Office of Industries
Working Paper ID-096

Taking a Bite Out of Cookies: The Implications of France's Cookie Policies on European Privacy Regulation

October 2022

Brian Daigle and Mahnaz Khan

Abstract

Cookies, a cute name to describe small text files that websites place on a user's device when they are browsing, underpin enormous segments of the digital economy in part because they contain a wealth of data about a particular user. Such data are subsequently monetized and contribute to a multi-billion dollar global digital advertising market. Within this segment of the digital economy, the issue of consenting to the use of cookies as a user browses the web has led to growing attention and increasing oversight from EU regulators. France has been at the forefront of EU efforts to infuse consent into this tracking technology, and the country has sought to curb the use of cookies and similar tracking technologies, in particular following the EU-wide implementation of the General Data Protection Regulation (GDPR) in 2018. Beyond this law, France has developed its own data governance framework, which has increasingly pushed for a more far-reaching approach to cookies regulation within the context of its own domestic laws as well as existing EU directives and regulations. France's data regulator, the Commission Nationale de L'informatique et des Libertés (CNIL), has issued more than €400 million in fines from 2020 to the present for violations, mainly against large U.S.-based multinational tech firms such as Google and Meta. The implication of these new rules and enforcement mechanisms suggests that the use of cookies by firms to turn search results into advertising revenue may be challenged by these developments, particularly in France, and possibly extending to Europe and beyond.

Taking a Bite Out of Cookies: The Implications of France's Cookie Policies on European Privacy Regulation

Brian Daigle and Mahnaz Khan

Office of Industries
U.S. International Trade Commission (USITC)
October 2022

Brian Daigle is a former international trade analyst with the Office of Industries of the U.S. International Trade Commission (USITC). Mahnaz Khan is an international trade analyst with the Office of Industries of the USITC. Office of Industries working papers are the result of ongoing professional research by USITC staff. Working papers are circulated to promote the active exchange of ideas between USITC staff and recognized experts outside the USITC, and to promote professional development of office staff by encouraging outside professional critique of staff research.

 Please direct all correspondence to Mahnaz Khan, Office of Industries, U.S. International Trade Commission, 500 E Street, SW, Washington, DC 20436, telephone: 202-205-2046, email: mahnaz.khan@usitc.gov.

The authors would like to thank Sarah Oliver, Heidi-Colby-Oizumi, and John Fry, for their helpful comments and suggestions and Trina Chambers for her production support.

Introduction

As both the U.S. and global economies now largely depend on transactions facilitated to some degree online, governance of the digital world has become increasingly important from both legal and economic perspectives. In particular, the intersection of individual rights online, especially privacy rights, and commercial transactions have grown in importance across a variety of jurisdictions, including the United States, Brazil, China, the European Union, South Africa, and India. Occasionally, in the interest of protecting individual rights, a regulatory authority or legislative body may bar entire classes of online activity (particularly with respect to terrorism and the rights of children); more often, regulations with the intent of protecting privacy and other human rights usually focus on *how* certain activity may be permitted to occur within the digital space while protecting such rights.

This paper will focus on one instance in this latter category, specifically France's framework for the treatment of "cookies"—online packets of data that track a user's activity and can be carried over from website to website, or within websites. Although cookies may seem functionally obscure, cookies (particularly "third party" cookies)[1] allow firms to monetize the habits and interests of individual users by assessing likely purchasing preferences and facilitating targeted advertising to such users. This process contributes to a digital advertising industry worth hundreds of billions of dollars globally, and supports other industries such as e-commerce and social media.[2] Digital advertising and e-commerce from firms helps to drive global digital trade flows because they facilitate cross-border digital services and physical goods.[3]

Due to a concern that collection and monetization of personal data can lead to significant privacy concerns (as this data can reveal sensitive or personal elements about the user), the European Commission and some European countries have tried to curb the use of cookies.[4] In particular, the issue of cookies consent has drawn considerable attention and increasing oversight from EU and European regulators.[5] France, Belgium, Austria, Germany, Spain and the United Kingdom have all published guidance on the use of cookies and similar tracking technologies after the implementation of the EU-wide General Data Protection Regulation (GDPR) in 2018, with an aim to provide privacy controls to their citizens.[6]

Among these countries, France has been at the forefront, both in the EU and globally, in trying to develop and push a newer and more far-reaching approach to cookies regulation within the context of their own domestic laws, as well as through the use of existing EU directives and regulations.[7] France's main legal framework governing the use of cookies is embodied in a variety of laws and regulations including: EU regulations and human rights law, French national legislation, guidance issued by France's

[1] TechTarget, "What is a Third-Party Cookie," (accessed September 9, 2022).
[2] McKinsey, "The Demise of Third Party Cookies," April 21, 2021.
[3] Office of the U.S. Trade Representative, "Key Digital Trade Barriers," (accessed October 6, 2022).
[4] Trevisan et al., "4 Years of EU Cookie Law: Results and Lessons Learned," 2019.
[5] IAPP, "ICO, CNIL, German and Spanish DPA Revised Cookies Guidelines: Convergence and Divergence," August 2019.
[6] IAPP, "ICO, CNIL, German and Spanish DPA Revised Cookies Guidelines: Convergence and Divergence," August 2019.
[7] Kadar et. al, "Cookie Fines in France in January 2022: Is it the Beginning of a "Cookie Gate"?" February 17, 2022.

data protection authority (Commission Nationale de L'informatique et des Libertés, referred to in this paper as the "CNIL"), and case law from French administrative courts.

Within this multi-tiered framework, the legal grounds and rationale for firms to obtain consent from users in France to place cookies on their devices are principally embodied in two main legal policies: the French Data Protection Act (which implements the EU ePrivacy Directive), and the GDPR.[8] In addition to these laws, there are also a series of recent CNIL guidance documents regarding the use of cookies. Although such guidance is not legally enforceable and not binding on other EU countries, the guidance sheds light on how the CNIL views privacy concerns around the use of cookies.[9] Finally, France's cookie governance is also being shaped by decisions made at the highest French administrative courts, which may lead to spillover policy ramifications throughout the EU and globally.

Privacy experts contend that the CNIL has taken some of the most aggressive action globally on determining when firms can use cookies to collect personal data on their websites, often adopting narrow and specific guidance on the use of cookies.[10] France also adopted more aggressive advocacy on other digital trade policies generally during the French EU presidency from January to June 2022, stating publicly a particular focus on the regulation of cookies for both international and domestic firms.[11] To date, the CNIL has issued over 100 orders and sanctions related to non-compliance with cookie laws and regulations since their cookie legislation went into force on March 31, 2021.[12] In 2022 alone, France fined firms €210 million for non-compliance with cookies rules, significantly more than the total fines issued by France for all other data protection violations under GDPR.[13]

In order to properly frame the discussion on France's approach to cookie regulation and enforcement, this paper will begin with an introduction to cookies and an exploration of the wider importance of cookies in global digital trade. It will continue with a review of France's contemporary framework for the governance of cookies, followed by a look at how France's cookie governance operates in a wider European context. The paper concludes with a review of recent enforcement action by France's digital regulatory authority, the National Commission for Information and Rights (CNIL), which has issued more than €500 million in fines against firms for non-compliance with France's regulation of cookies; these fines were mainly against large U.S.-based multinational tech firms such as Google and Meta (formerly known as Facebook) since 2021.

