THE JBBA

PEER REVIEWED RESEARCH

OPEN ACCESS
ISSN Online: 2516-3957
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-3-2-(1)2020

Browser-based Crypto Mining and EU Data Protection and Privacy Law: A Critical Assessment and Possible Opportunities for the Monetisation of Web Services

Christopher F. Mondschein
European Centre on Privacy and Cybersecurity (ECPC), Maastricht University, The Netherlands

Correspondence: c.mondschein@maastrichtuniversity.nl
Received: 17 March 2020 **Accepted:** 24 March 2020 **Published:** 12 April 2020

Abstract
Recently, browser-based crypto mining (or browser mining) received attention in academic literature, mainly from the work in the field of computer science. Browser-based crypto mining describes the act of websites or other actors mining cryptocurrencies for their own gain on client-side user hardware, which mainly takes place by mining Monero through Coinhive or similar codebases. Although the practice gained infamy through the various ways in which it was illicitly deployed, browser mining has the potential to act as an alternative means for the monetization of web services and digital content. A number of studies explored browser mining for monetization purposes and highlighted its short-comings compared to the traditional advertisement-based monetisation strategies. This paper discusses the practice in light of EU data protection and privacy law, notably the General Data Protection Regulation (GDPR) and the ePrivacy Directive (ePD), which is currently being overhauled and aligned with the GDPR. It adds to the discussion surrounding the feasibility of browser mining as a potential alternative for monetization by exploring the legality of browser mining in relation to EU data protection and privacy law and by identifying possible benefits regarding the protection of individuals' personal data and privacy by deploying browser mining. It is argued that employing browser mining in a transparent and legitimate manner may be an additional option to financing websites and online services due to the growing legal pressure on advertisement models such as programmatic advertisements that rely on the exploitation of large amounts of personal data and ad networks.

Keywords: *Cryptocurrency; Mining, Blockchain, GDPR, ePrivacy, Privacy and Data Protection, EU Fundamental Rights*
JEL Classifications: *K24, K42*

1. Introduction

The monetization of web services mainly relies on the advertising revenue, with a large part of the revenue stemming from programmatic advertising and behavioural targeting, with an estimated €16.8 billion market share in Europe [1]. Programmatic advertising entails the mostly automated buying, selling and matching of digital advertising spaces and advertisers over a number of platforms and aggregators, in order to display relevant ads to consumers browsing the web. The buying and selling of an ad space is automated and happens through real-time bidding (RTB) auctions within milliseconds. The ads are then displayed to users based on the users' deduced preferences that are established over the course of being tracked and profiled based on their behaviour while surfing multiple websites [2].
Online advertising, especially programmatic advertising, is criticized for its impact on individuals' privacy and the protection of their personal data for a number of reasons: these include the large quantities of personal data collected and processed, including sensitive personal data (such as sexual orientation, health data, religious belief and so on), and the general lack of awareness that the users have of these practices. Further, the practice also entails the automated sharing of personal data with many entities at high velocity, leading to the risk of data getting leaked which cannot be accounted for, thus breaching the principles of EU data protection law [3]. In this context, we also see that access to a website is often made conditional upon the acceptance of tracking and advertising (so-called tracking walls), affecting the legality of the consent collected under these practices [4].
Hence, browser-based crypto mining (or browser mining) was envisioned as an alternative to the tracking and targeting practice that is dominating online advertising [5]. Browser mining entails websites or other actors injecting mining code into client-side hardware in order to mine cryptocurrencies using those devices' computational power, thereby converting end-user devices' computational power into cryptocurrencies for the benefit of the entities deploying the mining code. Although being conceived as an alternative to online advertising, browser-based crypto mining (or browser mining) mostly garnered public attention due to scandals that revolved

around its illicit use, especially during the period of 2017–2018.

Browser mining also drew the attention of academics in the field of computer science and information security studies, who mainly focused on identifying the prevalence and spread of crypto mining and its detection [6] as well as on its feasibility for monetizing web services compared to the traditional online advertising models [7]. While a large part of the the body of research touches upon browser minings' privacy and data protection implications [8], none has yet comprehensively addressed these issues. This paper discusses the practice of browser-based crypto mining in light of EU data protection and privacy law, focusing on the General Data Protection Regulation (GDPR) [9], the ePrivacy Directive (ePD) [10] and the proposal for an ePrivacy Regulation (ePR) [11]. In doing so, the paper explores the legality of browser mining in relation to EU data protection and privacy law and identifies possible benefits regarding the protection of individuals' personal data and privacy by deploying browser mining over traditional online advertisement strategies.

The paper is structured as follows: Section 1 introduces the topic and frames the discussion. Section 2 presents a short history of browser mining, describes the practice and illustrates deployment methods of browser mining. Section 3 analyses browser mining in light of EU privacy and data protection law. Section 4 identifies possible benefits that browser mining has over online advertising practices that utilize personal data and assess what measures could be taken within the current EU privacy and data protection framework to accommodate browser mining. It further adds an outlook on where the legal framework may warrant for amendment, specifically addressing the proposal for an ePR.

1. Browser mining

a. A brief history of browser mining

The emergence of the idea of browser-based crypto mining as an alternative to finance web services dates back to 2013–2014, with an example of the MIT-based student project Tidbit. As a project, Tidbit was the product of a hackathon and was conceived with the purpose of offering an alternative to online advertising [12]. The project came under legal scrutiny soon after, leading to proceedings in New Jersey, due to Tidbit being viewed as malware and having the potential to afflict serious harm to consumers as they 'may have their computers "co-opted" or "hijacked" without their consent by unscrupulous website operators using the Tidbit code' [13]. This assessment foreshadowed the malicious applications of browser mining that would become prevalent, and the case led to the shutting down of Tidbit due to the mounting legal pressure. Yet in an interesting statement in the proceedings, the Superior Court of New Jersey acknowledged the need for openness towards innovative technological solutions, stating that

> this investigation, may be acting to discourage creative and 'cutting edge' new technology. (…) it appears that the Tidbit program and other similar creative endeavors serve a useful and legitimate purpose. There is nothing presented to the Court that evidences an inherently improper or malicious intent or design by Plaintiff. Rather, Tidbit appears to be an instrumentality or tool that has great potential for positive utility. The Court is mindful, however, of the State's concerns that this tool could also be subject to abuse and misuse [14].

During the period of 2017–2018, scandals and news surrounding browser mining were abundant and saw a peak. The file-sharing website The Pirate Bay experimented with running mining code on its website in 2017 in order to monetize its service [15]. In 2018, the crypto mining code was illicitly injected into various websites, including the UK's data protection supervisory authority, the Information Commissioner's Office (ICO) [16], among many others, which mined cryptocurrencies through visitors' web browsers for the duration of their visit [17]. The US television giant CBS had mining code injected into its Showtime web-streaming service, which mined Monero in users' browsers, although it is unclear who was responsible for deploying it [18]. Crypto mining code was also deployed by a rogue employee of the E-Sports Entertainment Association (ESEA), leading to 14,000 devices being affected, which resulted in legal actions in New Jersey and California [19]. Further incidents involve the running of mining code in ad networks, Youtube ads, browser extensions, routers, Android mobile devices, fundraising campaigns by UNICEF and gaming mods, with numerous examples existing [20]. These scandals led to a negative perception of browser mining, with it being described as 'cryptojacking,' 'thieves in the browser' [21], and is widely being framed as a security issue.

