PrivacySmart: Automatic and Transparent Management of Privacy Policies

Cristòfol Daudén-Esmel[1,2][0000−0002−4607−4035], Jordi Castellà-Roca[1,2][0000−0002−0037−9888], Alexandre Viejo[1,2][0000−0003−2342−5100], and Eduard Josep Bel-Ribes[1]

[1] Universitat Rovira i Virgili
Departament d'Enginyeria Informàtica i Matemàtiques
[2] UNESCO Chair in Data Privacy, CYBERCAT-Center for Cybersecurity Research of Catalonia
Av. Països Catalans 26, E-43007 Tarragona, Catalonia, Spain
{cristofol.dauden,jordi.castella,alexandre.viejo}@urv.cat
eduardjosep.bel@alumni.urv.cat

Abstract. Privacy policies and the use of cookies on websites serve important functions but also raise concerns regarding the user's privacy and activity tracking. In order to address these concerns and adhere to legal requirements, web service providers utilize pop-ups to obtain the user's consent based on the notice-and-choice principle. However, a significant issue arises when users accept all policies without thoroughly reading or comprehending them, resulting in difficulties in managing and recalling previously accepted policies across various websites. To tackle this challenge, we propose PrivacySmart: an innovative system that manages privacy and cookie policy pop-ups for the users as they navigate and access online services, all while taking their privacy preferences into account. The system comprises two essential components: a plug-in that necessitates installation on users' browsers and a smartphone application that consolidates all accepted policies from different plug-ins. This system empowers users by granting them control over the policies they have accepted and their corresponding websites, while allowing them to avoid the policy management overhead. By implementing our tool as a Firefox extension, we have conducted thorough evaluations and obtained promising results from the experiments.

Keywords: Privacy and cookie policies · GDPR · Blockchain and Smart Contracts · Browser plug-in.

1 Introduction

A typical income source for web Service Providers (SPs) comes from the ads shown while users access their provided services and from the users' personal data collected while they use the service. This data can be sold to third parties which will process it to obtain some benefit, sometimes by creating profiles which allow personalized advertising [8, 12].

Although processing of this information facilitates free online services, it may result in the extraction of sensitive data which may jeopardize the users' privacy. This fact raised serious concerns about the technical, commercial, political, and ethical aspects of personal data collection and its analysis by platform owners such as Facebook and other third parties.

In light of the above, the European Union drafted and approved the General Data Protection Regulation (GDPR) [21] to mitigate possible abuses when collecting and processing massive personal user data, hence, keeping any data-hungry company at bay. The main objective of the GDPR is to guarantee specific privacy rights to Data Subjects (natural person to which personal data belongs), ensuring that their personal data "can only be gathered legally, under strict conditions, for a legitimate purpose;" as well as bringing full control back to the data owners.

The scientific community has already paved the way to manage the data processing consent between users and SPs in compliance with the GDPR. In this regard, some authors have already introduced the use of Smart Contracts (SCs) implemented over the blockchain technology (BC) to design and create general-purpose data management and storage schemes which promise to offer transparency, traceability, non-repudiation, integrity, immutability, and decentralization [23, 9, 28, 20, 6, 1, 16, 13, 5] among other features. However, even these works grant users the full control about how their data is used - solving the issue of *lack of transparency* [2] in the current paradigm - they do not provide the user with a practical solution to perform this management comfortably.

According to a study carried out on European websites [7], almost two years after the GDPR came into force, 81% of the reviewed sites use pop-up notifications to inform users about their privacy and cookie policies, fulfilling the current regulation. These pop-ups must generally be managed before accessing the service, thus annoying users and slowing down browsing. Furthermore, the average Internet user must manage privacy and cookies preferences on almost every website she visits - at least once a year, since according to the ePrivacy Directive[3], persistent cookies should expire after 12 months. Besides pop-up interaction required, many websites offer complicated and often misleading methods to eject cookies and privacy policies; sometimes they require several clicks; sometimes the option to reject them is not even offered. With all this, users usually end up accepting everything directly without checking anything to save time and effort. In addition, the volume of manually managed privacy and cookie policies is so high that they end up forgetting what they accepted and where.

1.1 Related Work

As it has been stated, privacy policies and cookies usage management is a tedious and uncomfortable process for users who just want to access to some service in the web [15]. In order to address this, some works have been proposed to facilitate this management. On the one hand, there are proposals that address

[3] GDPR Cookies `https://gdpr.eu/cookies/`

the consent management between users and Service Providers through the use of smart contracts and the blockchain technologies. On the other hand, some tools have been proposed to facilitate this privacy policies and cookies usage management by simply performing their automatic acceptance or rejection.