[8] Vibbert et. al, "Data Protection in France: Publication of Amended Guidelines and Recommendations on Cookies and Other Online Trackers," October 27, 2020.
[9] Vibbert et. al, "Data Protection in France: Publication of Amended Guidelines and Recommendations on Cookies and Other Online Trackers," October 27, 2020.
[10] Manancourt and Kayali, "France Flexes Muscles with Fines against Facebook, Google over Cookie Banners," January 6, 2022.
[11] Manancourt and Kayali, "France Flexes Muscles with Fines against Facebook, Google over Cookie Banners," January 6, 2022.
[12] Dent, "French Regulator Fines Google and Facebook a Combined $238 million Over Cookie," January 6, 2022.
[13] Dent, "French Regulator Fines Google and Facebook a Combined $238 million Over Cookie," January 6, 2022; Hodge, "France's CNIL fines Google, Facebook $237M Combined over Cookies Consent," January 6, 2022.

Defining Cookies

As noted above, cookies are small text files that websites place on a user's device when they are browsing online, which are then processed and stored by the browser.[14] Cookies are generally divided into two types: first-party cookies and third-party cookies. First-party cookies are placed on a user by the website they visit and can be used to collect personal data in order to track the user's behavior on a specific website for advertising purposes.[15] Third-party cookies operate differently because they are set by other domains that the user is not visiting, and are managed by a third party.[16] These third party cookies often collect substantial information about a user through a cumulative effort following the user from site to site.[17] These cookies may ultimately reveal age, place of residence, and buying patterns of a user, thus creating a profile of a user that can be used mainly for advertising purposes, often without the direct consent of the user.[18]

Cookies can also be classified depending on their duration. For example, "session cookies" are defined as temporary in nature and expire once a user closes their online browser or once their session ends.[19] This is in contrast to "persistent cookies" which remain on a user's hard drive until they are erased by the user or browser, depending on the cookie's expiration date which is often written into their code.[20]

Cookies and Digital Trade

As noted above, cookies can store a wealth of data on users, enough for potential disclosure of a user's personal information and their preferences without the user's consent.[21] Given the wealth of knowledge inherent in many these cookies, cookies are often used by websites to accomplish three basic functions: managing existing sessions between the user and the website (often first party cookies); personalizing advertisements based on existing tracked preferences (often third party cookies); and tracking items a user has viewed on the website both as a reference for users and to suggest similar items (both first and third party cookies).[22]

These distinct purposes foster the creation of new digital market sectors or amplify existing ones. Of these functions, the largest market amplified by cookies is the digital advertising market, derived from personalized advertisements (or "targeted" advertisements) that are more likely to solicit engagement from the user and subsequent purchases if directed to sellable products or services.[23] While the tracking of items a user has viewed on an individual website through cookies has also reportedly contributed to stronger digital trade growth (particularly in e-commerce), the size and growth of the digital targeted

[14] GDPR.EU website, "Cookies, the GDPR, and the ePrivacy Directive," (accessed May 24, 2022).
[15] CNIL, "Alternatives to Third-Party Cookies: What Consequences Regarding Consent?" (accessed May 24, 2022).
[16] CNIL, "Alternatives to Third-Party Cookies: What Consequences Regarding Consent?" (accessed May 24, 2022).
[17] CNIL, "Alternatives to Third-Party Cookies: What Consequences Regarding Consent?" (accessed May 24, 2022).
[18] CNIL, "Alternatives to Third-Party Cookies: What Consequences Regarding Consent?" (accessed May 24, 2022).
[19] GDPR.EU website, "Cookies, the GDPR, and the ePrivacy Directive," (accessed May 24, 2022).
[20] GDPR.EU website, "Cookies, the GDPR, and the ePrivacy Directive," (accessed May 24, 2022).
[21] GDPR.EU website, "Cookies, the GDPR, and the ePrivacy Directive," (accessed May 24, 2022).
[22] Kapersky, "What are Cookies?" (accessed May 24, 2022).
[23] Match2One, "Digital marketing post third-party cookies. Here's what you need to know," May 17, 2022.

advertising market in particular is substantial.[24] By one 2021 estimate, the global digital advertising market was valued at around $350 billion, with projected growth to $786 billion by 2027.[25] While estimates vary on the share of the global digital advertising market that is specifically targeted advertising, this sector likely represents the vast majority of the value of advertising online in both the United States and globally.[26] Additionally, the e-commerce market (which is often the intended destination of targeted product advertising) and social media industry (which can use cookies to direct users towards suggested friends and web pages to encourage continued and enhanced online engagement) have also both benefited from such third party cookies, though data on their direct impact is limited.

U.S. tech firms represent a substantial majority of the global digital advertising market, which is often underpinned by the collection of users' data via cookies. Globally, Google and Meta represented a majority of global digital advertising revenue in 2021 with Google (29 percent) and Meta (24 percent) representing around 53 percent of the global market.[27] These global market shares are particularly notable as China, the world's second largest digital advertising market after the United States, has practically zero presence from Google or Meta. In 2021, online advertising revenue in the United States was approximately $190 billion, with Google, Meta, and U.S. e-commerce firm Amazon constituting a combined 64 percent share.[28]

Specific market-level breakdowns of the digital advertising market in France are limited, but available information suggests that Google, Meta, and other U.S.-based tech companies play a similar role in the French digital advertising market as they do globally. For example, one estimate notes that 2021, digital advertising revenue in the search industry represented 42 percent of France's $7.7 billion total digital advertising revenue. [29] Given that Google represents 90 percent of internet search traffic in France, there is a strong probability that Google would likely constitute the vast majority of this digital advertising revenue.[30] Social media advertising, the second largest share of France's total advertising, represents 26 percent of the digital advertising market. Meta likely represents the bulk of the social media advertising revenue given that it is France's largest social media platform with 31 million users in France as of early 2022.[31]

[24] Research and Markets, "Global Digital Advertising and Marketing Market Report 2021," November 22, 2021.
[25] Research and Markets, "Global Digital Advertising and Marketing Market Report 2021," November 22, 2021.
[26] Lomas, "Targeted Ads Offer Little Extra Value for Online Publishers, Study Suggests," May 31, 2019.
[27] GlobalStats, Stats Counter, "Digital Advertising in France," (accessed May 24, 2022).
[28] Statista, "Online Advertising Revenue in the United States from 2000 to 2021," (accessed September 6, 2022), Insider Intelligence, "Google, Facebook, and Amazon to account for 64% of US digital ad spending this year," November 3, 2021.
[29] GlobalStats, Stats Counter, "Search Engine Market Share: France," (accessed May 24, 2022); Statista, "Digital Advertising in France," (accessed May 24, 2022).
[30] GlobalStats, Stats Counter, "Search Engine Market Share: France," (accessed May 24, 2022); Statista, "Digital Advertising in France," (accessed May 24, 2022).
[31] There are 50 million social media users in France, a substantial proportion of its 61 million residents in the country. About half of France's population use Meta's social media platforms, Facebook and Instagram. Statista, "Social Media Usage in France," (accessed May 24, 2022); Kemp, "Digital 2022: France," February 9, 2022.