With the demise of Coinhive in 2019, the browser mining landscape is in turmoil. However, security experts believe that the practice will prevail and surmise that it will also see a resurgence with the growth of (unsecured) IoT devices that could be exploited for the mining of cryptocurrencies [22].

b. A basic explanation of browser mining

'Mining' is one of the cornerstones of the functioning of blockchain-based cryptocurrencies. A number of cryptocurrencies rely on the so-called Proof-of-Work (PoW) distributed consensus algorithm in order to operate [23]. PoW requires participants in the cryptocurrency's network to solve cryptographical puzzles in order to validate transactions in the network, which is called 'mining.' Miners are rewarded, for solving cryptographical puzzles, a unit of cryptocurrency specified in the cryptocurrency's protocol [24]. The act of mining cryptocurrency was conceived as a way of sustaining a distributed network, and such a distribution functions as a means to prevent any party in the network from dominating it by owning 51% or more of the network's computational capacity, underlining the importance of a good distribution of mining power among devices and parties in the network [25].

As such, the idea of utilizing end-user devices to mine cryptocurrencies is not new and even follows the goal of a wide distribution of mining among devices in those networks. In this regard, a large number of mining services exist in the form of websites or apps that allow individuals to mine

cryptocurrencies using their personal devices such as computers, laptops, smartphones and so on, without being required to run a full node of the cryptocurrency's network [26]. Similarly, the idea of individuals being able to donate or lend computational power to specific causes has already seen many applications, with numerous applications for science [27]. Both of these approaches culminate in browser mining, as the mining of cryptocurrencies takes place in the end-user's device but the benefits (that is, the cryptocurrency that is mined) are received by the entity deploying the mining code.

The most popular codebase for browser mining is Coinhive [28], which mines the cryptocurrency Monero, but numerous similar codebases exist (for example, Crypto-Loot, CoinImp, Minr, deepMiner, JSECoin and Coinhave) [29]. Mining applications such as Coinhive usually take a percentage of any mined cryptocurrencies, for instance, Coinhive took a 30% cut, whereas Crypto-Loot took 12% [30]. At the height of its operation, it is estimated that the Coinhive codebase was deployed on 0.08% of 137 million .com/.net/.org sites and the Alexa Top 1M domains were inspected, resulting in the mining of 1.18% of all blocks of the Monero cryptocurrency as of mid-2018 [31]. Coinhive ceased its operations in March 2019, due to the diminishing returns it created as a result of the drop in prices of cryptocurrencies, which also affected the value of Monero and legal concerns surrounding the practice [32].

The prevalent cryptocurrency that is mined via browser mining is Monero, as it is a cryptocurrency that focuses on ASIC (application specific integrated circuits) resistance and privacy; however, a number of other cryptocurrencies are also frequently mined through browser-based crypto mining, including Ethereum, Zcash, LiteCoin, Dash and others, with some applications utilizing third-party mining libraries that allow for the mining of multiple cryptocurrencies. The prevalence of Monero in this context is based on developments visible in a number of cryptocurrency protocols, aiming to ensure that the effectiveness of specialized mining equipment (ASIC) is diminished in order to prevent parties from controlling too large a degree of a network's computational power. Therefore, Monero is one of the cryptocurrencies that is attractive to mine in end-user devices, and it is also the cryptocurrency most often mined in browsers, whereas mining Bitcoin via non-specialized equipment has become unprofitable.

c. The deployment of browser mining

It is important to highlight some deployment methods of browser mining in order to distinguish between outright malicious deployment methods and methods that could be legitimate, in order to inform the legal discussion in Section 3.

The most common form of deployment works by integrating a miner API into a website. This is the prevalent way to deploy Coinhive and several browser mining clones. These APIs offer a mining library which can easily be deployed on a website, which runs the miner via JavaScript or WebAssembly client-side. Website providers merely need to add a snippet of the code to their website and configure their cryptocurrency wallet in order to run Coinhive or similar miners, making deployment rather easy. Once deployed, the script is loaded client-side and executes the link when the page is loaded and launches the miner in a user's browser, with the miner being loaded from a third-party website for most mining APIs (for example, Coinhive and Crypto-Loot). Some miners are self-hosted by the website provider, bypassing the reliance on third-party websites (for example, DeepMiner) [33]. Next to the deployment described above, Coinhive also offered a number of other ways to deploy its mining code:

- Shortlink service: shortens a URL for easier forwarding;
- In-game mining for games;
- CAPTCHA, which is a test to determine whether a user is a person or a bot (Figure 1) [34].

Figure 1. Coinhive CAPTCHA

Coinhive also developed an SDK for Android app developers, facilitating the mining integration for mobile applications [35].

Regarding the transparency of the deployment of crypto mining, browser-based crypto miners such as Coinhive can usually be detected – and subsequently blocked – rather easily, based on the identification of links to the mining websites that are integrated in scripts deployed by the websites running the API, with some APIs presenting the ability for obfuscation as a selling point [36]. However, the obfuscation of links has led to more sophisticated methods of detection being researched that go beyond the establishment of blocking lists of known miner links found in scripts (blacklisting) [37]. In this regard, self-hosted miners allow for stronger obfuscation. It is noted for self-hosted miners that '[u]ltimately, this is more flexible for attackers. It also helps them avoid blacklists by using their own domains (changing it whenever they need) for the client script and the websocket proxy' [38].

Next to the obfuscation of the miner scripts, the transparency and awareness of users within the user interface is also an important issue. Some miners such as Crypto-Loot advertise themselves as stealthy and promise that users will not be able to identify whether a website has deployed the miner [39]. In addition, the so-called persistent drive-by crypto mining is another technique to deploy browser mining without user awareness. It is used by deploying the same browser-based mining script found in the Coinhive API or similar APIs, but this time, the user enters a website which runs a script to open a new browser window that runs the miner. This browser window is opened as a so-called pop-under (as opposed to a pop-up), and it is placed behind the desktop's taskbar, masking its presence. Users only see that the browser is open by virtue of the desktop icon but do not see how many different windows are open. Once they close all windows, the mining also ceases [40]. Arguably, these practices contribute to the perception of the practice as illicit or dodgy and, as is argued below, are also illegal in view of EU privacy and data protection law.

On the other hand, within the Coinhive family of products, the Authedmine API was developed with the aim of

facilitating the provision of information to users and the collection of consent for mining. It was developed to counter the illicit appearance of Coinhive and added an information notice and a consent option (see Figure 2). The miner is only engaged when users click the button in the pop-up. Similar configurations of Authedmine were deployed, for instance, in campaigns by UNICEF Australia and CPUforGood, in order to collect donations for good causes via browser mining [41].

