AN A.S. PRATT PUBLICATION
JANUARY 2020
VOL. 6 • NO. 1

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 6 | NUMBER 1 | JANUARY 2020

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*, [6] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [1] (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

(2020–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 inquiries 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, 646.539.8300. 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.

Cookies: A Coming-of-Age Story

By Mercedes Samavi and Alja Poler De Zwart*

The Court of Justice of the European Union in the Planet49 *case recently ruled that implied consent to accept cookies is not sufficient anymore, requiring website operators to seek active consent from users, which cannot be obtained by means of pre-ticked boxes, and any obtained consent will only be sufficiently informed if an average user can understand what cookies do and how they function. The authors explain the decision.*

One of the most recent chapters in the ongoing European Union ("EU") has come in the form of a recent ruling by the Court of Justice of the European Union ("CJEU") in the *Planet49* case.[1] The CJEU ruled that:

- Implied consent is not sufficient anymore, requiring website operators to seek active consent from users which cannot be obtained by means of pre-ticked boxes; and
- Any obtained consent will only be sufficiently informed if an average user can understand what cookies do and how they function.

The outcome of the case – while pivotal – does not come as a surprise considering the cookie developments in the EU over the past few years.

BACKGROUND

In 2003, when the current Privacy and Electronic Communications Directive ("ePrivacy Directive") came into effect, the use of cookies and similar technologies was not as advanced as it is now and did not process users' personal information in the same way and with such complexity. Sixteen years later, cookies and similar technologies have become an indispensable part of almost every business. The amount of useful details that companies learn about their users' interests and internet behavior through such technologies is vast and seemingly unlimited. As you would expect with such rapid technological development, the EU data protection authorities ("DPAs") have caught on that the technologies are a data goldmine.

While the EU ruminates over the precise wording of the upcoming ePrivacy Regulation that will replace the current ePrivacy Directive ("Regulation"), some DPAs have

* Mercedes Samavi is an associate at Morrison & Foerster LLP and a member of both the Technology Transactions Group and the Global Privacy Group. Alja Poler De Zwart is of counsel at the firm representing clients on privacy, data security, and e-commerce matters. The authors may be reached at msamavi@mofo.com and apolerdezwart@mofo.com, respectively.

[1] http://curia.europa.eu/juris/document/document.jsf;jsessionid=63307BE55F72BCA9701B6A79646E9764?text=&docid=218462&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2219854.

decided to take matters into their own hands. Last year alone, several DPAs across the EU proactively revised their regulatory guidance, which to a certain extent reflects, and on other points goes even further than, the *Planet49* ruling.

THE CJEU'S *PLANET49* RULING

The *Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband eV v Planet49 GmbH*[2] focused on a promotional lottery that Planet49 ran on its website. If users wished to enter the lottery, they would be presented with two checkboxes: (1) an unchecked box for receiving third-party advertising and (2) a pre-ticked box permitting Planet49 to set cookies to track the user's online behavior.

The CJEU decided that:

- A *pre-ticked checkbox does not constitute valid cookie consent*. The website operators must obtain an affirmative act from the user that demonstrates unambiguous consent.
- The *requirements for cookie consent are the same as the requirements for consent in the EU General Data Protection Regulation* ("GDPR"), regardless of whether personal information is processed when placing the cookies.
- Website operators are required to *inform users about: (i) cookie retention periods* and *(ii) whether third parties are given access to the cookies (ii) whether third parties are given access to the cookies*.
- Users must be provided with *clear and comprehensive information to allow them to easily determine the consequences of providing consent*. This information should be unambiguous and clearly comprehensible to the average internet user and sufficiently detailed to allow the user to understand the cookie functionalities.

THE DPAS AS SUPPORTING CHARACTERS

As already mentioned above, the *Planet49* ruling follows in the wake of several DPAs' guidelines. In particular, we focus on the guidance from the UK's Information Commissioner's Office[3] ("ICO") and France's Commission nationale de l'informatique et des libertés[4] ("CNIL"). Both guidelines chime with the *Planet49* ruling, even though they are not expressly referred to in the judgment. The table herein sets out an easy comparison of the main issues between the two DPAs:

[2] Case C-673/17.

[3] https://ico.org.uk/media/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies-1-0.pdf.

[4] https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000038783337.

	ICO	CNIL
Implied Consent	Implied consent is no longer sufficient – cookies and similar technologies require a GDPR-style consent. Users must take a clear, positive action to consent to non-essential cookies. Pre-ticked boxes or continuous use of a website is not valid consent.	
Cookie Walls	Cookie walls that restrict access to users in order to influence users to provide consent are likely invalid. Cookie walls are not compatible with the GDPR as they do not let users exercise their choice without suffering major inconveniences in case of denial/ withdrawal of consent.	
Essential Cookies	Consent is not required for cookies that are essential to providing the service requested by the user and cookies that are necessary for transferring information.	
Analytics Cookies	Analytics cookies are not strictly necessary and require user consent.	Analytics cookies do not require user consent, provided that certain conditions are met, including, but not limited to, limiting the lifespan of any analytic cookies to 13 months and that the analytics are placed by the website operator (thus only first-party analytics are allowed).
Proof of Consent	Organizations using cookies must be able to demonstrate proof of the obtained consent.	
Transparency Obligations	Users must receive the same kind of information as they would when their personal information is processed, including the cookies used and the purposes for which they are used. This extends to any cookies set by third parties.	In addition to general information requirements (e.g., the identity of the controller(s), the purposes of cookies and how to withdraw consent), the guidelines specify that there should be an "*exhaustive and regularly updated list of all entities (including third parties) using cookies.*" All information must be complete, visible and highlighted at the time of the collection of consent.