France's Cookie Policies in a Wider European Context

There are two main policies that govern the use of cookies throughout Europe: the EU GDPR and the ePrivacy Directive. The ePrivacy Directive was passed in 2002 and amended in 2009 and has since become known as the "Cookie Law."[32] As a directive, implementation of the ePrivacy Directive falls to EU member states, which have crafted a variety of laws that differ by scope, breadth, and enforcement.[33] In addition, the EU is working towards finalizing a draft ePrivacy Regulation, which if passed would heighten the requirements for cookie consent among European data subjects to be in line with the explicit consent provisions under GDPR.

In recognizing the privacy implications of the use of cookies, in 2009 the ePrivacy Directive was amended to mandate that EU members set up their own national cookie laws by May 2011. It also required that website owners obtain informed consent before storing or retrieving information on a EU user's device.[34] In mandating laws to be crafted to govern cookies, the ePrivacy Directive acknowledges that cookies could be used for "strictly necessary" basic functions of a website, for example cookies that manage items put in a shopping cart by the user.[35] The Directive also states that users must be given clear and comprehensive information by the website owner as to why their data is being processed, stored, or accessed.[36] Users must also be given a choice to refuse consenting to cookies by the website owner.[37] Following the amended ePrivacy Directive's new cookie provisions, one of the most obvious effects for users was the proliferation of cookie consent pop-ups on EU websites, which subsequently became commonplace across developed markets.[38]

[32] European Union, GDPR.EU, "Cookies, the GDPR, and the ePrivacy Directive," (accessed September 12, 2022).
[33] Under EU law, an EU directive requires EU member states to craft their own laws to address the goals envisioned by the directive at a national level. In contrast, an EU regulation is fully enforceable across the EU, though member states may need to pass subsequent implementing legislation if enforcement is partially or fully devolved to member states. European Union, "Types of Legislation," (accessed September 11, 2022).
[34] The 2002 ePrivacy Directive was known as the 'Directive on Privacy and Electronic Communications', with further amendments to cookie usage made in 2009. Ionos, "EU Cookie Laws and How They Affect your Business," February 16, 2022; Privacy Policies, "Ultimate Guide to EU Cookie Laws," November 15, 2021.
[35] JD Supra, "France Fines Facebook and Google for Violating the EU Cookie Law: You Need to Make it As Easy to Refuse as a Cookie, as it is to Accept One," January 10, 2022.
[36] JD Supra, "France Fines Facebook and Google for Violating the EU Cookie Law: You Need to Make it As Easy to Refuse as a Cookie, as it is to Accept One," January 10, 2022.
[37] JD Supra, "France Fines Facebook and Google for Violating the EU Cookie Law: You Need to Make it As Easy to Refuse as a Cookie, as it is to Accept One," January 10, 2022.
[38] The ePrivacy Directive, along with GDPR, appeared to have a set norms in certain markets such as Mexico, Canada, Nigeria, South Africa, Japan, among others where express consent was expected by data user for the use of cookies on websites. Ionos, "EU Cookie Laws and How They Affect your Business," February 16, 2022; Privacy Policies, "Ultimate Guide to EU Cookie Laws," November 15, 2021; Bateman, "Cookie Consent Outside the EU," August 24, 2022.

The EU Parliament recognized the need to update the ePrivacy Directive to bring the Directive in line with the privacy and consent principles contained in the GDPR.[39] During the time that GDPR was signed into law, the EU Parliament also drafted the ePrivacy Regulation, which promises to create more robust protections for protecting user's data and their metadata.[40] The draft ePrivacy Regulation reaffirms the principles in GDPR that cookies and trackers on a user's website will need explicit and affirmative consent from users before being used.[41] Given the ongoing debate about the consent and cookie provisions in the ePrivacy Regulation, privacy experts expect that the ePrivacy Regulation is unlikely to pass before 2023 with an implementation date of 2025 at the earliest.[42]

In 2016, the GDPR added to European cookie governance. While both GDPR and the ePrivacy Directive address the regulation of cookies in Europe and the general rules around tracking Internet users, the GDPR differs from the ePrivacy Directive in that it is a comprehensive regulation that has binding legal force throughout every EEA and EU member state.[43] GDPR, which became enforceable in May 2018, heightened the requirements for firms to obtain valid and express consent for the use of personal data.[44] While the GDPR implies that not all cookies can be considered personal data because they may not be used in a way that could identify users, practically speaking, the majority of cookies on EU websites are likely subject to GDPR because they are used for analytics, advertising and functional services.[45] Cookies are explicitly mentioned only once in the GDPR under Recital 30, which clarifies that cookies can be used to gather personal data because users may be associated with online identifiers provided by their devices, applications, tools and protocols (such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags), which may leave traces that can be combined with unique identifiers and other information to create user profiles and identify

[39] Koch and Rammos, "Cookies Under Attack – New Decisions by European Data Protection Authorities on Online Advertising," February 11, 2022.
[40] European Commission, "Proposal for an ePrivacy Regulation," (accessed May 24, 2022); Koch and Rammos, "Cookies Under Attack – New Decisions by European Data Protection Authorities on Online Advertising," February 11, 2022.
[41] Koch and Rammos, "Cookies Under Attack – New Decisions by European Data Protection Authorities on Online Advertising," February 11, 2022.
[42] The ePrivacy Regulation has been met with difficulties in the negotiation process since its first draft in January 2017. Since 2017, informal negotiations continued between the EU Commission, Parliament, and the Council of Ministers and a version of the draft was finally approved in February 2021. Despite the consensus from those three governing EU bodies, the European Data Protection Board (EDPB) had criticisms on the latest proposals in March 2021 because the EDPB interprets cookie walls as not compatible with the consent provisions in GDPR. EU regulations need a transition of 24 months before they can be implemented into EU law. Koch and Rammos, "Cookies Under Attack – New Decisions by European Data Protection Authorities on Online Advertising," February 11, 2022.
[43] Since May 2018, GDPR was implemented as a comprehensive law governing the protection of personal data and the privacy rights of individuals online for residents of the 27 countries in the EU, the three European Economic Area (EEA) member states not part of the EU (Norway, Liechtenstein, and Iceland), and the United Kingdom until the country formally exited the EU.
[44] GDPR.EU website, "Cookies, the GDPR, and the ePrivacy Directive," (accessed May 24, 2022).
[45] This notion is contained in Recital 26 of the GDPR because cookies may be considered personal data used to identify an individual either directly or indirectly (whether on its own or in conjunction with other information).EU General Data Protection Regulation, Article 4, May 25, 2018; Irwin, "How the GDPR Affects Cookie Policies," April 12, 2022; EU General Data Protection Regulation, Recital 26, May 25, 2018.

them.[46] It is up to the firms to find a legal grounds for processing the data under GDPR's provisions if the firm were to use data extracted from cookies.[47]