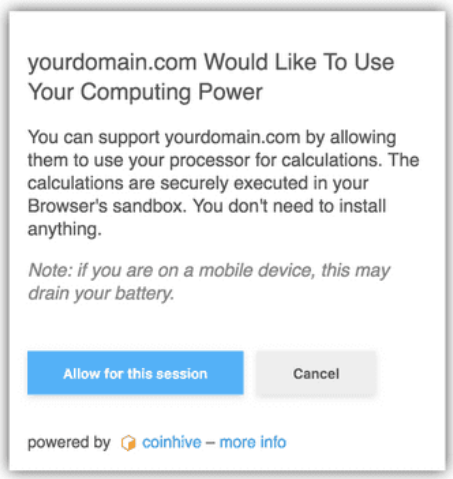

Figure 2. Authedmine notice example

d. Intermediate conclusion

Browser mining can be deployed in a number of different ways. APIs can be self-hosted or run scripts that link to third-party websites. Here, transparency and user awareness are issues with regard to the deployment of browser-based crypto miners. The mode of deployment and the intent of those entities deploying miners have to be taken into account, along with the actual deployment. Obfuscation arguably contributes to the perception of the practice as illicit or dodgy and as we will see, it also is illegal in the context of EU privacy and data protection law. The obfuscation of links in the script seems particularly questionable as this is used solely for the prevention of detection. The same holds true for persistent drive-by crypto mining. Conversely, solutions such as Authedmine strive for transparency and give the user an option to consent. These examples illustrate the broad range in which the technology can be utilized.

2. Browser mining in the light of EU privacy and data protection law

In order to establish the legality and the compatibility of browser mining in the light of EU privacy and data protection law, it is necessary to assess whether browser mining falls within the scope of the instruments in question, in particular the GDPR, the ePD and the proposal for an ePR.

Within the legal framework of the EU, a distinction is made between the fundamental right to privacy and the right of data protection. At the level of primary EU law, the former is enshrined in Article 7 of the Charter of Fundamental Rights of the EU (the Charter), whereas the right to data protection is explicated in Article 8 of the Charter and in Article 16 of the Treaty on the Functioning of the EU (TFEU). Article 16(2) TFEU provides a legal basis for the EU to adopt a secondary legislation on the protection of personal data [42]. The conceptualization of these two fundamental rights as separate rights and the relation between the rights are still subject to academic deliberation [43].

The EU is competent to adopt legislation in the field of data protection as well as in the scope of the functioning of the internal market. The EU also adopted legislation regarding the privacy of publicly available telecommunication networks and services in the form of the ePD, dating back to 2002. The ePD was updated in 2009 by the so-called Citizens' Rights Directive in order to regulate and clarify its applicability with respect to web tracking technologies such as cookies [44]. The EU adopted legislation in the field of data protection by virtue of the GDPR, which was adopted on the basis of Article 16(2) of TFEU, which replaced the Data Protection Directive (DPD) adopted in 1995. With the GDPR entering into force on 25 May 2018 [45], the EU started the reform process for the modernization of its data protection framework.

Within this reform effort, it was planned to have the revised ePR enter into force at the same time as the GDPR. One of the reasons to modernize the ePrivacy Framework was that, among Member States, the ePD was implemented in a variety of ways that undermined the protection of end-user devices due to the dilution of the provisions on tracking [46]. To remedy this, the European Commission published a proposal for the ePR in January 2017 [47]. However, the Council failed to reach a political agreement during this time, leading up to the failure of the proposal in the Council on 3 December 2019. During the Council's Telecomm Group on that day, the newly designated commissioner, Thierry Breton announced, a plan to withdraw and re-table the proposal, with the future of the ePR left unclear [48].

a. The GDPR and the ePrivacy Framework

The GDPR applies to fully or partially automated processing of personal data or processing of personal data using a filing system and applies to entities established in the territory of the EU/EEA which processes such data, as well as entities that are established outside of the EU but process data by either marketing goods or services in the EU or by tracking individuals located in the EU [49]. The scope of what constitutes personal data under the GDPR is wide and includes, for instance, dynamic IP addresses [50} and trackers and identifiers such as cookies [51].

The ePD protects individuals' privacy of telecommunication and applies 'to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community, including public communications networks supporting data collection and identification devices [52].' The ePD further holds specific provisions regarding the privacy of end-user devices in Article 5(3):

> Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that

> the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.

The provision makes the storing of information or the accessing or reading out of information stored in end-user devices conditional upon the user giving his or her consent after receiving clear and comprehensive information, with the exception of purely technical operations.

The provisions of the ePD form *lex specialis* to those of the GDPR, with a number of provisions of the Directive particularizing those of the GDPR and others complementing the provisions found in the GDPR [53]. After the GDPR replaced the 1995 DPD [54], references to provisions in the DPD found in the ePD had to be replaced with references to the GDPR [55]. This was previously established in a number of opinions of advisory bodies and was confirmed in the case law of the Court of Justice of the European Union (CJEU) [56].

b. The GDPR, the ePrivacy Framework and browser mining

1. *The application of the GDPR*

Regarding the applicability of the GDPR to browser mining, it is necessary to assess whether browser mining entails the processing of personal data. The operations of a website may entail a number of different processes that fall within the material scope of the GDPR as personal data is processed: these can include audience measurement, tracking of users for monetization purposes, ensuring the security of the website against cyberattacks and so on [57]. When comparing these operations to the running of a script in the end-user's device, it is difficult to establish that browser mining entails the processing of personal data. In this regard, the aforementioned processing operations have to be seen as separate operations with their own purpose, with personal data collected and processed, and require separate legal bases [58].

From a technical perspective, it therefore becomes doubtful whether the GDPR applies to browser mining, as the material scope of processing of personal data does not seem to be triggered.

Nevertheless, if this were the case and the GDPR were to apply, the full set of compliance obligations would come into effect. This would create a number of difficulties in the context of browser mining, as the GDPR does not sit well with blockchain applications [59]. One of the key issues to resolve are, on the one hand, the designation of controller(s) and processor(s) in order to attribute the obligations arising from the GDPR, and on the other hand, the designation of data subjects, who derive rights from the GDPR. A problem arises as roles can conflate in the context of blockchain applications: on the one hand, the end-user whose device is used to mine cryptocurrencies would become a data subject, whereas the end-user also mines cryptocurrencies for the benefit of the website operator, thereby potentially becoming a data processor [60].“In this situation it becomes problematic when considering whether personal data (that is, the transactional data) is processed by third parties (that is, the miners) in this situation, especially when dealing with privacy-focused cryptocurrencies such as Monero [61]. An orthodox reading of the GDPR would result in accepting the privacy-preserving measures of such cryptocurrencies merely as additional measures to secure personal data; however, the GDPR would still apply in full. This would also align with the fundamental rights logic of the GDPR that aims at securing the protection also for new technological developments. On the other hand, the development of new protocols such as CryptoNote [62] and its derivatives (such as CryptoNight, used for the Monero cryptocurrency) asserts pressure on the client-server paradigm that underlies the GDPR's regulatory structure.

In sum, it is rather doubtful whether browser mining falls within the material scope of the GDPR; however, if the GDPR applies, compliance becomes difficult.

