines, and cloud computing services should fall within scope of the new rules.

Member States are not required under the NIS Directive to conduct the same identification exercise for DSPs as they are for OESs, as described above. Instead, DSPs will be under the jurisdiction of the Member State in which they have their "main establishment", *i.e.*, head office in the Union.

The UK government proposes further definitions for "online marketplaces," "online search engines," and "cloud computing services" (including IaaS, PaaS, and Business SaaS), and requested feedback on these definitions.

WHAT SECURITY MEASURES MUST BE IMPLEMENTED?

OESs

The NIS Directive requires Member States to ensure that OESs:

- take appropriate and proportionate technical and organizational measures to manage the risks posed to the security of network and information systems that they use in their operations; and
- take appropriate measures to prevent and minimize the impact of the incidents affecting the security of the network and information systems used in the provision of their service, with a view to ensuring the continuity of the service.

The UK government proposes to implement these provisions through a "guidance and principles based approach." This will involve the government setting out high level security principles (set out in Annex 3 of the consultation), which will be complemented by more detailed guidance that may be generic or sector specific.

OESs will be required to demonstrate to the relevant competent authority that they are applying appropriate measures to manage the risks to their network and information

systems. The consultation also states that "the operator will also be responsible for identifying the relevant network and information systems that will need to comply with the security requirements, agreeing these with the relevant competent authority who will have the final say."

The UK government intends to publish over the course of 2017 and 2018 further information on minimum security expectations, what "good" looks like for each sector, and a framework to determine the extent to which requirements are being met.

DSPs

The security requirements under the Directive are similar for DSPs. The government aims to ensure that the UK's guidance on security for DSPs mirrors that of the European Network and Information Security Agency (ENISA).

WHAT INCIDENTS MUST BE REPORTED?

OESs

The NIS Directive requires designated OESs to "notify, without undue delay, the competent authority or the [Computer security incident response teams ("CSIRT")] of incidents having a significant impact on the continuity of the essential services they provide." Incident reporting requirements are not limited to "cybersecurity" incidents or external threats; an "incident" is defined as "any event having an actual adverse effect on the security of network and information systems." Accordingly, this may include physical events (such as power failures), insider threats, and accidents as well as intentional actions.

The UK government proposes that:

- for the purpose of defining an incident, there is an impact on continuity where there is a "loss, reduction or impairment of an essential service";
- the threshold for defining what constitutes a significant impact will vary for each sector and should be determined by the relevant competent authorities (following this current consultation); and
- the OES must report an incident "without undue delay" and "at a maximum no later than 72 hours after having become aware of the incident." This is aligned with the breach notification rules under the EU General Data Protection Regulation ("GDPR").

In order to reduce bureaucratic burdens, all NIS incident reporting will be made to one body, namely the National Cyber Security Centre ("NCSC") as the dedicated CSIRT for the purposes of the Directive. The NCSC will be required to copy NIS incident reports to the relevant competent authority within each sector.

DSPs

The incident requirement for DSPs is similar to the requirement for OESs. The government intends to align incident reposting requirements with the framework developed by the European Commission. Notably, the UK government intends to focus the threshold not just on incidents that impact continuity, but also the confidentiality or integrity of the service. The government proposes to run a smaller, targeted consultation on incident reporting for DSPs at a later date, and requested those that are interested in taking part provide appropriate contact details.

WHO ARE THE COMPETENT AUTHORITIES FOR EACH SECTOR/ SUBSECTOR?

The NIS Directive requires Member States to designate a NIS competent authority (one or more) to be responsible for implementing the NIS Directive, publishing guidance, ensuring compliance and enforcing the rules. As explained above, competent authorities have different powers in relation to OESs and DSPs, as it was agreed that DSPs should be subject to a "lighter touch" regime.

Instead of a single national competent authority, the UK government proposes to nominate multiple sector-based competent authorities, which are set out in Annex 2 of the consultation document. For example:

Sector	Subsector(s)	Proposed Competent Authority
Energy	Electricity and gas (downstream)	Secretary of State, Department for Business, Energy and Industrial Strategy ("BEIS"); certain functions may be delegated in whole or part to the Office of Gas and Electricity Markets (Ofgem).
	Gas (upstream) and oil (downstream)	Secretary of State, BEIS; certain functions may be delegated to industry relevant bodies.
Transport	Air transport	The Secretary of State, Department for Transport (DfT), with some functions delegated to the Civil Aviation Authority (CAA).
Digital Infrastructure	N/A	Office of Communications (Ofcom).
Digital Service Providers	online marketplaces; search engines; cloud service providers.	The Information Commissioner's Office (ICO).

Competent authorities for the banking and financial market infrastructures sectors are not being formally identified under this Directive. Firms and financial market infrastructure within these sectors must continue to adhere to requirements and standards as set by the Bank of England and/or the Financial Conduct Authority.

Different authorities are proposed for England, Wales, and Scotland for the water and health sectors, and for the road transport sub-sector. Determining these authorities will require separate engagement with the Devolved Administrations.

The NCSC will provide technical support to each competent authority. It also will act as the UK's "Single Point of Contact" (SPoC) and will be designated as the UK's Cyber Emergency Response Team (or CERT) under the Directive. The consultation seeks responses to the UK government's approach and whether the proposed competent authorities are suitable.

PENALTIES

The NIS Directive leaves it to Member States to lay down the rules on penalties when Member States implement the Directive in their respective national laws. Penalties must be "effective, proportionate and dissuasive."

The UK government believes that the NIS Directive needs to set a high bar for the maximum level of penalty. Accordingly, it proposes to impose penalties that are similar to those under the GDPR, *i.e.*, a two-tier framework:

- tier one fines, for lesser offences (such as failure to cooperate with the competent authority or failure to report a reportable incident), set at a maximum of EUR 10 million or two percent of global turnover; and
- tier two fines, for failure to implement appropriate and proportionate security measures, set at a maximum of EUR 20 million or four percent of global turnover (whichever is greater).

When determining fines, competent authorities will assess whether the incident was foreseeable, whether effective risk management was in place, and whether the OES or DSP had appropriate security measures in place.

The government states that "financial penalties should only be levelled as a last resort where it is assessed appropriate risk mitigation measures were not in place without good reason." Organizations may take a further limited degree of comfort from the statement that "the penalties listed above are maximum penalties, for use in the most egregious incidents, and it is expected that mitigating factors including sector-specific factors will be taken into account by the competent authority when deciding appropriate regulatory response."

In the event of a fine, the organization will be notified and afforded an opportunity to make representations. Decisions taken by the competent authority will be enforceable by civil proceedings, and appealable through the court system.

WHAT IMPACT WILL BREXIT HAVE?

Finally, no UK related post is complete these days without mentioning the "B" word — Brexit. That said, as with the GDPR, the impact of Brexit is likely to be limited.

Until the UK has negotiated its exit from the EU, the UK remains a full member of the EU and all the rights and obligations of EU membership remain in force. This means that the UK is required, as an EU member, to implement the NIS Directive. It is the UK government's intention that on exit from the EU, EU legislation will continue to apply in the UK (at least initially), including the NIS Directive and its UK implementing legislation.