Under GDPR, the concept of consent is viewed as fundamental in ensuring a user's right to privacy. Article 4 of the GDPR explicitly states that consent is only valid from a user if it is "freely given, specific, informed and unambiguous indication of the data subject's wishes" and there needs to be a "clear affirmative action" by the user to signify agreement to the processing of personal data relating to the user.[48] In order to obtain this type of explicit consent to process data from the user through the use of cookies, firms have been using two main methods to obtain consent: 1) cookie walls, or 2) consent by continuing to scroll by placing a narrow banner at the top of the screen that states to the user that "by continuing to scroll, you provide consent to the use of cookies."[49] However, one problematic provision for firms when using these methods of obtaining consent for cookie use is that Article 7(3) requires that it "shall be as easy to withdraw as to give consent" to the use of personal data.[50] As a result, many of these traditional methods of soliciting consent have been subject to legal action in both the EU and national EU member states' courts due to their ambiguous nature of the term "consent" and how easily users can withdraw their consent under GDPR.[51]

The GDPR and the ePrivacy Directive are enforced through different mechanisms, which inadvertently leads to differences in enforcement approaches within countries or throughout the EU. The GDPR delegates most enforcement to EU member states' data protection authorities with larger umbrella organizations such as the European Data Protection Board carrying supranational and coordinating authorities, as well as court of last resort authorities for disputes between data protection authorities and interested parties. In practical terms, member states have enforced different GDPR provisions differently based on the focus of data protection authorities, and industries have also been impacted unevenly.[52] In contrast, the ePrivacy Directive must be implemented into a country's national law, and each EU member state has the sole authority to determine individually how the law is enforced within its own country.[53] As a result, enforcement activity under the ePrivacy Directive varies greatly. Some countries only reportedly minimally enforce their national cookie oversight obligations, while France's

[46] EU General Data Protection Regulation, Recital 30, May 25, 2018. GDPR.EU website, "Cookies, the GDPR, and the ePrivacy Directive," (accessed May 24, 2022).
[47] Irwin, "How the GDPR Affects Cookie Policies," April 12, 2022.
[48] EU General Data Protection Regulation, Article 4, May 25, 2018.
[49] A "cookie wall" is a script or popup screen that bars users from seeing a site's content unless they consent to cookies. The cookie wall blocks the visitor from accessing content unless they click the "Accept cookies" button on the popup. Dearie, "GDPR Cookies: Consent & Policy Requirements," October 4, 2021.
[50] EU General Data Protection Regulation, Article 7(3), May 25, 2018.
[51] Lomas, "Targeted Ads Offer Little Extra Value for Online Publishers, Study Suggests," May 31, 2019.
[52] Daigle and Khan, "The EU General Data Protection Regulation: An Analysis of Enforcement Trends by EU Data Protection Authorities," June 2020; European Data Protection Board, "Opinion 5/2019 on the Interplay between the ePrivacy Directive and the GDPR, in Particular Regarding the Competence, Tasks and Powers of Data Protection Authorities," March 19, 2019.
[53] European Data Protection Board, "Opinion 5/2019 on the Interplay between the ePrivacy Directive and the GDPR, in Particular Regarding the Competence, Tasks and Powers of Data Protection Authorities," March 19, 2019.

CNIL has enforced its national cookie law aggressively, using heavier fines than those issued under GDPR.[54]

In addition to the discussions around updating the ePrivacy Directive, the mechanics of how to legally consent to cookies has been the focus of recent EU judicial cases. In October 2019, the EU Court of Justice (CJEU), ruled that a German company, Planet49, violated GDPR and the ePrivacy Directive when Planet49's website operators used pre-ticked boxes for cookie consent.[55] In the ruling, the CJEU stated that the only form of valid consent for processing user data in the EU is explicit consent, and defined "explicit consent" as consent that is actively and specifically given by the website users by ticking an un-ticked box (as opposed to accepting a pre-ticked box), for example.[56] The CJEU noted in its decision that, in addition to specific and explicit consent, information that the website owner must give a user includes the duration of the operation of cookies and whether or not third parties may have access to those cookies.[57] The verdict by the CJEU was the first post-GDPR court decision that deals squarely with consent provisions in EU privacy laws relating to website cookies and tracking.[58]

The European Data Protection Board (EDPB), an independent European body whose purpose is to ensure consistent application of European data protection regulations, has been quick to adopt new guidance in its attempt to comply with recent EU court cases regarding the interpretation of consent of cookies.[59] After the 2019 CJEU decision noted above, the EDPB released new cookie guidance in May 2020 to note that "cookie walls" did not fulfill the consent provisions of European law.[60] France's CNIL also issued subsequent guidance on cookies in October 2020, following the EDPB and CJEU decisions.[61] Although the CNIL's guidance is not binding on the EU as a whole, it does reflect a more stringent view on how consent can validly be obtained from users for cookies, which is explored in the section below. Most recently, in January 2022, the EDPB established a "cookies task force" to continue to develop a harmonized approach to EU-wide data protection rules and a "consistent interpretation of cookie consent requirement" by the EDPB.[62]

[54] Manancourt and Kayali, "France Flexes Muscles with Fines against Facebook, Google over Cookie Banners," January 6, 2022.
[55] The case was brought by the German Federation of Consumer Organizations to challenge a German company, Planet49, right to use of pre-ticked checkboxes in connection with online promotional games, by which internet users wishing to participate consent to the storage of cookies. CookieBot, "Active Consent and the Case of Planet49," January 17, 2022; Court of Justice of the European Union, "Judgment in Case C-673/17," October 1, 2019.
[56] CookieBot, "Active Consent and the Case of Planet49," January 17, 2022; Court of Justice of the European Union, "Judgment in Case C-673/17," October 1, 2019.
[57] Court of Justice of the European Union, "Judgment in Case C-673/17," October 1, 2019.
[58] CookieBot, "Active Consent and the Case of Planet49," January 17, 2022.
[59] European Data Protection Board, "Who We Are," (accessed May 24, 2022).
[60] Bateman, "French Cookie Compliance 2021 Crackdown," May 9, 2022.
[61] Bateman, "French Cookie Compliance 2021 Crackdown," May 9, 2022.
[62] European Data Protection Board, "EDPB Adopts Guidelines on Right of Access and Letter on Cookie Consent," January 19, 2022, JD Supra, "EDPB Adopts Guidelines on Right of Access and Letter on Cookie Consent," January 22, 2022.

France's Regulatory Framework for Cookies

France's CNIL is one of Europe's most active regulators and has publicly stated that cookies compliance ranks high on its list of enforcement priorities.[63] The CNIL is responsible for enforcing both the GDPR and the ePrivacy Directive vis-a-vis the French Data Protection Act (French DPA).[64] France transposed the ePrivacy Directive into Article 82 of the French Data Protection Act, which states that any user of an electronic communication service will be "informed in a clear and comprehensive manner by the controller regarding the purpose of any action intended to provide access, electronically, to information previously stored in his electronic connection terminal device, or to record data on this device."[65] In enforcing the French DPA, the CNIL has focused on how cookie collection practices do not comply with GDPR provisions and how these practices have created an unbalanced system where acquiescing to consent is easy on the part of the user, but withdrawal of consent by the user is much more difficult.[66]

The CNIL has issued a series of guidance documents pursuant to the French DPA to address how they view cookie compliance in the face of the changing privacy landscape within Europe. After GDPR went into effect, the CNIL updated its 2013 cookie guidelines because its advice was not compatible with the definition of "consent" contained in the GDPR.[67] In 2019, France issued additional guidelines for cookies to clarify the need for firms need to gain consent for cookies from their users, noting that if a user is simply browsing a website, this action in itself did not constitute valid consent by the user to accept cookies placed on their browser.[68]