2. *The application of the ePD*

Conversely, Article 5(3) ePD is applicable in the context of browser mining. Article 5(3) is one of the provisions that particularizes the GDPR [63]. The provision has a wider material scope than personal data and applies to any information, including non-personal data [64]. The rationale behind this is the guarantee of an effective protection of end-user devices' privacy in light of technological developments. Indeed, the scope of Article 5(3) ePD was clarified on numerous occasions and the provision was adapted by the Citizen's Rights Directive in 2009 in order to accommodate new technological developments [65]. These changes were guided by the legislator's and the regulators' will to ensure a technologically neutral approach that allows for the application of the provision to technological developments such as cookies, browser fingerprinting and similar technologies [66]. The extension of protection under Article 5(3) ePD, regardless of whether the processing of personal data takes place, was also affirmed by the CJEU stating that the 'provision aims to protect the user from interference with his or her private sphere, regardless of whether or not that interference involves personal data' [67]. Further, the CJEU opined 'that protection applies to any information stored in such terminal equipment, regardless of whether or not it is personal data, and is intended, in particular, as is clear from that recital [Recital 24 ePD], to protect users from the risk that hidden identifiers and other similar devices enter those users' terminal equipment without their knowledge' [68].

The scope of protection offered by Article 5(3) ePD also extends to forms of interactions with end-user devices that differ from tracking based on cookies or device fingerprinting. It has to be questioned whether browser mining falls into the scope of this provision since the method does not intend to track users but makes use of a device's computational power for the duration of the visit to a website.

In this regard, other forms of intrusion in end-user devices have been deemed to fall within the scope of Article 5(3) ePD, as is illustrated by the *Sony-MediaMax* case [69]. The automatic and unobtrusive installation of content rights management software deployed when playing media stored on CDs, CD-ROMs, and USB keys was deemed an unlawful intrusion, contravening Article 5(3) ePD [70]. The use of spyware or other intrusive means to access end-user devices was brought into the scope of the ePD [71]. Further, in the guidance issued by the Dutch data protection supervisory authority, it is also stated that 'the prohibition of cookiewalls is not restricted to the setting of cookies. Not only cookies are covered by this description, but also similar technical solutions that require consent fall within the scope. These are technical solutions such as *JavaScript*, Flash cookies, HTML5-local storage and/or web beacons' [72]. Following these developments, the application of Article 5(3) ePD to browser mining seems logical, as running scripts in end-user devices would require valid consent.

Yet this conclusion still highlights the uneasy relation between browser mining as a new technological development and the legal framework at issue. Similar to earlier developments in tracking technologies, the legal framework is pushed to its boundaries due to these new developments, as witnessed with cookies, device fingerprinting and the *Sony-MediaMax* debate. With regard to browser mining, the complexities surrounding the interplay between the GDPR and the ePD are highlighted once more: the fact that this interplay largely hinges on the processing of personal data and that a form of monetization of web services devoid of any interest in the person behind the device was not envisioned by the legislator creates legal uncertainty regarding the application of the law to browser mining. However, given the *telos* of the provision – the protection of fundamental rights and especially the protection of individuals' sphere of privacy with regard to their devices – it is likely that browser mining falls within the scope of Article 5(3) ePD.

3. *Application under proposal for the ePR*

According to Article 8(1) of the proposed ePR, '[t]he *use of processing and storage capabilities* of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware, other than by the end-user concerned' is conditional either upon the end-user's consent, technical necessity in the context of electronic communications, the provision of an information society service explicitly requested by the user or for audience measurement, provided that such measurement is carried out by the provider of the information society service requested by the end-user (emphasis added). The proposed Regulation continues the wide definitional approach of its predecessor and clarifies that the use of processing and storage abilities falls within the ambit of its provisions. Hence, from the wording of Article 8(1) ePR, it can be deduced that browser mining would fall within the scope of the ePR.

c. Compliance under the ePrivacy Framework

It is unlikely that browser mining falls within the scope of the GDPR, however, it likely falls within the ambit of Article 5(3) ePD, and the wording of Article 8(1) ePR similarly applies to browser mining. This means that any operator deploying a miner must do so in a compliant manner.

Article 5(3) ePD makes the valid deployment of a miner conditional upon prior notification of the user and collection of the user's consent prior to running the mining script on their device. Even in the event of personal data being processed, the entity deploying the miner would be bound to consent as a legal basis as opposed to a choice of legal basis under Article 6 GDPR, as the provision of the Directive applies according to the *lex specialis* rule.[73] Further, the technical exemptions envisioned in Article 5(3) ePD, second sentence have to be construed narrowly and are not applicable to browser mining.

Similarly, Articles 8 and 9 ePR would apply, mandating prior informed consent with reference to Articles 4(11) and 7 GDPR by virtue of Article 9 ePR.

In assessing these requirements, it is clear that the obfuscated deployment of a miner contravenes the provisions of both the ePD and the ePR and must therefore be deemed illegal. Regarding the various forms of deployment such as a CAPTCHA or a shortlink service, the same requirements apply as with browser-based mining, requiring the provision of information and the prior collection of user consent.

1. *The provision of information*

Article 5(3) ePD states that users should be provided with 'clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing.' The provision contains similar requirements to former Article 10 DPD [74], which is now replaced by Article 13 GDPR. The information in that provision relates, inter alia, to the identification of relevant actors (controller(s), processor(s), third parties who receive personal data), the purposes and legal bases related to the processing, the rights of data subjects, the existence of data transfers to non-EU/EEA states and the modalities of such transfers and the existence of automated decision-making. In the context of browser mining, this information may not be relevant or might not even exist as there is arguably no processing of personal data. It therefore needs to be questioned what information should be provided. Given that the ambit of Article 5(3) ePD extends beyond the scope of personal data, even when there is no processing of personal data involved, there must be meaningful information for users [75]. The Authedmine user interface offers some general information on the use and also a warning of the potential battery drainage (see Figure 2). The website is indicated as the entity deploying the miner and the purpose is explained. Here, any third party should also be named. The legal obligation here is uncertain and it has to be questioned if such information is 'meaningful.' In sum, the exact information requirements for browser mining are not clearly laid out in the law, and the burden is put on the entity deploying the miner to ensure that the information is clear and comprehensive and that at least the purpose and the entities involved are named as the validity of consent hinges upon this. Again, the probable lack of awareness of the practice becomes apparent as it seems at odds with the regulatory mechanism in the provision.

This also holds true for the provision on the information requirements in the ePR: Article 8(1)(b) mandates the collection of consent and Article 9 links the modalities and the validity of consent to those set out in the GDPR in Articles 4(11) and 7. This means that consent must be 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her' (Article 4(11) GDPR). Given that the validity of the consent is tied to it being, inter alia, informed, it can be deduced that users are required to receive sufficient information. However, also in the case of the ePR, the scope of the information required, its format and its modalities are not clear in the context of browser mining. In this situation, the tension arises as the ePR would apply but the GDPR would not, something that has not been fully accounted for in the ePR and an issue that the ePR does not rectify [76].