There are several proposals in the literature that fall into the first category, systems for the GDPR compliance of the consent management, some relevant examples are [23], [9], [28], [20], [6], [1], [16], [13] and [5]. These schemes follow a similar approach. In particular, they combine a decentralized storage system, the Ethereum blockchain, and smart contracts, in order to provide a dynamic consent management system that targets personal data usage under the GDPR. More specifically, these scheme systems allow individuals to control the collection and usage consent of their personal data throughout the data life-cycle. An example can be found in [5], where authors propose a blockchain-based GDPR-compliant personal data management system that, first, it provides mechanisms for Data Subjects to control and manage their personal data; and, second, it provides publicly accessible and immutable evidences which are useful for a Service Provider to prove the agreements made between a Data Subject and her about the Data Subject's personal data. These evidences might be then used by a Supervisory Authority that performs an auditing procedure on the Service Provider to verify that this entity is doing the data processing exactly as agreed with the affected Data Subjects. However these proposals do not provide a practical solution for users to manage their personal data consent when they access different services on the web, specifically they do not take into account privacy policies and cookies usage pop-ups paradigm which is currently established now.

Focusing on solutions that address automatic management of users' privacy and cookie policies, Vyas et al. propose in [22] a framework for automatically producing privacy policies for users' personal web contents based on a small amount of annotation information. However, this work is limited to the generation of individual policies for each content published into a social network, they do not consider general consent given when accessing different web services that request users' data collection. In a more general ambit, authors in [26] and [27] present CookiePicker, a system that automatically validates the usefulness of cookies from a Web site and set the cookie usage permission on behalf of users. This system identifies those cookies that cause perceivable changes on a web page as useful, while simply classifying the rest as useless, thus enabling useful cookies and disabling the rest. However, this system does not take into account current paradigm where web service providers do not limit data collection from cookies but from other sources, making the users also to accept their privacy policies. Finally, authors in [14], present a concept for a privacy-friendly cookie setting interface that tries to help users during cookies preferences configuration. Their concept uses an assistant that guides the user to configure their privacy preferences via a series of questions. These preferences will be applied in the cookies configuration to all visited websites. However, the interface just manages the functionalities available in the cookie settings of common browsers, it does not consider available configurations on individual websites, neither the pri-

vacy policies that must be accepted on these websites. If a user wants a specific privacy and cookie policies configuration according to her privacy preferences on each website, it must be done manually.
A part from the scientific works trying to address the aforementioned issue with the automatic and transparent management of privacy and cookie policies, modern web browsers also provide users with some solutions. A user can set detailed cookie privacy options for web sites before or during visiting these sites. However, these cookie privacy options use to fail when are used in practice, as they are confusing for regular users [10].
On the other hand, we can find some commercial cookie management software for regular web browsers. While analyzing these tools, we have observed that although they all manage some cookie pop-ups and are convenient to use, they are not so versatile in terms of the number of web pages with which they can interact. For example, Polish Cookie Consent [11] automatically accepts cookie policy/GDPR on websites. On the other hand, Ninja Cookie [4] and Auto Cookie Output [3] have a more restrictive policy by removing cookie banners and rejecting the use of non-essential cookies. Finaly, Super Agent [19] automatically fills out website's cookie consent forms on user's behalf based on their preferences. This tool splits optional cookies into three categories (Advertising, Functional and Performance), thus automatically opt out of cookies that are not clearly within any of these categories and let users control the remaining three. Although a combination of these tools could be efficient in terms of cookies acceptance/rejection, they do not offer cookies management, as none offers the possibility of consulting the consent they manage neither take into account privacy policies that also must be managed along with cookies.

After evaluating the available proposals pertaining to privacy policies and the administration of cookie usage, we have come to recognize two main trends. On one hand, there are proposals aimed at addressing consent management between users and service providers, but these often lack practicality. On the other hand, there are tools designed to streamline the management of privacy policies and cookie usage by employing automatic acceptance or rejection mechanisms. However, these tools limit users' ability to maintain comprehensive control over the consents they grant. In light of these findings, there is a clear necessity for a practical solution that enables users to effortlessly and transparently handle privacy policies and cookie usage while retaining full control over all granted consents.

1.2 Contribution and plan of this paper

This paper presents the development and deployment of PrivacySmart, a system aimed at effectively managing privacy and cookie policies pop-ups for users engaging with online services. Our system offers an automated and transparent approach to managing these policies, ensuring a seamless user experience when navigating, and registers the provided consent on a Smart Contract deployed on the blockchain. The system comprises two essential components: a plug-in that manages the policies, and a smartphone application that offers control over the

acceptance of policies across various websites.
Given a privacy level provided by the user, the designed plug-in must:

- Perform an automatic acceptance of the cookies, according to the privacy level specified by users, thus allowing an easier and faster browsing of the web.
- Register the given consent on each website through a Smart Contract, that will be deployed in the blockchain.
- Be compatible with the main websites privacy and cookie policies pop-ups.