The CNIL's 2019 guidance on what constitutes consent for cookies was met with resistance from industry. Several professional associations comprising online advertising and commerce professionals took legal action before the French Administrative Supreme Court (Council of State), a government body that acts as a legal advisor for the executive branch and the supreme court for administrative justice.[69] In June 2020, the Council of State largely validated CNIL's 2019 cookie guidelines but noted an exception that the CNIL exceeded its authority when it determined that a user's access to a website could not be conditioned on the user's acceptance of a cookie wall because it was inconsistent with the provisions of GDPR.[70]

Following the decision of the Council of State, the CNIL amended its 2019 guidelines and adopted the 2020 guidelines to tackle the issue of the use of cookie walls.[71] After the Council of State's decision, the

[63] JD Supra, "Whether You Like it or Not, Cookies are Back on the Menu and UK and EU Data Protection Authorities are Taking Enforcement Action," July 27, 2021.
[64] Hennel, "FAQs: What Do I Need to Know about France's Cookie Law Guidelines?" (accessed May 24, 2022).
[65] French Data Protection Act, Unofficial Translation, June 1, 2019.
[66] JD Supra, "Whether You Like it or Not, Cookies are Back on the Menu and UK and EU Data Protection Authorities are Taking Enforcement Action," July 27, 2021.
[67] JD Supra, "CNIL Publishes FAQ Clarifying Cookie Use," April 1, 2021.
[68] CNIL, "Cookies and Other Tracking Devices: the CNIL Publishes New Guidelines," July 23, 2019.
[69] Vibbert et. al, "Data Protection in France: Publication of Amended Guidelines and Recommendations on Cookies and Other Online Trackers," October 27, 2020.
[70] Vibbert et. al, "Data Protection in France: Publication of Amended Guidelines and Recommendations on Cookies and Other Online Trackers," October 27, 2020.
[71] CNIL, "Cookies and Other Tracking Devices: the Council of State issues its Decision on the CNIL Guidelines," June 29, 2020.

CNIL stated that, pending permanent clarification on this issue by European legislators, they would determine the legality of cookie walls on a case-by-case basis.[72] In other words, there was no blanket ban on the use of cookie walls in the 2020 guidance, as there was in the 2019 guidance from the CNIL.[73] The CNIL clarified that they would pay close attention to whether websites offer satisfactory alternatives to a cookie wall or other easy methods to withdraw consent.[74] In practice, the CNIL recommends that websites contain a consent collection interface that includes not only an "accept all" button but also a "refuse all" button.[75] An interesting trend noted from CNIL's 2020 guidelines is that France is expanding the reach of their policy decisions to target the use of cookies on a broad number of tracking technologies on various devices such as tablets, smartphones, desktop computers, laptops, game consoles, connected TVs, connected vehicles, voice assistants, among others.[76]

In 2020, the EDPB explicitly stated that cookie walls were not compliant with the GDPR's consent requirement, while the CNIL's 2020 guidance stated they would be examined on a case-by-case basis.[77] France was in a difficult position because it had to comply with the EDPB's decision, leaving a large regulatory gap for the cookies issue in France.[78] In order to reconcile the regulatory discrepancies, the CNIL issued new guidance in 2022 on cookie walls indicating that GDPR's requirements on consent (that is must be specific and freely given) does not mean that cookie walls are generally prohibited.[79] The new guidance states that cookie walls may be valid if "a real and satisfactory alternative" exists that allows a user to refuse the cookie wall and this alternative option does not create an imbalance for the user refusing the cookies.[80] Moreover, CNIL's 2022 guidance states that firms are allowed to charge a reasonable subscription fee designed to compensate for the loss of advertising revenue, which must be paid before a site can be accessed (i.e., a paywall).[81] The guidance makes it clear that no cookies should be placed where the user has opted for paid access except for cookies that are essential for the website to function correctly.[82]

This 2022 guidance was in stark contrast to the CNIL's 2019 guidance that stipulated that cookie walls were generally prohibited on the basis that they violate the principle of "free consent."[83] While the CNIL now allows for the use of cookie walls, industry experts state that there is not clear and tangible criteria

[72] CNIL, "Questions and Answers on the Amending Guidelines and the CNIL's "Cookies and other Tracers" Recommendation," May 4, 2022.
[73] Galanis and Crouzet, "France: CNIL Opens Door to Cookie Walls - A Closer Look at the New Criteria," May 2022.
[74] CNIL, "Questions and Answers on the Amending Guidelines and the CNIL's "Cookies and other Tracers" Recommendation," May 4, 2022.
[75] CNIL, "Cookies and Other Tracers: the CNIL Publishes Amending Guidelines and its Recommendation," October 1, 2020.
[76] Vibbert et. al, "Data Protection in France: Publication of Amended Guidelines and Recommendations on Cookies and Other Online Trackers," October 27, 2020.
[77] European Data Protection Board, "Guidelines 05/2020 on consent under Regulation 2016/679," adopted May 4, 2020.
[78] Galanis and Crouzet, "France: CNIL Opens Door to Cookie Walls - A Closer Look at the New Criteria," May 2022.
[79] Lanois, "France's CNIL Issues Guidance on the Issue of Cookie Walls," (accessed September 8, 2022).
[80] Lanois, "France's CNIL Issues Guidance on the Issue of Cookie Walls," (accessed September 8, 2022).
[81] Hewson, "Data Protection Update – May 2022," June 1, 2022.
[82] Hewson, "Data Protection Update – May 2022," June 1, 2022.
[83] Lanois, "France's CNIL Issues Guidance on the Issue of Cookie Walls," (accessed September 8, 2022).

to perform this case-by-case analysis.[84] For example, industry experts expressed concern that the CNIL's 2022 guidance will require additional interpretation by firms, especially with respect to what is a "fair price" or which websites can be considered as "dominant or essential service providers."[85] This ambiguity may leave firms open to more judicial action, while increasing their business costs and restricting digital trade in France.

France's Approach to Data Protection Act Enforcement

As part of the CNIL's focus on cookie compliance relative to other European data protection authorities, the CNIL has issued more than €500 million in fines against firms for violating French data regulatory policies specifically focusing on non-compliance with French residents' privacy rights in not adequately soliciting consent in the use of cookies.[86] Nearly 90 percent (€445 million) of these fines have been issued against large U.S. technology companies under Article 82 of France's Data Protection Act, and they were calculated based on CNIL's estimate of the advertising revenue that was gained from users that likely would have otherwise rejected cookies (or, as in recent cases, if rejecting cookies was not as easy as accepting them).[87] In addition to these fines, the CNIL warned more than 90 companies in 2022 of potential non-compliance concerns with France's cookies obligations and has issued more than 100 judgments overall against firms for non-compliance with cookies regulations. Table 1 below represents the known fines issued by CNIL for non-compliance with cookies obligations and represents the vast majority of all data governance fines issued by France in the last two years.

[84] Galanis and Crouzet, "France: CNIL Opens Door to Cookie Walls - A Closer Look at the New Criteria," May 2022.
[85] Faber, "Fresh from the Oven: The CNIL's Criteria for Allowing Cookie Walls in France," May 17, 2022.
[86] These fines include €59 million under GDPR and €450 million under Article 82 of the French Data Protection Act.
[87] Other smaller fines have also been issued for firms' violation cookies provisions of the French Data Protection Act. In August 2021, the CNIL issued a €2.3 million fine to a large retailer for failing to use cookies (among other violations, while a bank was fined that same month €800,000 for the same reason (also among other violations). CNIL, "The Sanctions Issued by CNIL," December 1, 2021.