2. *Consent for browser mining*

The legal uncertainty surrounding browser mining regarding the consent requirement under the ePD and ePR is even more striking: under the ePD, consent must be collected prior to the deployment of the miner. The CJEU clarified the conditions for consent in *Planet49*, linking the requirements under Article 5(3) ePD with those of the DPD and GDPR, stating that consent must be freely given, specific, informed and an unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her [77].

A similar construction is found in the ePR as Article 9 clarifies that consent has to be construed within the meaning of the GDPR.

In this regard, Article 7(1) GDPR explicates: 'Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.' Hence, the logic of shifting the burden to prove compliance with the lawful collection of consent for the controller seems logical when personal data is processed and such data needs to be protected under the principle of accountability. Here, a connection between the data and the data subject exists for the duration of the existence of the data, which extends beyond the phase of collection. This begs the question of how and whether this provision applies with regard to browser mining, which arguably does not entail the processing of personal data.

Here, it can be argued that browser mining only connects a user to the entity deploying the miner during the time of mining, i.e. when the user vists the website and the script runs. Thus, the point of connection between a user and a website operator is effectively severed once the mining script stops running and the transaction of computing power for cryptocurrency has ceased and no personal data is processed for the mining. The logic behind the ongoing protection of personal data and the placing of the burden of proof on the entities handling personal data rests on the fact that the processing of personal data poses an ongoing risk to the data subject for the time the data exists, i.e. longer than the mere visiting of a website.

In applying the provision to browser mining, the creation of a consent trail would necessitate the processing of personal data in order to record the consent of the user at a specific time in connection to a notification that was provided in order to comply with Article 7(1) GDPR, which becomes applicable in this situation by reference under the ePrivacy Framework. Essentially, this means that in order to prove valid consent for browser mining – a process intended to replace the need for the processing of personal data – personal data would have to be processed so that the entity deploying the miner can prove it collected lawful consent. At face value, this seems somewhat absurd, however, the alternative would mean that no valid proof would be established whenever utilizing browser mining. Even if the user is informed and his or her consent was collected in a valid way, there would be no proof of this.

From the viewpoint of protecting the privacy and integrity of an end-user device, the lack of proof of intrusion in such a device would also require the collection of consent in a demonstrable fashion. Here, it would be beneficial for the legislator to add clarity by introducing self-standing provisions in the ePR that explicate similar principles as the GDPR, something that a number of scholars have suggested [78].

3. The benefits of browser mining

In the discussion surrounding the monetization of web services, previous research on browser mining has shown it to be largely a lacklustre replacement for programmatic advertisement from a financial perspective [79]. Further, the practice is also subject to the volatility of the cryptocurrencies mined [80]. The major question that arises when comparing browser mining as a monetization strategy with other forms of monetization is what the privacy impact on users is. In this respect, browser mining would indeed be beneficial to users in case it is deployed as an *alternative* to monetization strategies that rely on the processing of personal data, such as programmatic advertising. However, other forms of online advertising, such as contextual advertising, offer a similarly privacy-friendly solution [81]. The context of deployment is important in gauging the profitability of these means: contextual advertising relies on the finding of relevance to a website/the context in which advertising is shown, thereby detaching the selection of advertisement from the individual and relying on the broader context to establish the meaning for advertising. Where such a context can be deduced, contextual advertising becomes attractive, albeit it is still being questioned on how well it performs against programmatic advertisements [82]. Where such a context cannot be deduced, such as on general news sites or web services that do not offer a stream-lined contextual setting, the personalization of advertising becomes necessary. Here, browser mining poses an interesting alternative. For the profitability of browser mining, the duration of a user visiting a website is also decisive [83].

A further consideration is the use of personal data and users' perception of such practices in relation to website monetization. Research has shown that users seem to be

reluctant in accepting tracking and profiling practices [84] and would prefer browser mining [85]. This information has to be taken with a grain of salt, as research on self-reporting on privacy and data protection matters shows that many users lack a basic understanding of the intricacies and the trade-offs they are engaging with [86]. Nevertheless, browser mining could be viewed as a privacy-friendly alternative. However, this is conditional on it being applied as an *alternative*. It would therefore be undesirable to apply browser mining as an additional source of revenue next to programmatic advertisement.

This also plays into the current debate surrounding tracking walls. Tracking walls force users to consent to tracking for monetization purposes and make such consent the condition for accessing a website or web service [87]. In essence, the practice creates a zero-sum game between users, on the one hand, and websites and third-party providers, on the other hand: either the user preserves their privacy and the website operator and the related third parties do not receive any revenue or the user loses his privacy so the operator and the related third parties can make a profit.

Throughout the existence of both the ePD and the proposed ePR, tracking walls have been a persistent point of disagreement among Member States. The 2009 Citizen's Rights Directive did not lead to a uniform interpretation of Article 5(3) ePD [88], and the disagreement among Member States in the Council led to the failure of the ePR in its current state. The validity of consent collected via tracking walls has been challenged, along with other issues surrounding non-compliance in programmatic advertisement, with data protection supervisory authorities in some EU Member States prohibiting tracking walls [89]. In its *Planet49* judgement, the CJEU clarified the conditions for consent under Article 5(3) ePD, yet it availed itself from taking a stance in the dispute surrounding tracking walls [90]. Advocate General Szpunar however stated in his opinion that the 'selling' of personal data and the processing of personal data for the purpose of monetizing a service could be a condition for access to such service [91]. This hints at an acceptance of the conditionality of providing personal data for 'free' services (in that case, participation to a lottery), a view that opposes the opinions and guidance by a number of data protection supervisory authorities outlined above.

Here, browser mining might help by softening the adversarial nature that exists between users wanting to protect their personal data and privacy and website operators wishing to monetize their services by offering a means to preserve user privacy while at least creating some revenue for website operators. In this regard, the current uncertainty surrounding the status of the proposal might allow for a reconsideration.

Regarding tracking walls in the ePR, Zuiderveen Borgesius et al. illustrate a number of measures the legislator could take [92]. They note that a full or partial ban of tracking walls can take place and make a compelling argument for at least a partial ban for circumstances including 'public service media, commercial media, professions with specific confidentiality rules, and the public sector' [93]. In these circumstances, they propose a blacklist, along with a grey list:

> If a situation is on the grey list, there is a legal presumption that a tracking wall makes consent involuntary, and therefore invalid. Hence, the legal presumption of the grey list shifts the burden of proof. For situations on the grey list, it is up to the company employing the tracking wall to prove that people can give 'freely given' consent, even though the company installed a tracking wall [94].

If one were to accept that a total ban on tracking walls is not a realistic option, given the political disagreement and legal uncertainty, a compromise next to the one proposed above could be that tracking walls may be accepted in limited circumstances where one of the options provided as an alternative to the processing of personal data is to allow browser mining.

The law would have to clarify that this would be an alternative and may not be used in conjunction with tracking. Further, the same transparency and consent modalities would need to be applied. Regarding the collection of consent, the collection of personal data for this purpose should be legitimized and the scope of the information provision should be clarified, mirroring the spirit of the GDPR but contextualized for sitatuions in which no personal data is processed. Lastly, the competence of the supervisory authorities should also be clarified with regard to the enforcement of infringements of the provisions pertaining to browser mining [95].