The rest of the paper is organized as follows: First, in Section 2 we introduce and describe our proposed system. Then, in Section 3 we analyze and discuss the system. And finally, in Section 4 we present the conclusions of this paper and future work directions.

2 Proposal Description

In this section we describe our system for the automatic management of cookie and personal data usage policies which comprises the agreements between Data Subjects and Service Providers about DSs' personal data, automatically and transparently to the users while they navigate and access online services.

The plug-in offers several key functionalities: Firstly, it automatically accepts cookies and privacy policies based on user-specified privacy levels, making web browsing easier and faster. Secondly, it registers user consent on each website using a Smart Contract, ensuring a secure record of the provided consent. The plug-in is compatible with cookie pop-ups from major websites, it effectively identifies cookie and privacy policies configuration pop-ups, and it determines the appropriate selections that align with the user's privacy preferences. This process includes deploying a Smart Contract on the blockchain to record the provided consent, allowing the user to control and manage accepted privacy and cookie policies for each visited website.
In addition, we provide a smartphone application that consolidates all privacy and cookie policies managed by the plug-in, empowering the user with complete control over their personal data while giving them a clear overview of the management of their privacy preferences.

2.1 System Architecture Overview

As shown in Figure 1 we can identify four components on our working environment: our proposed plug-in, the provided smartphone application through which the user has full control of the accepted policies, the blockchain where SCs are deployed, and the web browser - where the plug-in is installed - that the user uses to access different websites. The plug-in consists of three main modules: the core module, the pop-up interaction module and the configuration module. The core module identifies the privacy pop-up of the web site visited, it initializes the module responsible of directly interacting with the pop-up and deploys a new

SC with the cookies and privacy policies accepted. Then, the pop-up interaction module - which consists of a set of scripts, each designed specifically for a concrete pop-up - accepts or rejects the cookies and privacy policies on the pop-up and returns the configuration set to the main program. Finally, the configuration module allows the user to set-up her privacy preferences, to configure the keys used for interacting with the blockchain, and to manage all the consents given by the plug-in trough a UI. The smartphone application plays a crucial role in enhancing the user's control and convenience. It seamlessly downloads all the consent Smart Contracts (SCs) deployed on the blockchain, effectively summarizing all policies that have been accepted by the plug-ins installed across any users' browsers. This consolidated view offers a comfortable and user-friendly review of the collection of accepted policies.

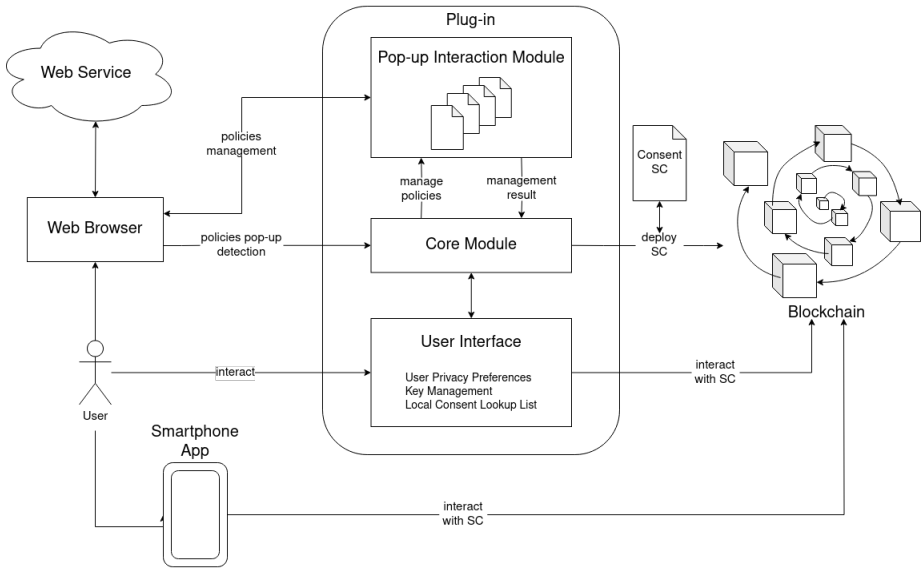


Fig. 1: System Architecture Overview

2.2 User Privacy Preferences

The Privacy policies state who will be able to use the user's collected data, for which purpose can be used and for how long it can be kept. These policies can be represented at different levels of specification and data granularity, like a formal notice or like a more structured notice using templates. Formal notice allows Service Providers to set up a more customized privacy policies thus being able to arbitrarily create rules that describe how data will be managed. These policy notices are difficult to interpret, to read and to match automatically due to the

variability in the terms and phrasing used across websites when describing the rules. A clear example of this kind of policies are the Terms and Conditions a user must accept when signing up to certain services. Some Service Providers opt for more structured notices, such as cookies and privacy policies configuration pop-ups. These pop-ups consist of templates provided by some "*cookies providers*" which are easier to interpret and manage automatically. According to this, work focuses on the management of these web policy pop-ups according to the user's pre-established privacy preferences.