Table 1 France's Fines under the French Data Protection Act for Cookie Violations, 2020–22

Company	Date	Fine	Reasons for Violation
Google	March 2020	€100 million	Not providing French users sufficient knowledge or consent on seven cookies that were dropped into users' terminals as they used Google products.
Google	December 2020	€100 million	Alleged failure to: (1) obtain the consent of users of the French version of Google's search engine (google.fr) before setting advertising cookies on their devices; (2) provide users with adequate information about the use of cookies; and (3) implement a fully effective opt-out mechanism to enable users to refuse cookies (subsequently confirmed by the Council of State in January 2022).
Amazon	December 2020	€35 million	Alleged failure to: (1) obtain the consent of users of the amazon.fr site before setting advertising cookies on their devices; and (2) provide adequate information about the use of cookies (subsequently confirmed by the Council of State in June 2022).
Google	December 2021	€150 million	Lack of ease for users to reject the use of cookies on Google.fr and Youtube.com.
Meta (Facebook)	December 2021	€60 million	Lack of ease for users to reject the use of cookies on Facebook.com.
Total Fines		€445 million	

Sources: CNIL, "The Sanctions Issued by CNIL," December 1, 2021; Hunton Andrews Kurth. "CNIL Fines Google and Amazon 135 Million Euros for Alleged Cookie Violations." December 14, 2020; European Data Protection Board, "The CNIL's Restricted Committee Imposes a Financial Penalty of 50 Million Euros against Google LLC," January 19, 2019.

As noted in the table above, France's enforcement fines for violating cookies obligations under the Data Protection Act since 2020 have been mainly against three main U.S. tech firms—Amazon, Google, and Meta (Facebook). The French regulator has so far honed in on two key types of cookie violations: 1) failure to allow users to refuse cookies as easily as accept them; and 2) automatically placing cookies on users' devices before they have a chance to accept or refuse them. While it is possible that these types of violations are widespread across Europe (as these are often fairly standard practices), privacy experts argue that so far among data protection authorities only the CNIL appears to be focused on addressing these violations through large-scale fines; this fine was upheld by the French Council of State in January 2022.[88] In the March 2020, December 2020, and December 2021 cases, CNIL criticized Google and Meta's complicated design for rejecting cookies, requiring several clicks to reject cookies, while allowing cookies only required a single click.[89] With respect to the most recent fines in particular, the CNIL has made it clear in its determinations that one of its overarching data governance arguments is that the

[88] Commission Nationale de L'informatique et des Libertés (CNIL). "Deliberation of the Restricted Formation n°SAN-2021-023 of December 31, 2021 Concerning the Companies Google LLC and Google Ireland Limited," January 6, 2022; Koch and Rammos, "Cookies Under Attack – New Decisions by European Data Protection Authorities on Online Advertising," February 11, 2022; Ghebali, "Rejecting Cookies Should be as Easy as Accepting Cookies: New Sanctions by the French Authority (CNIL)," February 14, 2022.

[89] Koch and Rammos, "Cookies Under Attack – New Decisions by European Data Protection Authorities on Online Advertising," February 11, 2022; Armingaud and Scarparo. "GDPR, Cookies, and the Ever-Filling Jar of European Data Protection," January 26, 2022.

ability for users to reject cookies should be as easy and readily available as it is to accept them (in alignment with GDPR).

The CNIL has increasingly employed the provisions of France's Data Protection Act in pursuing data governance and regulatory enforcement within French territory (at least from the perspective of monetary penalties for non-compliance), rather than through the use of GDPR.[90] Privacy experts argue that the CNIL's growing trend of imposing heavy fines for cookie law violations using their national cookie law as opposed to GDPR may be in part motivated by a desire to maintain a degree of control over the protection of French data and French user rights when the structure of GDPR does not provide France with the authority to act as it otherwise would.[91] When compared to the fines issued by France for GDPR non-compliance, or of fines issued by other data protection authorities against these same U.S. tech platforms under GDPR, the CNIL has often adopted far higher monetary penalties for violating the cookie law. France's data protection authority has justified this by noting that they have the authority to impose sanctions on cookie law violations outside of the mechanisms of GDPR (which states that fines should be imposed by the data protection authority where the firm is headquartered in the European Union, rather than in the EU country where the violation occurred).[92] Often, when GDPR fines are imposed on firms by the countries where they are headquartered (such as Ireland), France has reportedly expressed skepticism that such fines are often too low, and would represent a smaller penalty than the country would have preferred had they had the ability to do so. Thus, privacy experts note that France's use of the cookie law may represent an effort to circumvent this limitation.[93]

Privacy experts observe that CNIL's decisions were reached in the context of a global compliance strategy regarding cookies, initiated by the CNIL more than two years ago.[94] The CNIL continues to push the envelope for cookies regulations because the agency publicly stated that new control measures will be used to target national and international private actors and public organizations that use cookies to collect data, especially those that are political party websites.[95] Privacy experts note that orders and enforcement fines for cookie violations were against U.S. tech firms that have their EU headquarters located outside of France. In the case of both Google and Meta, their lead supervisory authority is Ireland, which has been reportedly slower in enforcement actions for cookies violations than France. So far, the CNIL's fines for cookie violations under their national law currently exceeds Ireland's total fines against U.S. tech companies for GDPR violations.[96] In June 2022, the French Council of State affirmed

[90] Lexology, "French Regulator Issues Record Fines for Facebook and Google Cookie Violations," February 1, 2022.
[91] Duball, "CNIL's ePrivacy Fines Reveal Potential Enforcement Trend," January 10, 2022.
[92] Azim-Khan, "Record €210 Million in Fines for Breach of Cookies and Website Tracking Rules—Note e-Privacy Directive, Not Just GDPR," January 10, 2022.
[93] Azim-Khan, "Record €210 Million in Fines for Breach of Cookies and Website Tracking Rules—Note e-Privacy Directive, Not Just GDPR," January 10, 2022.
[94] Kadar, Daniel, Laetitia Gaillard and Sarah O'Brien Kadar. "Cookie Fines in France in January 2022: Is it the Beginning of a "Cookie Gate"?" Technology Law Dispatch. February 17, 2022.
[95] Pollet, "Cookies: French Data Protection Watchdog Welcomes Increased Compliance," September 14, 2021.
[96] Duball, "CNIL's ePrivacy Fines Reveal Potential Enforcement Trend," January 10, 2022; Manancourt and Kayali, "France Flexes Muscles with Fines against Facebook, Google over Cookie Banners," January 6, 2022.

that the CNIL is allowed to impose sanctions on cookies outside of the "one-stop-shop" mechanism under the EU GDPR.[97]