Against these two DPAs' guidance, it is easy to see why the *Planet49* ruling should not be treated as an outlier. In fact, a number of regulators have presented guidelines and recommendations, taking similar positions to the ICO and CNIL, such as the Dutch[5] and the Irish[6] DPAs. Adding fuel to the fire, the Spanish DPA ("AEPD") just issued a €30,000 fine against an organization: users must be provided with the choice to opt out from the placement of cookies, otherwise the act of browsing a website is not by itself a sufficient indication of valid consent. The AEPD fine is likely not the last.

This is not to say that it is the same for all DPAs. Germany has never implemented the ePrivacy Directive. The German Data Protection Conference (which is the body of all German DPAs), however, did publish guidance in April 2019,[7] stating that legitimate interest could be used for some non-essential cookies, provided that the use is proportionate to the impact on the users' privacy rights. It will be hard for a website operator to reconcile this with the ICO's position that active consent is the only option. Similarly, the AEPD has issued guidance[8] stating that implied consent is possible in certain circumstances, which is an interesting divergence from the positions that the ICO and CNIL have taken.

Other DPAs are still in the process of finalizing their guidance. Denmark, for example, has indicated that it plans to issue revised guidance in the near future. It is currently unclear what this guidance will bring, although it is expected that the DPAs will likely not stray far from the above-mentioned approach of their EU counterparts.

All in all, there appears to be no overall harmonization in sight on this topic, so multinational organizations will have a hard time coming up with a practical and cost-efficient approach to compliance.

TAKEAWAYS

The recent developments show that website operators should at least consider the following steps:

- *Reassess your cookie consent mechanism/tool to check that there are no pre-ticked or pre-selected consent boxes or sliders*. The user must be able to actively turn on/toggle any consent boxes/sliders, otherwise they are not considered to be providing valid consent.
- *Include both "accept" and "decline" buttons on your cookie banner, giving the user a clear choice.* EU institutions (like the European Parliament and Commission)

[5] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/normuitleg_ap_cookiewalls.pdf.

[6] https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190612%20Guidance%20on%20Cookies%20and%20Similar%20Technologies.pdf.

[7] https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf.

[8] https://www.aepd.es/media/guias/guia-cookies.pdf.

have all set up their banners in this way. Note that if a user clicks an "x" button to make the banner disappear, this does not mean that they are giving their consent.

- *Review your cookies and similar technologies notice* to determine whether: (i) it adequately covers the information specified in the *Planet49* ruling (i.e., retention periods and third-party recipients) and (ii) it is written in a clear, concise and user-friendly manner that would be understood by an average internet user (and not just your privacy lawyer and IT team who drafted it).

As shown above, the DPAs do not appear to agree which cookies should be made exempt from the consent requirement. Again, this has led to different rules per EU Member States, a scenario that the Regulation will ideally resolve. Until then, some consideration will be needed as to whether you want to apply a pan-European approach, which satisfies the strictest DPA, or a more nuanced approach.

THE NEVER-ENDING STORY

We cannot ignore the ongoing narrative of the Regulation, which has seen some movement recently after a period of inertia. According to the latest draft of the Regulation[9] (as of November 2019), the use of these technologies requires GDPR-standard consent. There are, however, exceptions for technologies that track audience measuring (when carried out by third-party processors), as well as security, fraud prevention, and technical fault detection. These exceptions appear to take a business-friendly approach and in parts are not as restrictive as the ICO's position on the same. In particular, the ICO guidance explicitly defines audience measurement cookies as analytics cookies. (As mentioned above, the ICO requires consent to be obtained for analytics cookies.)

The European Council originally planned on finalizing the draft by December 2019 but the current draft has not received sufficient support as yet to be put in front of the European Parliament.

It is becoming obvious that cookies will be an area of increased regulatory scrutiny over the next few months and beyond. For certain industries, such as analytics and advertising, the *Planet49* ruling and the surrounding DPA guidance will at best stymie future product development and marketing efforts. As a matter of simple psychology, asking users for explicit consent will lead to significantly lower cookies acceptance rates. An average user is more likely to turn off the cookie banner for good, without clicking on the accept button or changing the cookie settings. Organizations have reported to us that implementing the ICO's consent approach for all analytics cookies has practically obliterated their analytics metrics. Consequently, requiring a

[9] https://data.consilium.europa.eu/doc/document/ST-14068-2019-INIT/en/pdf.

GDPR-standard consent for analytics that are not privacy-intrusive and that may not even involve personal information seems like a step too far.

The *Planet49* ruling and the DPAs guidance may have already stolen a march on the upcoming Regulation regarding what constitutes valid consent. However, the GDPR and the Regulation were never meant to stand in the way of organizations doing their business or frustrate whole industries. The EU still has the chance to take a more practical and business-friendly approach that does not compromise individuals' privacy rights. Organizations can therefore only hope that the final version of the Regulation will exempt cookies that are not privacy-intrusive from the consent requirement, harmonizing the conflict in opinion between various DPAs. When it comes down to cookies and similar technologies, this appears to be the most pressing outstanding issue for the Regulation to resolve.

This is therefore not a happy-ending story (yet), and the plot thickens.