To ease the policy specification process, we consider using policy templates, as suggested in [18]. These templates represent different privacy levels, defined according to the configuration alternatives that offer the studied pop-ups. These privacy levels can be divided into four main categories – from the most restrictive level one to the most permissive level four – which are:

1. Reject all: all cookies or all non-essential cookies are rejected.
2. Reject profiling cookies and third parties: this configuration rejects the use of cookies for profiling interest. Furthermore, it rejects the use of the collected data by third parties or web site partners.
3. Reject third parties: this option just rejects the use of the collected data by third parties or web site partners.
4. Accept all: all cookies are accepted.

In order to set up this privacy preferences value, the user must be requested to select one of the provided options when the plug-in is installed in the web browser.

2.3 Pop-up interaction module

In the current model, websites offer management of their privacy and cookie policies through pop-ups. In order to cover this need, there are companies, privacy and cookie policies banner providers, that are dedicated to the design of these cookie management pop-ups and provide these tools to other companies which can use them in their websites. In this way, website providers can comply with the GDPR thus presenting the users their privacy policies and a way to grant them.

Each website provider can modify the visual section and the content of the pop-up, by specifying which types of cookies will be used, which data can be collected and which third parties will process the collected data. The main interoperability issue here is that each cookies provider makes its own standard, so the solutions to manage the forms on each website can be very different.

In order to decide which privacy and cookie policies banner providers take into account, we have considered the most used ones according to a study performed by Wrappalyzer [24], where they have analyzed over 1.200.000 websites. The selected ones on this study are Didomi[4], CookieYes[5], CookieNotice[6] and

[4] Didomi: `https://www.didomi.io/es/`
[5] CookieYes: `https://www.cookieyes.com/`
[6] Cookie Notice: `https://cookiesnotice.com/`

OneTrust[7]. For each of these providers we have implemented a script in the pop-up interaction module responsible of interacting with the banner and manage the consent on users' behalf. The result of the operation is sent back to the Core module, which will record it into an SC. In the case some privacy and cookie policies pop-up does not allow the consent management using a privacy level lower than the one set by the user, the pop-up interaction module, hides the banner without accepting anything, in such a way that the user can access to the web content without being annoyed. This modularity of the system allows the tool to be able to work with more privacy and cookie policies banners of other providers by simply adding specific scripts for them to this module.

2.4 Consent Smart Contract

The Consent SC is responsible for storing the consent managed by the plug-in when it interacts with the web browser pop-up. The SC consists in a single class that holds:

- Web service url: Uniform resource locator of the web page where consent has been managed through the plug-in (*url* argument).
- Privacy level: Integer value that indicates the privacy level established by the user and the one used by the plug-in to perform the acceptance of policy cookies (*privacyLevel* argument).
- Consent validity period: This indicates the dates from which the consent is valid(*beginningDate* and *expirationDate* arguments).

Once the *Consent Smart Contract* instance is created, the following methods can be used to interact with it:

- *whichWeb()* method returns the url value stored in the SC.
- *whichPreference()* method returns the privacy level value stored in the SC.
- *isValid()* method checks that the consent lifetime period has not expired.

2.5 Workflow

The proposed plug-in workflow can be divided into three main phases: the set-up phase, where the plug-in is installed on the web browsers and the user indicates her privacy policy preferences; ii) the navigation phase, when the user accesses to different web pages, and; iii) the control phase, where the user can manage all cookies and privacy policies accepted by the plug-in.

1. Set-up phase
   User
   (a) Install the plug-in on the web browser.
   (b) Configure the plug-in.
      i. Set privacy policy preferences in the plug-in using the UI.

[7] OneTrust: `https://www.onetrust.es/`

ii. Chose wheter to use and existing key pair for the deployment of the SCs or to generate a new one. In the first case, the user must input the mnemonic words associated to that key pair and move to step 1d; otherwise, the workflow continues as stated.

Plug-in

(c) Execute the BIP-39 protocol [17], such generating 24 mnemonic words and a 512 bits seed, the *BIP-39 seed*.
NOTE: The user must keep these mnemonic words in a safe place, without them she will not be able to recover the keys or use the same account into another web browser or the smartphone application.

(d) Execute the BIP-32 protocol [25] using the *BIP-39 seed* as input. This process generates user's Secret Key (SK_u).

(e) Derives user's Public Key (PK_u) by means of SK_u.

(f) Create a local consent lookup list. This list is internally used by the plug-in to check if the privacy and cookie policies on a particular website have already been managed.

2. Navigation phase

User

(a) Access a web page with cookies and privacy policies configuration banner.