With these large fines, several subsequently upheld by French administrative courts, privacy experts noted trends emerging from France that may change the trajectory of the use of cookies throughout Europe, or possibly globally.[98] Although the use of cookies has long been on the radar of privacy watchdogs in the EU, the extendibility of French cookies governance norms across the EU will depend on the enforcement regulations and domestic laws adopted by other EU member states.[99] Recent decisions by the CNIL and the French courts based on the French Data Protection Act send a clear signal to firms that they need to comply with CNIL's cookie guidelines and recommendations with respect to cookies despite the fact that CNIL's decisions are only binding in France. Firms are naturally worried that they may be subject to fines if they have similar cookie banners as Meta and Google in other European countries, so firms may be forced to adopt a global compliance strategy based on France's strict cookie laws to lessen their risk of overall fines in Europe.[100]

While one European data privacy expert noted that the CNIL is somewhat "isolated" in its enforcement of cookies consent among EU member states, there are several small signs that other EU countries may adopt a more aggressive approach on seeking full and robust consent to the collection and use of cookies.[101] In December 2021, Austria's data protection authority ruled that Google's standard contractual clauses (as well as other measures) within the framework of Google Analytics were not sufficient to prevent the possibility of access by U.S. authorities.[102] The collective German data protection authorities (each state in Germany has its own data protection authority, in addition to the German national data protection authority) have also worked on draft guidance regarding the governance of cookies and consent provisions in Germany with respect to both GDPR and the 2021 German Telecommunications Telemedia Data Protection Act. Finally, the UK Information Commission Office (ICO) adopted guidance that indicated that "nudge behavior" that tilts users in favor of accepting cookies would likely be non-compliant with UK laws.

---

[97] GDPR provides for one-stop shop enforcement by the lead supervisory authority, which is determined based on the "main establishment" of a company in the EU (often where the company is headquartered in the EU). The one-stop shop enforcement allows for other supervisory authorities to join in enforcement with the lead supervisory authority. The one-stop shop enforcement under GDPR was to streamline EU-wide enforcement under GDPR but has met with resistance from some EU data protection authorities. CNIL, "Cookies: the Council of State Confirms the 2020 Sanction Imposed by the CNIL Against Amazon," June 28, 2022; IAPP, "The CJEU Did Not Rescind the One-Stop Shop. Quite the Opposite," July 1, 2022.

[98] Kadar, Daniel, Laetitia Gaillard and Sarah O'Brien Kadar. "Cookie Fines in France in January 2022: Is it the Beginning of a "Cookie Gate"?" Technology Law Dispatch. February 17, 2022, Tech Crunch, "Google to Update Cookie Consent Banner in Europe Following Fine," April 21, 2022.

[99] Koch and Rammos, "Cookies Under Attack – New Decisions by European Data Protection Authorities on Online Advertising," February 11, 2022; Duball, "CNIL's ePrivacy Fines Reveal Potential Enforcement Trend," January 10, 2022.

[100] Kadar, Daniel, Laetitia Gaillard and Sarah O'Brien Kadar. "Cookie Fines in France in January 2022: Is it the Beginning of a "Cookie Gate"?" Technology Law Dispatch. February 17, 2022.

[101] Duball, "CNIL's ePrivacy Fines Reveal Potential Enforcement Trend," January 10, 2022.

[102] Koch and Rammos, "Cookies Under Attack – New Decisions by European Data Protection Authorities on Online Advertising," February 11, 2022.

More significantly, in February 2022, the Belgian Data Protection Authority (APD) ruled that the cookie consent policies of IAB Europe, Europe's premier online advertisers' consortium (headquartered in Brussels), were invalid under GDPR.[103] The ruling noted that the transparency and consent string, which consists of the information of an individual user when they click "accept all cookies," represented "personal data" and could thus be subject to GDPR provisions.[104] As this represented personal data and its processing for ad purposes, the Belgian Data Protection Authority ruled that IAB Europe had failed to provide a sufficient legal basis to process such information for adtech providers, violating articles 12, 13, and 14 of GDPR.[105] The ruling also noted that some processes used were too general and vague to gain sufficiently informed consent, that the identification of purposes associated with authorization were unclear, and that the large number of third parties that could receive this personal data were either not compatible with GDPR's consent provisions or with wider GDPR transparency obligations.[106] By linking the collection of cookies with personal data, this ruling could provide further opportunities for EU data protection authority to extend GDPR oversight to cookies (though litigation on this case remains ongoing, and the Belgian APD ruling and its interpretation of cookies as representing personal data is not binding on other EU countries), and IAB Europe is currently being tasked with forming a plan to ensure that the collection and use of cookies for digital advertising using its framework (used by the majority of European websites) is legal under GDPR.[107]

Conclusion

The future of cookies regulation in Europe may depend on existing draft legislation, particularly the ePrivacy Regulation. Even in the absence of such binding EU-wide legislation, other European countries slowly adopting guidance similar to France's, especially within the context of GDPR, may lead to more aggressive oversight of the use of cookies for targeted advertising purposes by large and small technology platforms and firms. In certain instances, this oversight may already be having an impact on internal firm operations; in July 2022, Google announced that it would block third-party tracking cookies in the Chrome browser by the end of 2024.[108] This followed an agreement with the UK Competition and Markets Authority on how Google develops and releases its "Privacy Sandbox" on Chrome globally.[109] The significance of these changes for the wider digital advertising, e-commerce, and social media companies that have previously derived substantial revenue on third-party tracking cookies designed to provide more precise targeted advertising remains uncertain and the subject of debate. However, this

[103] Carroll, "The Cookie Clutter Crumbles: Ad Tech Industry's Consent Framework Isn't GDPR-Compliant," February 2, 2022.
[104] Carroll, "The Cookie Clutter Crumbles: Ad Tech Industry's Consent Framework Isn't GDPR-Compliant," February 2, 2022.
[105] Carroll, "The Cookie Clutter Crumbles: Ad Tech Industry's Consent Framework Isn't GDPR-Compliant," February 2, 2022.
[106] Carroll, "The Cookie Clutter Crumbles: Ad Tech Industry's Consent Framework Isn't GDPR-Compliant," February 2, 2022.
[107] Kadar, Daniel, Laetitia Gaillard and Sarah O'Brien Kadar. "Cookie Fines in France in January 2022: Is it the Beginning of a "Cookie Gate"?" Technology Law Dispatch. February 17, 2022.
[108] This deadline actually represented a delay in its initial plan to block third party tracking cookies on Chrome, which had originally been scheduled to conclude at the end of 2022 following a 2020 announcement. Business Standard, "Google Now Delays Blocking 3rd Party Cookies in Chrome to Late 2024," July 28, 2022.
[109] Business Standard, "Google now delays blocking 3rd party cookies in Chrome to late 2024," July 28, 2022.

evolving regulatory field will likely continue to impact U.S. and other countries' technology firms operating in Europe which have historically relied on this technology to derive advertising revenue or ongoing user engagement, whether due to fines for non-compliance (as noted above) or changes in industry practice.[110]

[110] Kadar et. al, "Cookie Fines in France in January 2022: Is it the Beginning of a "Cookie Gate"?" February 17, 2022.

Bibliography

Armingaud, Claude-Étienne and Camille Scarparo. "GDPR, Cookies, and the Ever-Filling Jar of European Data Protection." The National Law Review. January 26, 2022.

Azim-Khan, Rafi. "Record €210 Million in Fines for Breach of Cookies and Website Tracking Rules—Note e-Privacy Directive, Not Just GDPR." JD Supra. January 10, 2022.