Competing Interests:
None declared.

Ethical approval:
Not applicable.

Author's contribution:
Christopher F. Mondschein designed and coordinated this research and prepared the manuscript in entirety.

Funding:
None declared.

Acknowledgements:
I would like to thank the anonymous reviewers.

References:

[1] IAB Europe, 'IAB Europe European Programmatic Ad Spent Report 2018', *IAB Europe* (2019), https://iabeurope.eu/wp-content/uploads/2019/09/IAB-Europe_European-Programmatic-Ad-Spend-2018-Report_Sept-2019.pdf.

[2] ICO, 'Update report into adtech and real time bidding', ICO (2019), https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf, p. 8-9 and footnote 4.

[3] See for example Lynskey, O., 'Track[ing] changes: an examination of EU Regulation of online behavioural advertising through a data protection lens', 36 *European Law Review* (2011); Zuiderveen Borgesius, F.J., *Improving privacy protection in the area of behavioural advertising* (PhD Thesis, UV Amsterdam, 2014); Clifford, D., 'EU Data Protection Law and Targeted Advertising – Consent and the Cookie Monster – Tracking the crumbs of online user behaviour', 5 *Journal of Intellectual Property, Information Technology and E-Commerce Law* (2014); Markou, C., 'Behavioural Advertising and the "New Cookie Law" as a Victim of Business Resistance and a Lack of Official Determination', in S. Gutwirth, R. Leenes and P. de Hert (eds.), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection* (Springer, 2016). Also, Opinion 2/2010 of the Article 29 Working Party on online behavioural advertising, 22.6.2010, WP 171; Opinion 04/2012 of the Article 29 Working Party on Cookie Consent Exemption, 7.6.2012, WP 194; Opinion 9/2014 of the Article 29 Working Party on the application of Directive 2002/58/EC to device fingerprinting, 25.11.2014, WP 224.

[4] See R.E. Leenes and E. Kosta, 'Taming the Cookie Monster with Dutch Law – A Tale of Regulatory Failure', 31 *Computer Law and Security Review* (2015); F.J. Zuiderveen Borgesius et al., 'Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation', 3 *European Data Protection Law Review* (2017).

[5] See ENISA, 'Cryptojacking – Cryptomining in the browser', ENISA (2017), https://www.enisa.europa.eu/publications/info-notes/cryptojacking-cryptomining-in-the-browser. The idea goes as far back as 2013/2014, with BitCoinPlus.com and the MIT-based project called 'Tidbit.' See Securitytrails, 'How much cryptocurrency can a web cryptominer actually mine?', *SecurityTrails* (2018), https://securitytrails.com/blog/how-much-cryptocurrency-can-a-cryptominer-actually-mine#a-little-on-the-history-of-browser-mining.

[6] S. Eskandari et al., 'A first look at browser-based Cryptojacking', *IEEE Security & Privacy on the Blockchain (IEEE S&B)* (2018), https://arxiv.org/abs/1803.02887; J. Rüth et al., 'Digging into Browser-based Crypto Mining', *IMC '18: Internet Measurement Conference* (2018), https://arxiv.org/abs/1808.00811; M. Musch et al., 'Thieves in the Browser: Web-based Cryptojacking in the Wild', Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES '19) (2019), https://doi.org/10.1145/3339252.3339261; M. Saad, A. Khormali and A. Mohaisen, 'End-to-End Analysis of In-Browser Cryptojacking', *arVix* (2018), https://arxiv.org/abs/1809.02152. R.K. Konoth, et al., 'Minesweeper: An in-depth look into drive-by cryptocurrency mining and its defense', *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (2018); A. Kharraz, et al., 'Outguard: Detecting In-Browser Covert Cryptocurrency Mining in the Wild', *WWW '19: The World Wide Web Conference* (2019), https://dl.acm.org/doi/10.1145/3308558.3313665.

[7] P. Papadopoulos, P. Ilia and E.P. Markatos, 'Truth in Web Mining: Measuring the Profitability and Cost of Cryptominers as a Web Monetization Model', *arXiv* (2018), https://arxiv.org/abs/1806.01994; S. Venskutonis, F. Hao and M. Collison, 'On legitimate mining of cryptocurrency in the browser – a feasibility study', *arXiv* (2018-2019), https://arxiv.org/abs/1812.04054.

[8] For instance, by P. Papadopoulos, P. Ilia and E.P. Markatos, 'Truth in Web Mining: Measuring the Profitability and Cost of Cryptominers as a Web Monetization Model', *arXiv* (2018), https://arxiv.org/abs/1806.01994.

[9] Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJ L 119/1.

[10] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (e-Privacy Directive), [2002] OJ L 201/37, as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (Text with EEA relevance) (The Citizen's Rights Directive), [2009] OJ L 337/11.

[11] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM/2017/010 final – 2017/03 (COD).

[12] Superior Court of New Jersey, *Jeremy Rubin d.b.a. TIDBIT v. State of New Jersey Division of Consumer Affairs*, 24 November 2014, available at https://www.eff.org › files › 2014.11.24_-_rubin_v._dca_opinion.pdf, p. 2.

[13] Ibid., p. 24.

[14] Ibid., p. 14–15.

[15] TorrentFreak, 'The Pirate Bay Website Runs a Cryptocurrency Miner (Updated)', *TorrentFreak* (2017), https://torrentfreak.com/the-pirate-bay-website-runs-a-cryptocurrency-miner-170916/; TorrentFreak, 'Pirate Bay is Mining Cryptocurrency Again But Forum Staff Aren't Worried', *TorrentFreak* (2018), https://torrentfreak.com/the-pirate-bay-is-mining-cryptocurrency-again-but-forum-staff-arent-worried-180702/.

[16] See, for instance, C. Williams, 'UK ICO, USCourts.gov... Thousands of websites hijacked by hidden crypto-mining code after popular plugin pwned', *The Register* (2018), https://www.theregister.co.uk/2018/02/11/browsealoud_compromised_coinhive/; C. Osborne, 'UK government websites, ICO hijacked by cryptocurrency mining malware', *ZDNet* (2018), https://www.zdnet.com/article/uk-government-websites-ico-hijacked-by-cryptocurrency-mining-malware/. M. Burgess, 'UK government websites were caught cryptomining. But it could have been a lot worse', *Wired* (2018), https://www.wired.co.uk/article/browsealoud-ico-texthelp-cryptomining-how-cryptomining-work.

[17] For a list of websites affected, see PublicWWW: https://publicwww.com/websites/browsealoud.com%2Fplus%2Fscripts%2Fba.js/.

[18] K. McCarthy, 'CBS's Showtime caught mining crypto-coins in viewers' web browsers', *The Register* (2017), https://www.theregister.co.uk/2017/09/25/showtime_hit_with_coinmining_script/.

[19] R. McMillan, 'Gaming Company Fined $1M for Turning Customers Into Secret Bitcoin Army', *Wired* (2013), https://www.wired.com/2013/11/e-sports/

[20] J. Segura, 'The state of malicious cryptomining', *Malwarebyte* Labs (2018), https://blog.malwarebytes.com/cybercrime/2018/02/state-malicious-cryptomining/; C. Cimpanu, 'Coinhive cryptojacking service to shut down in March 2019', *ZDNet* (2019), https://www.zdnet.com/article/coinhive-cryptojacking-service-to-shut-down-in-march-2019/.