Plug-in - Core module

(b) If the cookies and privacy policies have already been managed on this web and the consent is valid - *isValid()* method of the Consent SC returns True - no banner will appear and the process will end. Otherwise, if the cookies and privacy policies have already been managed on this web but the consent is not valid - *isValid()* method of the Consent SC returns False - the pertinent cookies are removed from the browser and the process follows as if the consent had not yet been managed.

(c) Detect the emerging pop-up and identifies the script in the pop-up interaction module responsible of managing it.

(d) Initialize the pop-up interaction module script, indicating the user's privacy policy preferences.

Plug-in - Pop-up interaction module

(e) The script interacts with the pop-up, performs the cookies and privacy policies configuration management, and returns the result to the core module.

Plug-in - Core module

(f) The core module deploys a new Consent SC on the blockchain - using the key pair (PK_u, SK_u) - indicating the consent granted and the lifetime of the consent. This process returns an identifier of the SC.

(g) The core module adds the web url along with the SC's identifier to the consent lookup list.

3. Management phase

User

(a) Requests the consents managed by the plug-in through the UI.

Plug-in

(b) The plug-in displays the consent lookup list with all consents managed.

(c) In the case the user wants to see the details of a given consent, she selects it on the display.
(d) The plug-in gets the details of the selected consent from the blockchain and displays them for the user.

The provided smartphone application empowers the users with complete control over all privacy and cookie policies managed by all the associated plug-in installed on any browsers by the user. To ensure a comfortable and user-friendly experience, the application offers these simple functionalities:

1. Add s new key pair: This allow users to add a new key pair (PK_i, SK_i) by introducing the mnemonic words provided by the different plug-ins during the set-up phase. By using these mnemonic words, the app will execute BIP-39 and BIP-32 protocols, as in the plug-in Set-up phase, thus recovering the cryptographic keys. After adding a new key pair the app will have full access to all SCs containing the managed policies.
2. Access and Review: Users can conveniently access and review the entire collection of accepted policies through the application. This allows an easy monitoring and management of privacy preferences.

By providing these functionalities, the smartphone application ensures that the user has a seamless and user-friendly experience, enabling them to exercise complete control over their privacy and cookie policies across different plug-ins installed on their browsers.

3 Discussion

After implementing the described proposal, we have validated its efficacy through live experiments.

3.1 Implementation

We have implemented our plug-in as a Firefox extension coded in JavaScritp[8], HTML[9] and CSS[10] (source code available in Github [11]). We have chosen Firefox because it is one of the most used browsers, it is very extensible, and it allows programmers to add new features or modify existing ones. The scripts in the pop-up interaction module - each to manage a different banner provider - are coded in JavaScript. Concerning the deployment of the Consent SCs, we have used web3.js library [12], so the plug is able to connect into an existing blockchain.

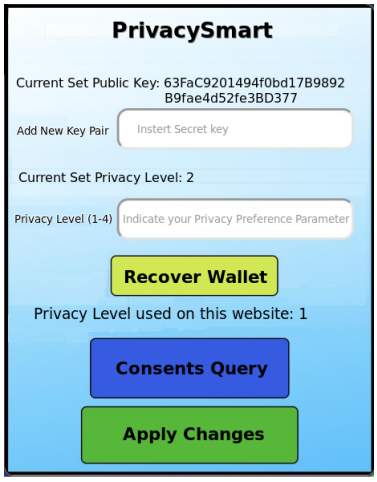
[8] JavaScript: `https://developer.mozilla.org/en-US/docs/Web/javascript`
[9] HyperText Markup Language: `https://developer.mozilla.org/en-US/docs/Web/HTML`
[10] Cascading Style Sheets: `https://developer.mozilla.org/en-US/docs/Web/CSS`
[11] Source Code: `https://github.com/EduardBel/PrivacySmart`
[12] Web3.js: `https://web3js.org/#/`

Summarizing, our plug-in is installed on Firefox as an add-on, wihtout modifying the browser's source code. We omit further details on the tool implementation and only describe plug-in's main interfaces (Figure 2): the plug-in Configuration module main interface and the consent display interface. The configuration module interface, shown in Figure 2a, allows users to i) manually modify the key pair used to deploy the SCs where the consent is registered; ii) recover an old key pair using the mnemonic words set; iii) change user's privacy preference parameter, and; iv) manage the consents given by the plug-in on the different web sites the user has visited. In order to update the new values for the new key pair or the privacy preference parameter, after adding the new values, the user has to click the "Apply Changes" button. On the same way, if the user wants to see all consents given by the tool, she must click the "Consents Query" button, and the consent display interface will pop-up. Finally, if the user needs to recover an old key pair, she must click the "Recover Wallet" button, and a new interface will appear to introduce the mnemonic words. This UI also shows the user the consent given in the current web site, if any.
The consent display interface shows all privacy and cookie policies managed by the plug-in on the different websites the user has visited. As shown in Figure 2b, it displays each of the sites, along with the privacy level used on that site and a button in the case the user wants more detailed information of the consent given.
Concerning the smartphone application, it has been coded using Java and web3j library for blockchain interactions. Figure 3, shows the main display interfaces of the application. On the one hand, Figure 3a shows how the application displays on which websites the policies have been managed by a selected a plug-in (the plug-in has been selected in a previous layout, and these plug-ins are added to the app by specifying the key pair used for deploying the Consent SC). On the other hand, after a user selects a specific website, all information about the consent given is shown as in Figure 3b.