Bateman, Robert. "French Cookie Compliance 2021 Crackdown." May 9, 2022.

Bateman, Robert. "Cookie Consent Outside the EU." Term Feeds. August 24, 2022.

Carroll, David. "The Cookie Clutter Crumbles: Ad Tech Industry's Consent Framework Isn't GDPR-Compliant." Tech Policy Press. February 2, 2022.

Commission Nationale de L'informatique et des Libertés (CNIL). "Alternatives to Third-Party Cookies: What Consequences Regarding Consent?" (accessed May 24, 2022).

Commission Nationale de L'informatique et des Libertés (CNIL). "Cookies and Other Tracking Devices: the CNIL Publishes New Guidelines." July 23, 2019.

Commission Nationale de L'informatique et des Libertés (CNIL). "Cookies and Other Tracking Devices: the Council of State issues its Decision on the CNIL Guidelines." June 29, 2020.

Commission Nationale de L'informatique et des Libertés (CNIL). "Cookies and Other Tracers: the CNIL Publishes Amending Guidelines and its Recommendation." October 1, 2020.

Commission Nationale de L'informatique et des Libertés (CNIL). "Deliberation of the restricted formation n°SAN-2021-023 of December 31, 2021 concerning the companies Google LLC and Google Ireland Limited." January 6, 2022.

Commission Nationale de L'informatique et des Libertés (CNIL). "Questions and Answers on the Amending Guidelines and the CNIL's "Cookies and other Tracers" Recommendation." May 4, 2022.

Commission Nationale de L'informatique et des Libertés (CNIL). "The Sanctions Issued by CNIL." December 1, 2021.

Commission Nationale de L'informatique et des Libertés (CNIL). Deliberation of the restricted committee no SAN-2020-012 of December 7, 2020 concerning the companies Google LLC and Google Ireland Limited. December 7, 2020.

Commission Nationale de L'informatique et des Libertés (CNIL). Deliberation of the restricted formation no SAN-2020-013 of December 7, 2020 concerning the company Amazon Europe CORE. December 7, 2020.

CookieBot. "Active Consent and the Case of Planet49." January 17, 2022.

Court of Justice of the European Union (CJEU). "Judgment in Case C-673/17." October 1, 2019.

Dearie, KJ. "GDPR Cookies: Consent & Policy Requirements." Termly. October 4, 2021.

Dent, S. "French Regulator Fines Google and Facebook a Combined $238 Million Over Cookie." EnGadget. January 6, 2022.

Duball, Joseph. "CNIL's ePrivacy Fines Reveal Potential Enforcement Trend." IAPP. January 10, 2022.

EU General Data Protection Regulation (GDPR). May 25, 2018.

European Commission. "Proposal for an ePrivacy Regulation." (accessed May 24, 2022).

European Data Protection Board (EDPB). "Opinion 5/2019 on the Interplay between the ePrivacy Directive and the GDPR, in Particular Regarding the Competence, Tasks and Powers of Data Protection Authorities." March 19, 2019.

European Data Protection Board (EDPB). "The CNIL's Restricted Committee Imposes a Financial Penalty of 50 Million Euros against Google LLC." January 19, 2019.

European Data Protection Board (EDPB). "Who We Are," (accessed May 24, 2022).

French Data Protection Act. Unofficial Translation. OneTrust Data Guidance. June 1, 2019.

Galanis, Alexis and Sixtine Crouzet. "France: CNIL Opens Door to Cookie Walls - A Closer Look at the New Criteria." Data Guidance. May 2022.

GDPR.EU website. "Cookies, the GDPR, and the ePrivacy Directive," (accessed May 24, 2022).

Ghebali, Barbara. "Rejecting Cookies Should be as Easy as Accepting Cookies: New Sanctions by the French Authority (CNIL)." February 14, 2022.

GlobalStats. Stats Counter. "Digital Advertising in France," (accessed May 24, 2022).

GlobalStats. Stats Counter. "Search Engine Market Share: France," (accessed May 24, 2022).

Hennel, Christine. "FAQs: What Do I Need to Know about France's Cookie Law Guidelines?" (accessed May 24, 2022).

Hodge, Neil. "France's CNIL Fines Google, Facebook $237M Combined over Cookies Consent." Compliance Week. January 6, 2022.

Hunton Andrews Kurth. "CNIL Fines Google and Amazon 135 Million Euros for Alleged Cookie Violations." December 14, 2020.

International Association of Privacy Professionals (IAPP). "ICO, CNIL, German and Spanish DPA Revised Cookies Guidelines: Convergence and Divergence." August 2019.

Ionos. "EU Cookie Laws and How They Affect your Business." February 16, 2022.

Irwin, Luke. "How the GDPR Affects Cookie Policies." IT Governance. April 12, 2022.

JD Supra. "CNIL Publishes FAQ Clarifying Cookie Use." April 1, 2021.

JD Supra. "France Fines Facebook and Google for Violating the EU Cookie Law: You Need to Make it As Easy to Refuse as a Cookie, as it is to Accept One." January 10, 2022.

JD Supra. "Whether You Like it or Not, Cookies are Back on the Menu and UK and EU Data Protection Authorities are Taking Enforcement Action." July 27, 2021.

Kadar, Daniel, Laetitia Gaillard and Sarah O'Brien Kadar. "Cookie Fines in France in January 2022: Is it the Beginning of a "Cookie Gate"?" Technology Law Dispatch. February 17, 2022.

Kapersky. "What are Cookies?" (accessed May 24, 2022).

Kemp, Simon. "Digital 2022: France." February 9, 2022.

Koch, Nathalie and Thanos Rammos. "Cookies Under Attack – New Decisions by European Data Protection Authorities on Online Advertising," Taylor Wessing. February 11, 2022.

Lanois, Paul. "France's CNIL Issues Guidance on the Issue of Cookie Walls." California Lawyers Association (accessed September 8, 2022).

Lomas, Natasha. "Targeted Ads Offer Little Extra Value for Online Publishers, Study Suggests," May 31, 2019.

Manancourt, Vincent and Laura Kayali. "France Flexes Muscles with Fines against Facebook, Google over Cookie Banners." Politico. January 6, 2022.

Office of the U.S. Trade Representative, "Key Digital Trade Barriers," (accessed October 6, 2022).

Pollet, Mathieu. "Cookies: French Data Protection Watchdog Welcomes Increased Compliance." EurActiv. September 14, 2021.

Privacy Policies. "Ultimate Guide to EU Cookie Laws." November 15, 2021.

Research and Markets. "Global Digital Advertising and Marketing Market Report 2021." November 22, 2021.

Statista. "Digital Advertising in France," (accessed May 24, 2022).

Statista. "Online Advertising Revenue in the United States from 2000 to 2021," (accessed September 6, 2022).

Statista. "Social Media Usage in France," (accessed May 24, 2022)

Trevisan, Martino & Traverso, Stefano & Bassi, Eleonora & Mellia, Marco. "4 Years of EU Cookie Law: Results and Lessons Learned." Proceedings on Privacy Enhancing Technologies. 2019.

Vibbert, Jami, Alexander Roussanov Nancy L. Perkins Eftychia Sideri. "Data Protection in France: Publication of Amended Guidelines and Recommendations on Cookies and Other Online Trackers." Arnold and Porter. October 27, 2020.