[21] M. Musch et al., 'Thieves in the Browser: Web-based Cryptojacking in the Wild', *Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES '19)* (2019), https://doi.org/10.1145/3339252.3339261.

[22] S. Davidoff, 'Cryptojacking Meets IoT', *LMG Security* (2018), https://www.lmgsecurity.com/cryptojacking-meets-iot/.

[23] See for example A. Narayanan et al., *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction* (Princeton University Press, 2016), ch. 2.

[24] Ibid.

[25] Ibid.

[26] See, for example, Zerocrypted, 'Honey Miner Mining Alternatives', *Zerocrypted* (2019), https://zerocrypted.com/honey-miner-mining-alternatives/.

[27] See, for example, D. Oberhaus, 'Seven Ways to Donate Your Computer's Unused Processing Power', *Vice* (2015), https://www.vice.com/en_us/article/bmj9jv/7-ways-to-donate-your-computers-unused-processing-power.

[28] For a description of Coinhive, see B. Krebs, 'Who and What Is Coinhive?', *Krebs on Security* (2018), https://krebsonsecurity.com/2018/03/who-and-what-is-coinhive/. At time of writing, the Coinhive website was not accessible, and Coinhive is defunct.

[29] T. Mursch, 'How to find cryptojacking malware', *Bad Packets* (2018), https://badpackets.net/how-to-find-cryptojacking-malware/.

[30] See the website of Crypto-loot, www.crypto-loot.org.

[31] J. Rüth et al., 'Digging into Browser-based Crypto Mining', *IMC '18: Internet Measurement Conference* (2018), https://arxiv.org/abs/1808.00811.

[32] C. Cimpanu, 'Coinhive cryptojacking service to shut down in March 2019', *ZDNet* (2019), https://www.zdnet.com/article/coinhive-cryptojacking-service-to-shut-down-in-march-2019/.

[33] See the GitHub repository for DeepMiner, https://github.com/deepwn/deepMiner.

[34] At time of writing, the Coinhive codebase was not available online anymore, and the Coinhive website is offline. An overview of the services can be found at https://99bitcoins.com/webmining-monetize-your-website-through-user-browsers/

[35] S. Dashevskyi et al., 'Dissecting Android Cryptocurrency Miners', *arXiv* (2019), arXiv:1905.02602v2.

[36] Crypto-loot, www.crypto-loot.org.

[37] R.K. Konoth, et al., 'Minesweeper: An in-depth look into drive-by cryptocurrency mining and its defense', *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (2018); A. Kharraz, et al., 'Outguard: Detecting In-Browser Covert Cryptocurrency Mining in the Wild', *WWW '19: The World Wide Web Conference* (2019), https://dl.acm.org/doi/10.1145/3308558.3313665.

[38] D. Sinegubko, 'Malicious Website Cryptominers from GitHub. Part 2.', *Sucuri* (2018), https://blog.sucuri.net/2018/01/malicious-cryptominers-from-github-part-2.html.

[39] See the website of Crypto-loot, www.crypto-loot.org.

[40] J. Segura, 'Persistent drive-by cryptomining coming to a browser near you', *Malwarebyte Labs* (2018), https://blog.malwarebytes.com/cybercrime/2017/11/persistent-drive-by-cryptomining-coming-to-a-browser-near-you/.

[41] See Cryptojaxx, 'Does UNICEF Australia's use of web mining legitimise the activity?', *Steemit* (2018), https://steemit.com/cryptocurrency/@cryptojaxx/does-unicef-australia-s-use-of-web-mining-legitimises-the-activity; D. Roua, 'CPUforGood Wants To Free Slaves With Browser Mining', *Steemit* (2018), https://steemit.com/mining/@dragosroua/cpuforgood-wants-to-free-slaves-with-browser-mining.

[42] See Hijmans, H., *The European Union as a Constitutional Guardian of Internet Privacy and Data Protection: The Story of Article 16 TFEU* (University of Amsterdam and Vrije Universiteit Brussel, 2016).

[43] *Lynskey*, O., *The Foundations of EU Data Protection Law* (OUP, 2015), ch. 4.

[44] Directive 2009/136/EC of the European Parliament and of the *Council* of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (Text with EEA relevance) (The Citizen's Rights Directive), [2009] OJ L 337/11. See also, E. Kosta, *Consent in European Data Protection Law* (Nijhoff, 2014), p. 293 et seq.

[45] Article 99 GDPR.

[46] Article 5(3) ePrivacy Directive. See E. Kosta, 'ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation', *Study for the European Commission DG Communications Networks, Content* (2015) and the annexed tables to the study for a detailed analysis of the national divergence.

[47] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM/2017/010 final – 2017/03 (COD).

[48] S. Stolton, 'Commission to present revamped ePrivacy proposal', EurActiv (2019), https://www.euractiv.com/section/data-protection/news/commission-to-present-revamped-eprivacy-proposal/.

[49] Article 2 GDPR sets out the material scope and Article 3 GDPR sets out the territorial scope.

[50] Case C-582/14 *Partick Breyer v. Bundesrepublik Deutschland*, EU:C:2016:779.

[51] Recital 30 GDPR.

[52] Article 3 ePrivacy Directive. See for a detailed explanation E. Kosta, 'ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation', *Study for the European Commission DG Communications Networks, Content* (2015), p. 24 et seq.

[53] 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, adopted 12 March 2019.

[54] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, [1995] OJ L 281/31.

[55] 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, adopted 12 March 2019, para. 37 et seq.

[56] Ibid. See also C. Etteldorf, 'EDPB on the Interplay between the ePrivacy Directive and the GDPR', 2 *European Data Protection Law* Review (2019), p. 226–227 and the guidelines, opinions and judgements mentioned therein. Especially, Case C-673/17 *Planet49 GmbH v. Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV*, EU:C:2019:801.

[57] See Opinion 2/2010 of the Article 29 Working Party on online behavioural advertising, 22.6.2010, WP 171; Opinion 9/2014 of the Article 29 Working Party on the application of Directive 2002/58/EC to device fingerprinting, 25.11.2014, WP 224; Zuiderveen-Borgesius, F.J., 'Personal data processing for behavioural targeting: which legal basis?', 5 *IDPL* (2015); Case C-582/14 *Partick Breyer v. Bundesrepublik Deutschland*, EU:C:2016:779.

[58] Article 5(b) GDPR read in conjunction with Article 6 GDPR.