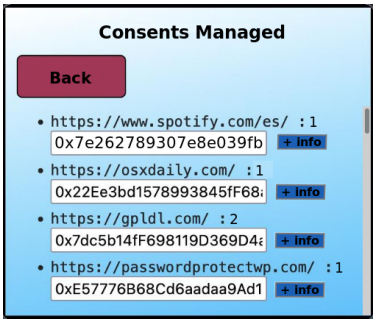
3.2 Evaluation

We installed our proposed plug-in on a Firefox web browser and used Ganache[13] for the simulation of a public blockchain in order to perform our experiments. On the experiments carried out, although key management system is already implemeted, we have used the keys provided by Ganache for the deployment of the ConsentSCs in the blockchain.
In order to determine the correctness of the proposed plug-in, we have evaluated its performance on some websites that use a pop-up offered by the most used privacy and cookie policies banner providers according to [24]. Here we have used different user's privacy parameter values and we have taken into account i) if the plug-in is able to manage the pop-up transparently and on users behalf, so the user does not even notices it, and; ii) if the consent has been performed

[13] Ganache: `https://trufflesuite.com/ganache/`

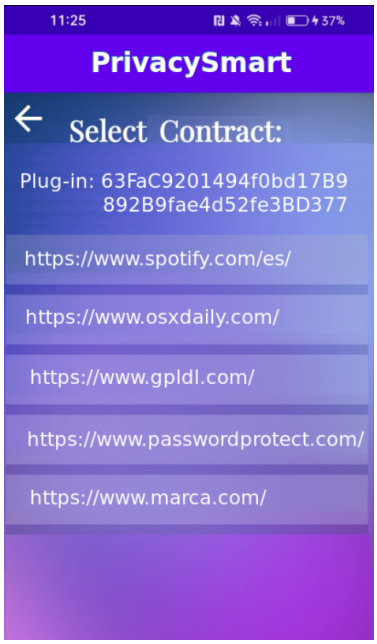


(a) Plug-in configuration module main interface.

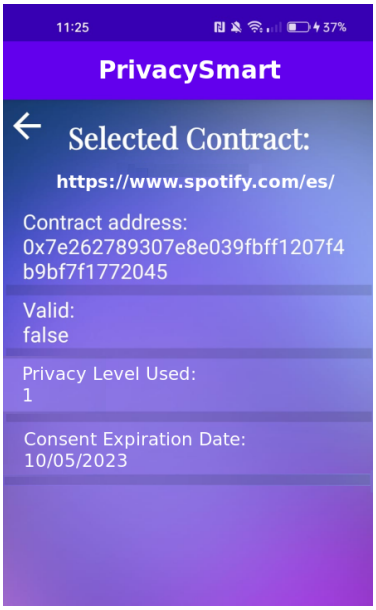


(b) Consent display interface.

Fig. 2: PrivacySmart: browser plug-in main interfaces.



(a) Interface for selecting a consent managed from a browser plug-in.



(b) Interface for viewing managed consent information.

Fig. 3: PrivacySmart: smartphone application main interfaces.

according to user privacy preferences. In the first parameter (*Transparent Management*, third column in Table 1), our evaluation primarily revolves around the plugin's capability to handle the pop-up discreetly, ensuring that the user remains unaware of its presence. We consider the scenario wherein consent cannot be managed in accordance with the user's specified privacy parameters, and in such cases, the plugin should adeptly conceal the pop-up, preventing any disruption or annoyance to the user. According to the second parameter we evaluate if the consent has been managed according to the user's privacy preference, and the Consent SC has been deployed correctly.
Results obtained, summarized in Table 1, show that our plug-in works perfectly with pop-ups provided by Didomi and OneTrust, allowing users to decide between different privacy preference levels. On the other hand, results obtained in relation to the management of the CookieYes and CookieNotice banners, show that there are pages that do not offer consent management beyond accepting all privacy and coolies policies. If user's privacy preference is set to level 4, it accepts the policy, on any other case the plug-in just hides the pop-up without accepting anything.

4 Conclusions and Future Work

This paper introduces, PrivacySmart, a system designed to manage privacy and cookie policies pop-ups seamlessly and transparently for users during their navigation and access to various online services. The system comprises two components: a plug-in that needs to be installed on each browser used by the user, and a smartphone application that empowers the user to maintain control over the accepted policies across different plug-ins and websites. By using this system, users can navigate the web with ease, as the plug-in automatically handles privacy and cookie policies pop-ups. The smartphone application serves as a centralized tool, enabling users to monitor and manage the acceptance of policies on a per-plug-in and per-website basis. This approach ensures transparency and allows users to maintain control over their privacy preferences throughout their online experiences. We have implemented our design as a Firefox extension and we evaluated its performance on some websites that use a pop-up offered by the privacy and cookie policies banner providers considered in this work. Results show that, although our plug-in has some issue to manage the consent on some websites depending on user's privacy preferences due to the service provider, the tool is able to manage all pop-ups transparently and on users behalf.

Regarding future work, we aim to manage the privacy and cookie policies banners of more service providers and implement the tool for other web browsers to increase the number of its users. On the other hand, the proposal that has been presented in this work is a first version of an end user tool for the management of web privacy and cookie policies, we plan to extend the system for the management of general consent under GDPR as stated in [5]. Furthermore we will perform a more in deep discussion taking into account usability of the proposal, a threat analysis of the code and an economic study evaluating over which net-

Provider	Website	Transparent Management	Privacy level used	Consent Correct
Didomi	marca.com	✓	1	✓
	as.com	✓	1	✓
	elpais.com	✓	2	✓
	giphy.com	✓	2	✓
	reverso.net	✓	3	✓
	elmundo.es	✓	3	✓
	bfmtv.com	✓	4	✓
	societe.com	✓	4	✓
CookieYes	wpmet.com	✓	1	✓
	sliderrevolution.com	✓	2	✓
	tympanus.net	✓	3	✓
	wpdatatables.com	✓	4	✓
	bezkoder.com	✓	3	✓
	wpthemedetector.com	✓	4	✓
			2	X
	styde.net	✓	4	✓
			1	X
CookieNotice	gpldl.com	✓	1	✓
			2	✓
	mailtrap.io	✓	1	X
	osxdaily.com	✓	2	X
	searchengineland.com	✓	3	X
	booster.io	✓	3	X
	wpbuffs.com	✓	3	✓
			4	✓
OneTrust	fiverr.com	✓	1	✓
	gitlab.com	✓	2	✓
	app.slack.com	✓	3	✓
	freepik.com	✓	4	✓
	udemy.com	✓	1	✓
	upwork.com	✓	2	✓
	open.spotify.com	✓	3	✓
	elementor.com	✓	4	✓

Table 1: Results of tool performance on websites that use a pop-up offered by the studied privacy and cookie policies banner providers.

work the system will be built (Ethereum, Consortium BC, Private BC...) and who will pay for the gas used to deploy the SCs.

Acknowledgments and disclaimer

This research is supported by the project "HERMES" funded by INCIBE and the European Union NextGenerationEU/PRTR, by project PID2021-125962OB-C32 "SECURING/DATA" funded by MCIN/AEI/10.13039/501100011033/ FEDER, UE, and by the grant 2021SGR 00115 from the Government of Catalonia. The

first author is also supported by the Spanish Government under an FPU grant (ref. FPU20/03254).