[59] See among others, Berberich, M., & Steiner, M., 'Practitioner's Corner: Blockchain Technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers?', 2 *European Data Protection Law* 3 (2016); Finck, M., 'Blockchains and Data Protection in the European Union', 4 *European Data Protection Law Review* 1 (2018); Finck, M., 'Blockchains and Data Protection in the European Union', *MPI for Innovation and Competition Research Paper* no. 18-01 (2018); Ramsay, S., 'The General Data Protection vs. The Blockchain: A legal study on the compatibility between blockchain technology and the GDPR', *DiVA* (2018); Schwerin, S., 'Blockchain and Privacy Protection in the Case of the European General Data Protection Regulation (GDPR): A Delphi Study', 1 *The Journal of The British Blockchain Association* 1 (2018); Blockchain Bundesverband, 'Blockchain, data protection, and the GDPR', *Blockchain Bundesverband* (2018); Kuner, C., et al., 'Blockchain versus data protection', 8 *European Data Privacy Law* 2 (2018). CNIL, 'Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data', *CNIL* (2018). EU Blockchain Observatory, 'Blockchain and the GDPR – a thematic report by the EU Blockchain Observatory', European Commission (2018), https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf?width=1024&height=800&iframe=true.

[60] L. Edwards et al., 'Data subjects as data controllers: a Fashion(able) *concept*?', *Internet Policy Review* (2019); Finck, M., 'Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law?', *European Parliament Research Service, Study for the STOA Committee* (2019).

[61] See CNIL, 'Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data', *CNIL* (2018), p. 3–4.

[62] N. van Saberhagen, 'CryptoNote v 2.0', *CryptoNote* (2013), https://cryptonote.org/whitepaper.pdf.

[63] 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, adopted 12 March 2019, para. 40.

[64] Case C-673/17 *Planet49 GmbH v. Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale* Bundesverband *eV*, EU:C:2019:801, para. 71.

[65] E. Kosta, *Consent in European Data Protection Law* (Nijhoff, 2014), p. 293 et seq.; E. Kosta, 'ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation', *Study for the European Commission DG Communications Networks, Content* (2015), p. 12 et seq.

[66] Opinion 2/2010 of the Article 29 Working Party on online behavioural advertising, 22.6.2010, WP 171; Opinion 9/2014 of the Article 29 Working Party on the application of Directive 2002/58/EC to device fingerprinting, 25.11.2014, WP 224. E. Kosta, *Consent in European Data Protection Law* (Nijhoff, 2014), p. 264.

[67] Case C-673/17 *Planet49 GmbH v. Bundesverband der Verbraucherzentralen* und *Verbraucherverbände – Verbraucherzentrale Bundesverband eV*, EU:C:2019:801, para. 69.

[68] Case C-673/17 *Planet49 GmbH v. Bundesverband der Verbraucherzentralen* und *Verbraucherverbände – Verbraucherzentrale Bundesverband eV*, EU:C:2019:801, para. 70.

[69] E. Kosta, *Consent in European Data Protection Law* (Nijhoff, 2014), p. 294–296; E. Kosta, 'ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation', *Study for the European Commission DG Communications Networks, Content* (2015), p. 51–51.

[70] Ibid.

[71] Ibid.

[72] Translation by author; emphasis added. Original: '*het verbod op cookiewalls ziet niet alleen op het plaatsen van cookies. Niet alleen cookies vallen onder deze beschrijving, maar ook daarmee vergelijkbare technieken waarvoor eveneens toestemming gevraagd moet worden. Dit zijn technieken zoals Javascripts, Flash cookies, HTML5-local storage en/of web beacons.*' Autoriteit Persoonsgegevens, 'Cookies', *Autoriteit Persoonsgegevens*, https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/cookies.

[73] 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, adopted 12 March 2019, para. 40.

[74] E. Kosta, 'ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation', *Study for the European Commission* DG *Communications Networks, Content* (2015), p. 60.

[75] Ibid.

[76] See F. Zuiderveen Borgesius et al., 'An assessment of the Commission's Proposal on Privacy and Electronic Communications', *Study for the LIBE Committee of the European Parliament* (2017), p. 23-24.

[77] Case C-673/17 *Planet49 GmbH v. Bundesverband der* Verbraucherzentralen *und Verbraucherverbände – Verbraucherzentrale Bundesverband eV*, EU:C:2019:801.

[78] F. Zuiderveen Borgesius et al., 'An assessment of the Commission's Proposal on Privacy and Electronic Communications', *Study for the LIBE Committee of the European* Parliament (2017), p. 25.

[79] P. Papadopoulos, P. Ilia and E.P. Markatos, 'Truth in Web Mining: Measuring the Profitability and Cost of Cryptominers as a Web Monetization Model', *arXiv* (2018), https://arxiv.org/abs/1806.01994.

[80] Ibid. S. Venskutonis, F. Hao and M. Collison, 'On legitimate mining of cryptocurrency in the browser – a feasibility study', *arXiv* (2018-2019), https://arxiv.org/abs/1812.04054.

[81] V. Marotta, K. Zhang and A. Acquisti, 'The Welfare Impact of Targeted Advertising', *SSRN* (2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2951322.

[82] Ibid.

[83] P. Papadopoulos, P. Ilia and E.P. Markatos, 'Truth in Web Mining: Measuring the Profitability and Cost of Cryptominers as a Web Monetization Model', *arXiv* (2018), https://arxiv.org/abs/1806.01994.

[84] F. Zuiderveen Borgesius et al., 'Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation', 3 *European Data Protection Law Review* (2017).

[85] S. Venskutonis, F. Hao and M. Collison, 'On legitimate mining of cryptocurrency in the browser – a feasibility study', *arXiv* (2018-2019), https://arxiv.org/abs/1812.04054.

[86] Christopher F. Mondschein, 'Some Iconoclastic Thoughts on the Effectiveness of Simplified Notices and Icons for Informing Individuals as Proposed in Article 12(1) and (7) GDPR', 2 *European Data Protection Law Review* (2016).

[87] R.E. Leenes and E. Kosta, 'Taming the Cookie Monster with Dutch Law – A Tale of Regulatory Failure', 31 *Computer Law and Security Review* (2015); F. Zuiderveen Borgesius et al., 'Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation', 3 *European Data Protection Law Review* (2017).

[88] E. Kosta, 'ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation', *Study for the European Commission DG Communications Networks, Content* (2015), p. 61 et seq.

[89] M. Trevisan et al., '4 Years of EU Cookie Law: Results and Lessons Learned', *Proceedings on Privacy Enhancing Technologies* (2019); C. Santos, N. Bielova and C. Matte, 'Are cookie

banners indeed compliant with the law? Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners', *arXiv* (2019), https://arxiv.org/abs/1912.07144, p. 46 et seq.

[90] Case C-673/17 *Planet49 GmbH v. Bundesverband der* Verbraucherzentralen *und Verbraucherverbände – Verbraucherzentrale Bundesverband eV*, EU:C:2019:801; Opinion of Advocate General Szpunar in Case C-673/17 *Planet49 GmbH v. Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV*, EU:C:2019:246, para. 57 et seq.

[91] Opinion of Advocate General Szpunar in Case C-673/17 *Planet49 GmbH v. Bundesverband der Verbraucherzentralen und* Verbraucherverbände – *Verbraucherzentrale Bundesverband eV*, EU:C:2019:246, para. 99.

[92] F. Zuiderveen Borgesius et al., 'Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation', 3 *European Data Protection Law Review* (2017).

[93] Ibid., p. 14.

[94] Ibid.

[95] 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, adopted 12 March 2019, para. 87–91.