References

1. Barati, M., Rana, O.: Tracking gdpr compliance in cloud-based service delivery. IEEE Transactions on Services Computing pp. 1–1 (2020). https://doi.org/10.1109/TSC.2020.2999559
2. Bu-Pasha, S., Alen-Savikko, A., Mäkinen, J.S., Guinness, R., Korpisaari, P.: Eu law perspectives on location data privacy in smartphones and informed consent for transparency. European Data Protection Law Review **2**(3/2016), 312–323 (Sep 2016)
3. CodyMcCodington: Auto cookie optout. `https://addons.mozilla.org/en-GB/firefox/addon/auto-cookie-optout/` (2022)
4. Cookie, N.: Ninja cookie. `https://addons.mozilla.org/en-GB/firefox/addon/ninja-cookie/` (2020)
5. Daudén-Esmel, C., Castellà-Roca, J., Viejo, A., Domingo-Ferrer, J.: Lightweight blockchain-based platform for gdpr-compliant personal data management. In: 5th IEEE International Conference on Cryptography, Security and Privacy, CSP 2021, Zhuhai, China, January 8-10, 2021. pp. 68–73 (2021)
6. Davari, M., Bertino, E.: Access control model extensions to support data privacy protection based on gdpr. In: 2019 IEEE International Conference on Big Data (Big Data). pp. 4017–4024 (Dec 2019). https://doi.org/10.1109/BigData47090.2019.9006455
7. Deloitte: Deloitte: Cookie benchmark study. `https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/risk/deloitte-nl-risk-cookie-benchmark-study.pdf` (2020)
8. Esteve, A.: The business of personal data: Google, Facebook, and privacy issues in the EU and the USA. International Data Privacy Law **7**(1), 36–47 (03 2017). https://doi.org/10.1093/idpl/ipw026, `https://doi.org/10.1093/idpl/ipw026`
9. Faber, B., Michelet, G., Weidmann, N., Mukkamala, R.R., Vatrapu, R.: Bpdims:a blockchain-based personal data and identity management system. In: Conference: Hawaii International Conference on System Sciences (January 2019). https://doi.org/10.24251/HICSS.2019.821
10. Ha, V., Inkpen, K., Al Shaar, F., Hdeib, L.: An examination of user perception and misconception of internet cookies. In: CHI'06 extended abstracts on Human factors in computing systems. pp. 833–838 (2006)
11. hawkeye116477, k.: Polish cookie consent. `https://addons.mozilla.org/en-GB/firefox/addon/polish-cookie-consent/` (2022)
12. Houser, K., Voss, W.: Gdpr: The end of google and facebook or a new paradigm in data privacy? SSRN Electronic Journal (07 2018). https://doi.org/10.2139/ssrn.3212210
13. Jung, S.S., Lee, S.J., Euom, I.C.: Delegation-based personal data processing request notarization framework for gdpr based on private blockchain. Applied Sciences **11**(22) (2021). https://doi.org/10.3390/app112210574, `https://www.mdpi.com/2076-3417/11/22/10574`
14. Kulyk, O., Mayer, P., Volkamer, M., Käfer, O.: A concept and evaluation of usable and fine-grained privacy-friendly cookie settings interface. In: 2018 17th IEEE

International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE). pp. 1058–1063. IEEE (2018)
15. McDonald, A.M., Reeder, R.W., Kelley, P.G., Cranor, L.F.: A comparative study of online privacy policies and formats. In: Privacy Enhancing Technologies: 9th International Symposium, PETS 2009, Seattle, WA, USA, August 5-7, 2009. Proceedings 9. pp. 37–55. Springer (2009)
16. Merlec, M.M., Lee, Y.K., Hong, S.P., In, H.P.: A smart contract-based dynamic consent management system for personal data usage under gdpr. Sensors **21**(23) (2021). https://doi.org/10.3390/s21237994
17. Palatinus, M., Rusnak, P., Voisine, A., Bowe, S.: Bip39: Mnemonic code for generating deterministic keys. `https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki` (2013)
18. Squicciarini, A., Bhargav-Spantzel, A., Czeskis, A., Bertino, E.: Traceable and automatic compliance of privacy policies in federated digital identity management. In: Privacy Enhancing Technologies: 6th International Workshop, PET 2006, Cambridge, UK, June 28-30, 2006, Revised Selected Papers 6. pp. 78–98. Springer (2006)
19. Super Agent, D.M.: Super agent - automatic cookie consent. `https://addons.mozilla.org/en-GB/firefox/addon/super-agent/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search` (2023)
20. Truong, N.B., Sun, K., Lee, G.M., Guo, Y.: Gdpr-compliant personal data management: A blockchain-based solution. IEEE Transactions on Information Forensics and Security **15**, 1746–1761 (2020)
21. Union, E.: Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 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) (text with eea relevance). Official Journal of the European Union L 119 **59**, 1–88 (5 2016), `https://eur-lex.europa.eu/eli/reg/2016/679/oj`
22. Vyas, N., Squicciarini, A.C., Chang, C.C., Yao, D.: Towards automatic privacy management in web 2.0 with semantic analysis on annotations. In: 2009 5th international conference on collaborative computing: networking, applications and worksharing. pp. 1–10. IEEE (2009)
23. Wirth, C., Kolain, M.: Privacy by blockchain design: A blockchain-enabled gdpr-compliant approach for handling personal data. In: Reports of the European Society for Socially Embedded Technologies (EUSSET) (2018)
24. Wrappalyzer: Cookie compliance technologies market share. `https://www.wappalyzer.com/technologies/cookie-compliance/` (2023)
25. Wuille, P.: Bip32: Hierarchical deterministic wallets. `https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki` (2012)
26. Yue, C., Xie, M., Wang, H.: Automatic cookie usage setting with cookiepicker. In: 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN'07). pp. 460–470. IEEE (2007)
27. Yue, C., Xie, M., Wang, H.: An automatic http cookie management system. Computer Networks **54**(13), 2182–2198 (2010)
28. Zichichi, M., Ferretti, S., D'Angelo, G., Rodríguez-Doncel, V.: Personal data access control through distributed authorization. In: 2020 IEEE 19th International Symposium on Network Computing and Applications (NCA). pp. 1–4 (Nov 2020). https://doi.org/10.1109/NCA51143.2020.9306721